



# **Documentazione di ONTAP 9**

## **ONTAP 9**

NetApp  
April 24, 2024

This PDF was generated from <https://docs.netapp.com/it-it/ontap/index.html> on April 24, 2024. Always check docs.netapp.com for the latest.

# Sommario

Documentazione di ONTAP 9 .....	1
Note di rilascio .....	2
Highlight sulla release ONTAP 9 .....	2
Supporto per la release ONTAP 9 .....	7
Novità di ONTAP 9.14.1 .....	8
Novità di ONTAP 9.13.1 .....	13
Novità di ONTAP 9.12.1 .....	18
Novità di ONTAP 9.11.1 .....	23
Novità di ONTAP 9.10.1 .....	28
Novità di ONTAP 9.9.1 .....	33
Integrazione di System Manager con BlueXP .....	38
Scopri i tuoi cluster direttamente da BlueXP .....	38
Scopri di più su BlueXP .....	39
Introduzione e concetti .....	40
Concetti di ONTAP .....	40
Configurazione, aggiornamento e ripristino del software e del firmware ONTAP .....	88
Configurare ONTAP .....	88
Aggiornare ONTAP .....	104
Aggiornamenti del firmware e del sistema .....	236
Ripristina ONTAP .....	243
Amministrazione del cluster .....	276
Gestione del cluster con System Manager .....	276
Gestione delle licenze .....	292
Gestione del cluster con la CLI .....	301
Gestione di dischi e Tier (aggregato) .....	417
Gestione dei livelli FabricPool .....	512
Mobilità dei dati SVM .....	567
Gestione delle coppie HA .....	578
Gestione delle API REST con System Manager .....	602
Amministrazione dei volumi .....	606
Gestione di volumi e LUN con System Manager .....	606
Gestione dello storage logico con la CLI .....	630
Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup .....	769
Gestione dei volumi FlexGroup con l'interfaccia CLI .....	771
Gestione dei volumi FlexCache .....	860
Gestione della rete .....	879
Inizia subito .....	879
Componenti di rete .....	883
Flusso di lavoro di failover del percorso NAS (ONTAP 9,8 e versioni successive) .....	888
Flusso di lavoro di failover del percorso NAS (ONTAP 9,7 e versioni precedenti) .....	896
Porte di rete .....	908
IPspaces .....	934

Domini di broadcast	941
Gruppi e policy di failover	963
Subnet (solo amministratori del cluster)	967
Creare SVM	975
Interfacce logiche (LIF)	982
Bilanciamento dei carichi di rete	1012
Risoluzione del nome host	1021
Proteggere la rete	1024
Contrassegno QoS (solo amministratori del cluster)	1039
Gestione SNMP (solo amministratori cluster)	1041
Gestire il routing in una SVM	1052
Visualizzare le informazioni di rete	1057
Gestione dello storage NAS	1090
Gestire i protocolli NAS con System Manager	1090
Configurare NFS con la CLI	1109
Gestisci NFS con la CLI	1177
Gestire il trunking NFS	1294
Gestire NFS su RDMA	1304
Configurare SMB con la CLI	1310
Gestire SMB con la CLI	1353
Fornire l'accesso del client S3 ai dati NAS	1707
Configurazione SMB per Microsoft Hyper-V e SQL Server	1716
Gestione dello storage SAN	1776
Concetti SAN	1776
Amministrazione SAN	1799
Protezione dei dati SAN	1873
Riferimento alla configurazione SAN	1894
Gestione dello storage a oggetti S3	1938
Scopri il supporto S3 in ONTAP 9	1938
Pianificare	1941
Configurare	1945
Proteggi i bucket con S3 SnapMirror	1995
Controllare gli eventi S3	2029
Autenticazione e controllo dell'accesso	2039
Panoramica dell'autenticazione e del controllo degli accessi	2039
Gestire l'autenticazione dell'amministratore e RBAC	2039
Autenticazione e autorizzazione utilizzando OAuth 2,0	2122
Configurare l'autenticazione SAML	2144
Gestire i servizi Web	2151
Verificare l'identità dei server remoti utilizzando i certificati	2161
Autenticare reciprocamente il cluster e un server KMIP	2164
Sicurezza e crittografia dei dati	2168
Panoramica sulla gestione della sicurezza con System Manager	2168
Proteggersi dal ransomware	2168
Proteggere dai virus	2193

Audit degli eventi NAS su SVM	2234
Utilizzare FPolicy per il monitoraggio e la gestione dei file su SVM	2283
Verificare l'accesso utilizzando il tracciamento di sicurezza	2344
Gestione della crittografia con System Manager	2356
Gestire la crittografia con la CLI	2357
Protezione dei dati e disaster recovery	2452
Protezione dei dati con System Manager	2452
Peering di cluster e SVM con CLI	2466
Gestire le copie Snapshot locali	2492
Replica del volume SnapMirror	2504
Gestire la replica del volume SnapMirror	2524
Gestire la replica di SnapMirror SVM	2566
Gestire la replica del volume root di SnapMirror	2599
Dettagli tecnici di SnapMirror	2603
Archiviazione e conformità con la tecnologia SnapLock	2611
Gruppi di coerenza	2655
Continuità aziendale di SnapMirror	2692
Servizio mediatore per MetroCluster e SnapMirror Business Continuity	2726
Gestire i siti MetroCluster con Gestione di sistema	2780
Protezione dei dati mediante backup su nastro	2790
Configurazione NDMP	2886
Replica tra il software NetApp Element e ONTAP	2902
Monitoraggio di eventi, performance e stato	2923
Monitorare le performance del cluster con System Manager	2923
Monitorare e gestire le performance del cluster utilizzando la CLI	2933
Monitorare le performance del cluster con Unified Manager	2971
Monitorare le performance del cluster con Cloud Insights	2971
Registrazione dell'audit	2973
AutoSupport	2978
Monitoraggio dello stato di salute	3007
Analisi del file system	3020
Configurazione EMS	3035
Riferimento al comando ONTAP	3052
Riferimenti ai comandi per le versioni supportate di ONTAP	3052
Riferimenti ai comandi per le versioni a supporto limitato di ONTAP (solo PDF)	3052
Tool di confronto CLI	3052
Note legali	3053
Copyright	3053
Marchi	3053
Brevetti	3053
Direttiva sulla privacy	3053
Open source	3053



# Documentazione di ONTAP 9

# Note di rilascio

## Highlight sulla release ONTAP 9

Ogni versione del software per la gestione dei dati ONTAP 9 offre funzioni nuove e migliorate che migliorano le funzionalità, la gestibilità, le prestazioni e la sicurezza di ONTAP.

Oltre a questi punti salienti, è possibile trovare una copertura completa per versione di tutte le nuove funzioni avanzate introdotte nelle recenti release di ONTAP.

Per informazioni dettagliate sul supporto di piattaforme hardware e switch, problemi noti e limitazioni in tutte le versioni di ONTAP 9 o per le funzioni introdotte nelle versioni precedenti a ONTAP 9.9.1, fare riferimento a ["Note sulla versione di ONTAP 9"](#). Per accedere alle Note di rilascio, è necessario accedere con l'account NetApp o creare un account.

Per eseguire l'aggiornamento all'ultima versione di ONTAP, vedere [Effettuare l'aggiornamento alla versione più recente di ONTAP](#) e [Quando è necessario aggiornare ONTAP?](#)

### Highlight di ONTAP 9.14.1

ONTAP 9.14.1 offre funzionalità nuove e migliorate nel campo di FabricPool, protezione anti-ransomware, OAuth e altro ancora. Per un elenco completo delle nuove funzioni e dei miglioramenti, vedere [Novità di ONTAP 9.14.1](#).

- [Riduzione prenotazione WAFL](#)

ONTAP 9.14.1 introduce un aumento immediato del 5% dello spazio utilizzabile sui sistemi FAS e Cloud Volumes ONTAP, riducendo la riserva WAFL sugli aggregati con 30 TB o più.

- [Miglioramenti apportati a FabricPool](#)

FabricPool offre un aumento di [performance di lettura](#) e permette la scrittura diretta nel cloud, riducendo il rischio di esaurire lo spazio e i costi storage grazie allo spostamento dei dati cold in un tier storage meno costoso.

- ["Supporto per OAuth 2,0"](#)

ONTAP supporta il framework OAuth 2,0, che può essere configurato tramite Gestione sistema. Con OAuth 2,0, è possibile fornire un accesso sicuro a ONTAP per framework di automazione senza creare o esporre ID utente e password a script di testo normale e runbook.

- ["Miglioramenti alla protezione autonoma dal ransomware \(ARP\)"](#)

ARP garantisce un maggiore controllo sulla protezione degli eventi, consentendo di regolare le condizioni che creano avvisi e riducendo la possibilità di falsi positivi.

- [Prova del disaster recovery di SnapMirror in System Manager](#)

System Manager offre un semplice flusso di lavoro per testare facilmente il disaster recovery in una posizione remota e per ripulirlo dopo il test. Questa funzione consente test più semplici e frequenti e una maggiore fiducia nei recovery time objective.

- [Supporto blocco oggetti S3](#)

ONTAP S3 supporta il comando object-lock API, consentendo di proteggere dalla cancellazione i dati scritti in ONTAP con S3

Utilizzo di comandi API S3 standard e per garantire che i dati importanti siano protetti per il tempo appropriato.

- [Cluster](#) e [volume](#) etichettatura

Aggiungi tag di metadati a volumi e cluster che seguono i dati quando vengono spostati da on-premise al cloud e viceversa.

## Highlight di ONTAP 9.13.1

ONTAP 9.13.1 offre funzionalità nuove e migliorate nel campo della protezione anti-ransomware, dei gruppi di coerenza, della qualità del servizio, della gestione della capacità dei tenant e molto altro ancora. Per un elenco completo delle nuove funzioni e dei miglioramenti, vedere [Novità di ONTAP 9.13.1](#).

- Miglioramenti alla protezione autonoma dal ransomware (ARP):

- [Abilitazione automatica](#)

Con ONTAP 9.13.1, ARP passa automaticamente dalla modalità di formazione alla modalità di produzione dopo aver ricevuto dati di apprendimento sufficienti, eliminando la necessità per un amministratore di abilitarla dopo il periodo di 30 giorni.

- [Supporto per la verifica multi-admin](#)

I comandi di disattivazione ARP sono supportati dalla verifica multi-admin, garantendo che nessun amministratore singolo possa disattivare ARP per esporre i dati a potenziali attacchi ransomware.

- [Supporto FlexGroup](#)

ARP supporta i gruppi flessibili che iniziano con ONTAP 9.13.1. ARP può monitorare e proteggere FlexGroup che coprono più volumi e nodi nel cluster, consentendo anche di proteggere con ARP anche i set di dati più grandi.

- [Monitoring delle performance e della capacità per i gruppi di coerenza in System Manager](#)

Il monitoraggio della capacità e delle performance fornisce dettagli per ogni gruppo di coerenza, consentendoti di identificare e segnalare rapidamente potenziali problemi a livello di applicazione piuttosto che a livello di oggetto dati.

- [Gestione della capacità del tenant](#)

I clienti multi-tenant e i service provider possono impostare un limite di capacità su ciascuna SVM, consentendo ai tenant di eseguire il provisioning self-service senza il rischio di un consumo eccessivo di capacità nel cluster da parte di un tenant.

- [Qualità del servizio soffitti e pavimenti](#)

ONTAP 9.13.1 consente di raggruppare oggetti come volumi, LUN o file in gruppi e di assegnare un livello massimo di qualità del servizio (IOPS massimi) o minimo (IOPS minimi), migliorando le aspettative di performance delle applicazioni.

## Highlight di ONTAP 9.12.1

ONTAP 9.12.1 offre funzioni nuove e migliorate per quanto riguarda protezione avanzata, conservazione, prestazioni e altro ancora. Per un elenco completo delle nuove funzioni e dei miglioramenti, vedere [Novità di ONTAP 9.12.1](#).

- [Snapshot a prova di manomissione](#)

Con la tecnologia SnapLock, le copie Snapshot possono essere protette dalla cancellazione sull'origine o sulla destinazione.

Mantenere più punti di recovery proteggendo le snapshot sullo storage primario e secondario dalle eliminazioni da parte di hacker o amministratori fuori controllo.

- [Miglioramenti alla protezione autonoma dal ransomware \(ARP\)](#)

Abilita immediatamente la protezione autonoma intelligente dal ransomware sullo storage secondario, in base al modello di screening già completato per lo storage primario.

Dopo un failover, identifica istantaneamente i potenziali attacchi ransomware sullo storage secondario. Una Snapshot viene acquisita immediatamente dei dati che iniziano a essere interessati e gli amministratori vengono avvertiti, aiutando a fermare un attacco e a migliorare il recovery.

- [FPolicy](#)

Attivazione con un clic di ONTAP FPolicy per abilitare il blocco automatico dei file dannosi conosciuti. L'attivazione semplificata aiuta a proteggersi dai tipici attacchi ransomware che utilizzano estensioni di file comuni e note.

- [Protezione avanzata: Registrazione della conservazione a prova di manomissione](#)

L'accesso alla conservazione a prova di manomissione in ONTAP che garantisce la compromissione degli account amministratore non può nascondere azioni dannose. La cronologia degli amministratori e degli utenti non può essere alterata o eliminata senza che il sistema ne sia a conoscenza.

Registrare e controllare tutte le azioni amministrative indipendentemente dall'origine, garantendo l'acquisizione di tutte le azioni che hanno un impatto sui dati. Un avviso viene generato ogni volta che i registri di controllo del sistema vengono manomessi in qualsiasi modo per informare gli amministratori della modifica.

- [Protezione avanzata: Autenticazione a più fattori estesa](#)

L'autenticazione a più fattori (MFA) per CLI (SSH) supporta dispositivi token hardware fisici Yubikey, garantendo che un utente malintenzionato non possa accedere al sistema ONTAP utilizzando credenziali rubate o un sistema client compromesso. Cisco DUO è supportato per MFA con System Manager.

- [Dualismo degli oggetti file \(accesso multiprotocollo\)](#)

Il dualismo degli oggetti file abilita l'accesso in lettura e scrittura nativo al protocollo S3 nella stessa origine dati che già dispone di accesso al protocollo NAS. Puoi accedere contemporaneamente allo storage come file o come oggetti dalla stessa origine dei dati, eliminando la necessità di disporre di copie duplicate dei dati da utilizzare con protocolli diversi (S3 o NAS), come per le analytics che utilizzano i dati degli oggetti.

- [Ribilanciamento FlexGroup](#)

Se i componenti di FlexGroup non sono bilanciati, è possibile ribilanciare e gestire FlexGroup senza

interruzioni da

CLI, API REST e System Manager. Per ottenere prestazioni ottimali, i membri costituenti di un FlexGroup devono avere la capacità utilizzata distribuita in modo uniforme.

- Miglioramenti della capacità di storage

La prenotazione dello spazio WAFL è stata notevolmente ridotta, fornendo fino a 400 TiB di capacità utilizzabile per aggregato.

## Highlight di ONTAP 9.11.1

ONTAP 9.11.1 offre funzioni nuove e migliorate nel campo della sicurezza, della conservazione, delle prestazioni e altro ancora. Per un elenco completo delle nuove funzioni e dei miglioramenti, vedere [Novità di ONTAP 9.11.1](#).

- [Verifica multi-admin](#)

La verifica con amministratori multipli (MAV) è un approccio nativo alla verifica, che richiede approvazioni multiple per attività amministrative sensibili come l'eliminazione di una snapshot o di un volume. Le approvazioni richieste in un'implementazione MAV impediscono attacchi dannosi e modifiche accidentali ai dati.

- [Miglioramenti alla protezione autonoma da ransomware](#)

La protezione autonoma dal ransomware (ARP) utilizza l'apprendimento automatico per rilevare le minacce ransomware con una maggiore granularità, consentendoti di identificare rapidamente le minacce e accelerare il recovery in caso di violazione.

- [Conformità SnapLock per FlexGroup Volumes](#)

Set di dati multi-petabyte sicuri per workload come electronic design automation e media & entertainment proteggendo i dati con blocco di file WORM in modo da non essere modificati o eliminati.

- [Eliminazione asincrona delle directory](#)

Con ONTAP 9.11.1, l'eliminazione dei file avviene in background nel sistema ONTAP, consentendo di eliminare facilmente directory di grandi dimensioni eliminando al contempo gli impatti di performance e latenza sull'i/o dell'host

- [Miglioramenti di S3](#)

Semplificare ed espandere le funzionalità di gestione dei dati a oggetti di S3 con ONTAP con endpoint API aggiuntivi e versione oggetto a livello di bucket, consentendo di memorizzare versioni multiple di un oggetto nello stesso bucket.

- Miglioramenti di System Manager

System Manager supporta funzionalità avanzate per ottimizzare le risorse storage e migliorare la gestione degli audit. Questi update includono funzionalità migliorate per gestire e configurare gli aggregati di storage, maggiore visibilità delle analisi del sistema e visualizzazione hardware per i sistemi FAS.

## Highlight di ONTAP 9.10.1

ONTAP 9.10.1 offre funzionalità nuove e migliorate nel campo del rafforzamento della sicurezza, dell'analisi

delle performance, del supporto del protocollo NVMe e delle opzioni di backup dello storage a oggetti. Per un elenco completo delle nuove funzioni e dei miglioramenti, vedere [Novità di ONTAP 9.10.1](#).

- [Protezione ransomware autonoma](#)

La protezione autonoma contro il ransomware crea automaticamente una copia Snapshot del tuo volume e avvisa gli amministratori quando vengono rilevate attività anomale, permettendoti di rilevare rapidamente attacchi ransomware e ripristinare più rapidamente.

- [Miglioramenti di System Manager](#)

System Manager scarica automaticamente gli aggiornamenti del firmware per dischi, shelf, service processor e offre nuove integrazioni con NetApp Active IQ Digital Advisor, BlueXP e la gestione del certificato. Questi miglioramenti semplificano l'amministrazione e mantengono la business continuity.

- [Miglioramenti alle file-System Analytics](#)

File System Analytics offre ulteriore telemetria per identificare i principali file, directory e utenti nella vostra condivisione di file, permettendoti di identificare i problemi di performance del carico di lavoro per migliorare la pianificazione delle risorse e l'implementazione della QoS.

- [Supporto NVMe over TCP \(NVMe/TCP\) per sistemi AFF](#)

Ottieni performance elevate e riduci il TCO per la tua SAN aziendale e i carichi di lavoro moderni sul sistema AFF utilizzando NVMe/TCP sulla rete Ethernet esistente.

- [Supporto NVMe over Fibre Channel \(NVMe/FC\) per i sistemi NetApp FAS](#)

Utilizza il protocollo NVMe/FC sui tuoi array ibridi per consentire una migrazione uniforme su NVMe.

- [Backup cloud ibrido nativo per lo storage a oggetti](#)

Proteggi i tuoi dati di ONTAP S3 in relazione alla tua scelta di destinazioni di storage a oggetti. Utilizza la replica SnapMirror per eseguire il backup su storage on-premise con StorageGRID, nel cloud con Amazon S3 o in un altro bucket ONTAP S3 su sistemi NetApp AFF e FAS.

- [Blocco globale dei file con FlexCache](#)

Garantire la coerenza dei file nelle posizioni della cache durante gli aggiornamenti dei file di origine con il blocco globale dei file utilizzando FlexCache. Questo miglioramento abilita blocchi esclusivi di lettura file in una relazione da origine a cache per i carichi di lavoro che richiedono un blocco avanzato.

## Highlight di ONTAP 9.9.1

ONTAP 9.9.1 offre funzionalità nuove e migliorate nel campo dell'efficienza dello storage, dell'autenticazione multifattore, del disaster recovery e molto altro ancora. Per un elenco completo delle nuove funzioni e dei miglioramenti, vedere [Novità di ONTAP 9.9.1](#).

- [Maggiore sicurezza per la gestione dell'accesso remoto CLI](#)

Il supporto per l'hashing di password SHA512 e SSH A512 protegge le credenziali dell'account amministratore da malintenzionati che stanno tentando di ottenere l'accesso al sistema.

- ["Miglioramenti di MetroCluster IP: Supporto per cluster a 8 nodi"](#)

Il nuovo limite è il doppio rispetto al precedente, offrendo supporto per le configurazioni MetroCluster e abilitando la disponibilità continua dei dati.

- [Miglioramenti alla continuità del business di SnapMirror](#)

Offre più opzioni di replica per backup e disaster recovery per container di dati di grandi dimensioni per workload NAS.

- [Migliori performance SAN](#)

Offre performance SAN fino a quattro volte superiori per le singole applicazioni LUN come i datastore VMware, in modo da poter raggiungere performance elevate nell'ambiente SAN.

- [Nuova opzione di storage a oggetti per il cloud ibrido](#)

Consente l'utilizzo di StorageGRID come destinazione per NetApp Cloud Backup Service per semplificare e automatizzare il backup dei dati ONTAP on-premise.

#### Passi successivi

- [Effettuare l'aggiornamento alla versione più recente di ONTAP](#)
- [Quando è necessario aggiornare ONTAP?](#)

## Supporto per la release ONTAP 9

A partire dalla release ONTAP 9,8, NetApp rilascia le release di ONTAP due volte all'anno. Anche se i piani sono soggetti a modifiche, l'intento è quello di rilasciare nuove release ONTAP nel secondo e quarto trimestre di ogni anno solare. Utilizzate queste informazioni per pianificare il periodo di tempo necessario per l'aggiornamento e usufruire della versione più recente di ONTAP.

Versione	Data di rilascio
9.14.1	Gennaio 2024
9.13.1	Giugno 2023
9.12.1	Febbraio 2023
9.11.1	Luglio 2022
9.10.1	Gennaio 2022
9.9.1	Giugno 2021

## Livelli di supporto

Il livello di supporto disponibile per una specifica versione di ONTAP varia a seconda della data di rilascio del software.

Livello di supporto	Supporto completo			Supporto limitato		Supporto self-service		
Anno	1	2	3	4	5	6	7	8
Accesso alla documentazione online	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Supporto tecnico	Sì	Sì	Sì	Sì	Sì			
Analisi delle cause alla radice	Sì	Sì	Sì	Sì	Sì			
Download di software	Sì	Sì	Sì	Sì	Sì			
Aggiornamenti di servizio (release di patch [release P])	Sì	Sì	Sì					
Avvisi sulle vulnerabilità	Sì	Sì	Sì					

Per eseguire l'aggiornamento all'ultima versione di ONTAP, vedere [Effettuare l'aggiornamento alla versione più recente di ONTAP](#) e [Quando è necessario aggiornare ONTAP?](#)

## Novità di ONTAP 9.14.1

Scopri le nuove funzionalità disponibili in ONTAP 9.14.1.

Per informazioni dettagliate sulle versioni precedenti di ONTAP 9, sul supporto per piattaforme hardware e switch, sui problemi noti e sulle limitazioni, fare riferimento a ["Note sulla versione di ONTAP 9"](#). Per accedere alle *Note sulla versione di ONTAP 9*, è necessario accedere con il proprio account NetApp o creare un account NetApp.

Per eseguire l'aggiornamento alla versione più recente di ONTAP, vedere [Prepararsi all'aggiornamento di ONTAP](#).

### Protezione dei dati

Aggiornare	Descrizione
<a href="#">NVE supportata su volumi root SVM</a>	È possibile crittografare i volumi root delle SVM utilizzando chiavi univoche con crittografia dei volumi di NetApp.



Aggiornare	Descrizione
<a href="#">Capacità di impostare il blocco delle copie Snapshot su copie Snapshot di conservazione a lungo termine e. Per reinizializzare il Compliance Clock</a>	Nei cluster con licenza SnapLock, è possibile impostare il blocco delle copie Snapshot a prova di manomissione per le copie Snapshot con conservazione a lungo termine per le copie Snapshot create su volumi di destinazione SnapMirror non SnapLock e il Compliance Clock può essere inizializzato in assenza di volumi SnapLock.
<a href="#">SnapMirror Business Continuity (SM-BC) supporta prenotazioni persistenti SCSI3 e Windows failover Clustering</a>	SCSI3 prenotazioni persistenti e Window failover Clustering per SM-BC supporta più nodi che accedono a un dispositivo bloccando al contempo l'accesso ad altri nodi, garantendo che il clustering per diversi ambienti applicativi rimanga costante e stabile.
<a href="#">Copia di Snapshot granulari dei volumi con gruppi di coerenza</a>	Puoi utilizzare i gruppi di coerenza per replicare le Snapshot SnapMirror asincrone e gli Snapshot granulari del volume nei gruppi di coerenza di destinazione, per un livello extra di disaster recovery.
<a href="#">Supporto di data Protection asincrona per gruppi di coerenza all'interno della relazione di disaster recovery delle SVM</a>	Se contiene un gruppo di coerenza, le SVM configurate per il disaster recovery delle SVM possono replicare le informazioni del gruppo di coerenza nel sito secondario.
<a href="#">"Supporto asincrono SnapMirror per destinazioni fanout 20"</a>	Il numero di destinazioni fanout asincrone SnapMirror supportate su sistemi A700 e superiori aumenta da 16 a 20 quando si utilizza ONTAP 9.14.1.
<a href="#">Supporto CLI per gruppi di coerenza</a>	Gestire i gruppi di coerenza utilizzando l'interfaccia CLI di ONTAP.

## Protocolli di accesso ai file

Aggiornare	Descrizione
<a href="#">Trunking sessione NFSv4,1</a>	Il trunking della sessione consente di utilizzare più percorsi per un datastore esportato. In questo modo è possibile semplificare la gestione e migliorare le performance con la verticale dei carichi di lavoro. È particolarmente appropriato in ambienti con carichi di lavoro VMware.

## MetroCluster

Aggiornare	Descrizione
<a href="#">Supporto dello storage a oggetti S3 su aggregati con mirroring e senza mirror</a>	Abilitazione di un server di storage a oggetti S3 su una SVM in un aggregato con mirroring o senza mirror nelle configurazioni MetroCluster IP e FC.
<a href="#">Supporto per il provisioning di un bucket S3 su aggregati con mirroring e senza mirror in un cluster MetroCluster</a>	È possibile creare un bucket su un aggregato con mirroring o senza mirror nelle configurazioni di MetroCluster.

Per ulteriori informazioni sui miglioramenti della configurazione di piattaforme e switch per le configurazioni MetroCluster, vedere ["Note sulla versione di ONTAP 9"](#).

## Storage a oggetti S3

Aggiornare	Descrizione
Il ridimensionamento automatico è stato abilitato sui volumi FlexGroup da S3 GB per eliminare l'allocazione di capacità eccessiva quando vengono creati dei bucket su di essi	Quando vengono creati o eliminati bucket da volumi FlexGroup nuovi o esistenti, i volumi vengono ridimensionati a una dimensione minima richiesta. La dimensione minima richiesta è la dimensione totale di tutti i bucket S3 in un volume FlexGroup.
Supporto dello storage a oggetti S3 su aggregati con mirroring e senza mirror	È possibile abilitare un server per lo storage a oggetti S3 su una SVM in un aggregato con mirroring o senza mirror nelle configurazioni IP e FC di MetroCluster.
Blocco degli oggetti in base ai ruoli degli utenti e al periodo di conservazione dei blocchi	È possibile bloccare la sovrascrittura o l'eliminazione degli oggetti nei bucket S3. La possibilità di bloccare gli oggetti si basa su utenti o tempo specifici.
Configurazione dell'accesso per i gruppi di utenti LDAP per supportare i servizi di directory esterni e aggiunta del periodo di validità per l'accesso e le chiavi segrete	<p>Gli amministratori di ONTAP possono configurare l'accesso per LDAP (Lightweight Directory Access Protocol) o gruppi di utenti Active Directory allo storage a oggetti ONTAP S3, con la possibilità di abilitare l'autenticazione in modalità di associazione rapida LDAP. Gli utenti di gruppi locali o di dominio o di gruppi LDAP possono generare i propri accessi e chiavi segrete per i client S3.</p> <p>È possibile definire un periodo di validità per le chiavi di accesso e le chiavi segrete di S3 utenti.</p> <p>ONTAP fornisce il supporto per variabili come <code>\$aws:username</code> per policy bucket e policy di gruppo.</p>

## SAN

Aggiornare	Descrizione
Rilevamento automatico dell'host NVMe/TCP	Per impostazione predefinita, il rilevamento degli host dei controller che utilizzano il protocollo NVMe/TCP è automatizzato.
Reporting e troubleshooting sul lato host NVMe/FC	Per impostazione predefinita, ONTAP supporta la capacità degli host NVMe/FC di identificare le macchine virtuali tramite un identificatore univoco e per gli host NVMe/FC di monitorare l'utilizzo delle risorse della macchina virtuale. Questo migliora il reporting e il troubleshooting sul lato host.
Assegnazione di priorità agli host NVMe	È possibile configurare il sottosistema NVMe in modo da assegnare priorità all'allocazione delle risorse per host specifici. A un host assegnato ad una priorità alta vengono assegnati conteggi di code i/o maggiori e profondità di coda maggiori.

## Sicurezza

Aggiornare	Descrizione
Supporto per l'autenticazione a più fattori Cisco DUO per gli utenti SSH	Gli utenti SSH possono eseguire l'autenticazione utilizzando Cisco DUO come secondo fattore di autenticazione durante l'accesso.

Aggiornare	Descrizione
"Miglioramenti al supporto di OAuth 2,0"	ONTAP 9.14.1 estende l'autenticazione basata sul token principale e il supporto OAuth 2,0 fornito inizialmente con ONTAP 9.14.0. L'autorizzazione può essere configurata utilizzando Active Directory o LDAP con mappatura da gruppo a ruolo. I token di accesso con vincoli di mittente sono inoltre supportati e protetti in base a mTLS (Mutual TLS). Oltre a Auth0 e Keycloak, Microsoft Windows Active Directory Federation Service (ADFS) è supportato come Identity Provider (IdP).
"Framework di autorizzazione OAuth 2,0"	Viene aggiunto il framework OAuth 2,0 (Open Authorization) che fornisce autenticazione basata su token per i client API REST ONTAP. In questo modo è possibile una gestione e un'amministrazione più sicure dei cluster ONTAP utilizzando workflow di automazione basati su script di API REST o Ansible. Sono supportate le funzionalità standard di OAuth 2,0, tra cui emittente, pubblico, convalida locale, introspezione remota, attestazione dell'utente remoto e supporto proxy. L'autorizzazione client può essere configurata utilizzando gli ambiti OAuth 2,0 autonomi o mappando gli utenti ONTAP locali. I provider di identità supportati (IdP) includono Auth0 e Keycloak che utilizzano più server simultanei.
Avvisi sintonizzabili per la protezione autonoma da ransomware	Configura la protezione autonoma dal ransomware per ricevere notifiche ogni volta che viene rilevata una nuova estensione di file o quando viene creata una snapshot ARP, ricevendo un avviso precedente a possibili eventi ransomware.
FPolicy supporta gli archivi persistenti per ridurre la latenza	FPolicy consente di configurare un archivio persistente per acquisire eventi di accesso ai file per policy asincrone non obbligatorie nella SVM. Gli archivi persistenti possono aiutare a separare l'elaborazione i/o dei client dall'elaborazione delle notifiche FPolicy per ridurre la latenza dei client. Le configurazioni obbligatorie sincrone e asincrone non sono supportate.
FPolicy supporta volumi FlexCache su SMB	FPolicy è supportato per volumi FlexCache con NFS o SMB. In precedenza, FPolicy non era supportato per i volumi FlexCache con SMB.

## Efficienza dello storage

Aggiornare	Descrizione
Tracciamento della scansione in file System Analytics	Tenere traccia della scansione di inizializzazione di file System Analytics con informazioni in tempo reale sull'avanzamento e la limitazione.
Aumento dello spazio degli aggregati utilizzabile sulle piattaforme FAS	Per le piattaforme FAS, la riserva WAFL per gli aggregati di dimensioni superiori a 30TB KB viene ridotta dal 10% al 5%, aumentando lo spazio utilizzabile nell'aggregato.
Modifica nel reporting dello spazio fisico utilizzato nei volumi TSSE	Nei volumi con l'efficienza dello storage sensibile alla temperatura (TSSE) abilitata, la metrica della CLI ONTAP per il reporting della quantità di spazio utilizzata nel volume include i risparmi di spazio realizzati come risultato di TSSE. Questa metrica si riflette nei comandi <code>volume show -physical-used</code> e <code>volume show-space -physical used</code> . Per FabricPool, il valore di <code>-physical-used</code> è una combinazione del tier di capacità e del tier di performance. Per i comandi specifici, vedere <code>volume show</code> e <code>volume show space</code> .

## Miglioramenti alla gestione delle risorse dello storage

Aggiornare	Descrizione
<a href="#">Ribilanciamento proattivo della FlexGroup</a>	FlexGroup Volumes offre il supporto per lo spostamento automatico di file in crescita in una directory in un componente remoto per ridurre i colli di bottiglia di i/o nei componenti locali.
<a href="#">Etichettatura delle copie Snapshot nei volumi FlexGroup</a>	È possibile aggiungere, modificare ed eliminare tag ed etichette (commenti) in per identificare le copie Snapshot e prevenire l'eliminazione accidentale di copie Snapshot nei volumi FlexGroup.
<a href="#">Scrivi direttamente nel cloud con FabricPool</a>	FabricPool aggiunge la capacità di scrivere dati in un volume in FabricPool in modo che venga trasferito direttamente nel cloud senza attendere la scansione del tiering.
<a href="#">Lettura aggressiva con FabricPool</a>	FabricPool fornisce una lettura aggressiva dei file, come i flussi dei film su FabricPool Volumes, per garantire che non vengano eliminati i frame.

## Miglioramenti alla gestione delle SVM

Aggiornare	Descrizione
<a href="#">La mobilità dei dati delle SVM supporta la migrazione di SVM che contengono quote e qtree di utenti e gruppi</a>	La mobilità dei dati di SVM, aggiunge il supporto per la migrazione di SVM che contengono quote e qtree di utenti e gruppi.
<a href="#">Supporto di un massimo di 400 volumi per SVM, un massimo di 12 coppie ha e pNFS con NFS 4,1 tramite mobilità dei dati delle SVM</a>	Il numero massimo di volumi supportati per SVM con mobilità dei dati delle SVM aumenta fino a 400 volte, mentre il numero di coppie ha supportate aumenta fino a 12.

## System Manager

Aggiornare	Descrizione
<a href="#">Supporto del failover di test SnapMirror</a>	Puoi utilizzare System Manager per eseguire le prove di failover di test di SnapMirror senza interrompere le relazioni di SnapMirror esistenti.
<a href="#">Gestione delle porte in un dominio di broadcast</a>	È possibile utilizzare System Manager per modificare o eliminare le porte assegnate a un dominio di broadcast.
<a href="#">Abilitazione di MAUSO (Automatic Unplanned Switchover) assistito da Mediator</a>	È possibile utilizzare Gestione di sistema per attivare o disattivare lo switchover non pianificato automatico assistito da Mediator (MAUSO) quando si esegue uno switchover e uno switchback di IP MetroCluster.
<a href="#">Cluster e. volume etichettatura</a>	Puoi utilizzare System Manager per usare i tag per categorizzare cluster e volumi in modi diversi, ad esempio per scopo, proprietario o ambiente. Ciò è utile quando ci sono molti oggetti dello stesso tipo. Gli utenti possono identificare rapidamente un oggetto specifico in base ai tag assegnati.
<a href="#">Supporto migliorato per il monitoring dei gruppi di coerenza</a>	System Manager visualizza i dati cronologici relativi all'utilizzo del gruppo di coerenza.

Aggiornare	Descrizione
<a href="#">Autenticazione NVMe in-band</a>	Puoi utilizzare System Manager per configurare l'autenticazione sicura, unidirezionale e bidirezionale tra un host e un controller NVMe sui protocolli NVMe/TCP e NVMe/FC utilizzando il protocollo di autenticazione DH-HMAC-CHAP.
<a href="#">Supporto per la gestione del ciclo di vita dei bucket S3 esteso a System Manager</a>	È possibile utilizzare System Manager per definire regole per l'eliminazione di oggetti specifici in un bucket e, attraverso queste regole, scadono tali oggetti bucket.

## Novità di ONTAP 9.13.1

Scopri le nuove funzionalità disponibili in ONTAP 9.13.1.

Per informazioni dettagliate sulle versioni precedenti di ONTAP 9, sul supporto per piattaforme hardware e switch, sui problemi noti e sulle limitazioni, fare riferimento a ["Note sulla versione di ONTAP 9"](#). Per accedere alle *Note sulla versione di ONTAP 9*, è necessario accedere con il proprio account NetApp o creare un account NetApp.

Per aggiornare ONTAP, vedere [Prepararsi all'aggiornamento di ONTAP](#).

### Protezione dei dati

Aggiornare	Descrizione
<a href="#">"Verifica multi-admin"</a>	L'amministratore del cluster può attivare esplicitamente la verifica con amministratori multipli su un cluster per richiedere l'approvazione del quorum prima dell'esecuzione di alcune operazioni SnapLock.
<a href="#">"Supporto avanzato per la gestione di gruppi di coerenza, incluso lo spostamento dei volumi e la geometria"</a>	È possibile spostare i volumi tra gruppi di coerenza, modificare la geometria dei gruppi di coerenza gerarchici e ottenere informazioni sulla capacità in gruppi di coerenza. System Manager supporta la creazione di un gruppo di coerenza con nuovi volumi NAS o namespace NVME.
<a href="#">"Ripristino NDMP con SnapMirror Synchronous"</a>	Il ripristino NDMP è supportato con SnapMirror sincrono.
Miglioramenti a SnapMirror Business Continuity (SM-BC)	<ul style="list-style-type: none"> <li>• <a href="#">"Aggiunta senza interruzioni di volumi a un gruppo di coerenza con una relazione SM-BC attiva."</a></li> <li>• <a href="#">"Utilizzare il ripristino NDMP con SM-BC"</a>.</li> </ul>
<a href="#">xref:./release-notes/"Supporto di SnapMirror asincrono con un singolo gruppo di coerenza"</a>	I gruppi di coerenza supportano le configurazioni SnapMirror asincrone, consentendo il vaulting di backup SnapMirror per singoli gruppi di coerenza.

### Protocolli di accesso ai file

Aggiornare	Descrizione
"NFSv4.x supporto storepool"	Pochi clienti consumano troppe risorse NFSv4.x storepool che portano ad altri client NFSv4.x che vengono bloccati a causa della non disponibilità delle risorse NFSv4.xstorepool. È possibile avere la possibilità di abilitare il rifiuto e il blocco dei client che consumano molte risorse di NFSv4.x storepool nei loro ambienti.

## MetroCluster

Aggiornare	Descrizione
"Transizione da MetroCluster FC a MetroCluster IP usando uno switch condiviso per lo storage collegato MetroCluster IP e Ethernet"	È possibile passare senza interruzioni da una configurazione MetroCluster FC a una configurazione MetroCluster IP (ONTAP 9,8 e versioni successive) utilizzando uno switch condiviso.
"Transizioni senza interruzioni da una configurazione MetroCluster FC a otto nodi a una configurazione MetroCluster IP"	Puoi trasferire senza interruzioni i carichi di lavoro e i dati da una configurazione FC MetroCluster a otto nodi esistente a una nuova configurazione IP MetroCluster.
"Aggiornamenti della configurazione IP MetroCluster a quattro nodi mediante switchover e switchback"	Upgrade dei controller in una configurazione MetroCluster IP a quattro nodi attraverso switchover e switchback con <code>system controller replace</code> comandi.
"Lo switchover non pianificato automatico assistito dal mediatore (MAUSO) viene attivato per uno spegnimento ambientale"	Se un sito si arresta senza problemi a causa di un arresto ambientale, viene attivato MAUSO.
"Supporto delle configurazioni MetroCluster IP a otto nodi"	È possibile aggiornare i controller e lo storage in una configurazione IP MetroCluster a otto nodi espandendo la configurazione fino a diventare una configurazione temporanea a dodici nodi, quindi rimuovere i vecchi gruppi di disaster recovery.
"Conversione della configurazione IP di MetroCluster in una configurazione di switch MetroCluster di storage condiviso"	È possibile convertire una configurazione IP di MetroCluster in una configurazione di switch MetroCluster di storage condiviso.

Per ulteriori informazioni sui miglioramenti della configurazione di piattaforme e switch per le configurazioni MetroCluster, vedere ["Note sulla versione di ONTAP 9"](#).

## Networking

Aggiornare	Descrizione
<a href="#">Supporto hardware esteso per cluster Interconnect RDMA</a>	ONTAP supporta i sistemi AFF A900, ASA A900 e FAS9500 per l'interconnessione in cluster RDMA con una scheda di rete del cluster X91153A per ridurre la latenza, ridurre i tempi di failover e accelerare la comunicazione tra i nodi.
Aumento dei limiti di LIF dei dati	ONTAP offre una maggiore flessibilità aumentando i limiti di scalabilità LIF dei dati per coppie ha e cluster.
Supporto IPv6 ore su 24, 7 giorni su 7 durante il setup del cluster sulle piattaforme A800 e FAS8700	Sulle piattaforme A800 e FAS8700, puoi utilizzare l'interfaccia a riga di comando di ONTAP per creare e configurare nuovi cluster in ambienti di rete solo IPv6.

## Storage a oggetti S3

Aggiornare	Descrizione
<a href="#">S3 Gestione del ciclo di vita della benna</a>	S3 le azioni di scadenza degli oggetti definiscono quando gli oggetti in un bucket scadono. Questa funzionalità consente di gestire le versioni degli oggetti in modo da soddisfare i requisiti di conservazione e gestire in modo efficace lo storage a oggetti S3 complessivo.

## SAN

Aggiornare	Descrizione
<a href="#">Supporto per NVMe/FC su host AIX</a>	ONTAP supporta il protocollo NVMe/FC sugli host AIX. Vedere <a href="#">"Tool di interoperabilità NetApp"</a> per le configurazioni supportate.

## Sicurezza

Funzione	Descrizione
<a href="#">Protezione ransomware autonoma</a>	<ul style="list-style-type: none"> <li>• <a href="#">Verifica della funzionalità degli amministratori multipli con la protezione autonoma dal ransomware</a></li> <li>• <a href="#">Passaggio automatico dall'apprendimento alla modalità attiva</a></li> <li>• <a href="#">Supporto FlexGroup</a>, Inclusi analytics e reporting per volumi e operazioni FlexGroup che comprendono l'espansione di un volume FlexGroup, conversioni da FlexVol a FlexGroup, ribilanciamento delle FlexGroup.</li> </ul>
<a href="#">Autenticazione a chiave pubblica SSH con Active Directory</a>	È possibile utilizzare una chiave pubblica SSH come metodo di autenticazione principale con un utente Active Directory (ad) oppure una chiave pubblica SSH come metodo di autenticazione secondario dopo un utente ad.
X,509 certificati con chiavi pubbliche SSH	ONTAP consente di associare un certificato X,509 alla chiave pubblica SSH per un account, fornendo maggiore sicurezza per la scadenza del certificato e i controlli di revoca al momento dell'accesso SSH.



Funzione	Descrizione
<a href="#">Notifica di errore di accesso al file FPolicy</a>	FPolicy supporta le notifiche per gli eventi di accesso negato. Le notifiche vengono generate per l'operazione del file non riuscita a causa della mancanza di autorizzazione, che include: Errore dovuto a autorizzazioni NTFS, errore dovuto a bit della modalità Unix e errore dovuto a NFSv4 ACL.
<a href="#">Autenticazione multifattore con TOTP (password monouso basate sul tempo)</a>	Configurare gli account utente locali con l'autenticazione a più fattori utilizzando una password monouso (TOTP) basata sull'ora. Il TOTP viene sempre utilizzato come secondo metodo di autenticazione. È possibile utilizzare una chiave pubblica SSH o una password utente come metodo di autenticazione principale.

## Efficienza dello storage

Aggiornare	Descrizione
Modifica nel reporting del rapporto di riduzione dei dati primari in System Manager	Il rapporto di riduzione dei dati primario visualizzato in System Manager non include più il risparmio dello spazio delle copie Snapshot nel calcolo. Rappresenta solo il rapporto tra lo spazio logico utilizzato e lo spazio fisico utilizzato. Nelle precedenti release di ONTAP, il rapporto di riduzione dei dati primario includeva benefici significativi per la riduzione dello spazio delle copie Snapshot. Di conseguenza, quando si esegue l'aggiornamento a ONTAP 9.13.1, si noterà un rapporto primario significativamente inferiore. È comunque possibile visualizzare i rapporti di riduzione dei dati con le copie Snapshot nella vista dettagli <b>capacità</b> .
<a href="#">Efficienza di conservazione sensibile alla temperatura</a>	L'efficienza dello storage sensibile alla temperatura aggiunge il packaging sequenziale di blocchi fisici contigui per migliorare l'efficienza dello storage. Quando i sistemi vengono aggiornati a ONTAP 9.13.1, il packing sequenziale dei volumi abilitati all'efficienza dello storage sensibile alla temperatura sarà automaticamente abilitato.
Applicazione dello spazio logico	L'applicazione dello spazio logico è supportata sulle destinazioni SnapMirror.
<a href="#">Supporto limitato della capacità delle VM di storage</a>	È possibile impostare limiti di capacità su una Storage VM (SVM) e abilitare avvisi quando la SVM si avvicina a una soglia percentuale.

## Miglioramenti alla gestione delle risorse dello storage

Aggiornare	Descrizione
Aumento del numero massimo di inodi	ONTAP continuerà ad aggiungere automaticamente gli inode (alla velocità di 1 inode per 32 KB di spazio di volume) anche se il volume cresce di oltre 680 GB. ONTAP continuerà ad aggiungere inodes fino a raggiungere il massimo di 2.147.483.632.
<a href="#">Supporto per la specifica di un tipo di SnapLock durante la creazione di FlexClone</a>	Puoi specificare uno dei tre tipi di SnapLock, compliance, Enterprise o non SnapLock, quando si crea un FlexClone di un volume di lettura/scrittura.
<a href="#">Attiva le analitiche del file system per impostazione predefinita</a>	Impostare l'opzione file System Analytics in modo che sia attivata per impostazione predefinita sui nuovi volumi.



Aggiornare	Descrizione
<a href="#">Disaster recovery delle SVM: Relazioni di fan-out con FlexGroup Volumes</a>	Viene rimossa la restrizione fanout del DR SVM con volumi FlexGroup. Il DR SVM con FlexGroup include il supporto per relazioni di fan-out SnapMirror in otto siti.
<a href="#">Operazione di ribilanciamento della singola FlexGroup</a>	È possibile pianificare una singola operazione di ribilanciamento FlexGroup per iniziare alla data e all'ora future specificate dall'utente.
<a href="#">Performance di lettura di FabricPool</a>	FabricPool offre performance di lettura sequenziale migliorate per i workload a singolo e multi-stream per il throughput di tiering e dati residenti nel cloud. Questo miglioramento può inviare una maggiore velocità di GET e put all'archivio di oggetti back-end. Se disponi di archivi di oggetti on-premise, dovresti considerare l'aumento delle performance nel servizio dell'archivio di oggetti e determinare se potrebbe essere necessario ridurre i punti FabricPool.
<a href="#">Modelli di policy QoS adattivi</a>	I modelli di policy adattivi di qualità del servizio ti consentono di impostare limiti minimi di throughput a livello di SVM.

## Miglioramenti alla gestione delle SVM

Aggiornare	Descrizione
<a href="#">Mobilità dei dati SVM</a>	Aumenta il supporto della migrazione di SVM contenenti fino a 200 volumi.
Supporto per la ricreazione delle directory SVM	Il nuovo comando CLI <code>debug vserver refresh-vserver-dir -node node_name</code> ricrea le directory e i file mancanti. Per ulteriori informazioni e per la sintassi dei comandi, vedere <a href="#">"La Guida comandi ONTAP"</a> .

## System Manager

A partire da ONTAP 9.12.1, System Manager è integrato con BlueXP. Scopri di più [Integrazione di System Manager con BlueXP](#).

Aggiornare	Descrizione
Modifica nel reporting del rapporto di riduzione dei dati primari	Il rapporto di riduzione dei dati primario visualizzato in System Manager non include più il risparmio dello spazio delle copie Snapshot nel calcolo. Rappresenta solo il rapporto tra lo spazio logico utilizzato e lo spazio fisico utilizzato. Nelle precedenti release di ONTAP, il rapporto di riduzione dei dati primario includeva benefici significativi per la riduzione dello spazio delle copie Snapshot. Di conseguenza, quando si esegue l'aggiornamento a ONTAP 9.13.1, si noterà un rapporto primario significativamente inferiore. I rapporti di riduzione dei dati con le copie Snapshot continuano a essere visualizzati nella vista dei dettagli sulla capacità.
<a href="#">Blocco delle copie Snapshot a prova di manomissione</a>	Puoi utilizzare System Manager per bloccare una copia Snapshot su un volume non SnapLock e fornire protezione contro gli attacchi ransomware.
<a href="#">Supporto per manager esterni delle chiavi</a>	Puoi utilizzare System Manager per gestire gestori di chiavi esterne per archiviare e gestire le chiavi di autenticazione e crittografia.

Aggiornare	Descrizione
<a href="#">Risoluzione dei problemi hardware</a>	<p>Gli utenti di System Manager possono visualizzare rappresentazioni visive delle piattaforme hardware aggiuntive nella pagina "hardware", comprese le piattaforme ASA e AFF C-Series.</p> <p>Il supporto per le piattaforme AFF C-Series è incluso anche nelle ultime versioni di patch di ONTAP 9.12.1, ONTAP 9.11.1 e ONTAP 9.10.1.</p> <p>Le visualizzazioni consentono di identificare problemi o problemi relativi alle piattaforme, fornendo agli utenti un metodo rapido per la risoluzione dei problemi hardware.</p>

## Novità di ONTAP 9.12.1

Scopri le nuove funzionalità disponibili in ONTAP 9.12.1.

Per informazioni dettagliate sulle versioni precedenti di ONTAP 9, sul supporto per piattaforme hardware e switch, sui problemi noti e sulle limitazioni, fare riferimento a ["Note sulla versione di ONTAP 9"](#). Per accedere alle *Note sulla versione di ONTAP 9*, è necessario accedere con il proprio account NetApp o creare un account NetApp.

Per aggiornare ONTAP, vedere [Prepararsi all'aggiornamento di ONTAP](#).

### Protezione dei dati

Aggiornare	Descrizione
<a href="#">Supporto di volumi FlexVol più grandi con SnapMirror Synchronous</a>	Le dimensioni massime del volume FlexVol supportate nelle configurazioni SnapMirror Synchronous sono aumentate da 100 TB a 300 TB. Entrambi i cluster di origine e di destinazione devono eseguire <i>ONTAP 9.12.1P2 o versioni successive</i> .
<a href="#">Supporto di dimensioni di file e LUN di dimensioni maggiori in SnapMirror Synchronous</a>	Le dimensioni massime di file e LUN supportate nelle configurazioni SnapMirror Synchronous sono aumentate da 16 TB a 128 TB. I cluster di origine e di destinazione devono eseguire ONTAP 9.12.1 P2 o versioni successive.
<a href="#">Supporto migliorato per i gruppi di coerenza</a>	<ul style="list-style-type: none"> <li>• È possibile aggiungere e rimuovere volumi da un gruppo di coerenza e clonare un gruppo di coerenza (anche da una copia Snapshot).</li> <li>• I gruppi di coerenza supportano il tagging delle applicazioni per ottimizzare i processi di gestione e protezione dei dati.</li> <li>• L'API REST ONTAP supporta la configurazione di gruppi di coerenza con volumi NFS/SMB o namespace NVMe.</li> </ul>
<a href="#">NDO sincroni di SnapMirror</a>	SnapMirror Synchronous supporta le operazioni senza interruzioni (NDO) di ha takeover e giveback, spostamento dei volumi e altre operazioni correlate alla manutenzione. Questa funzione è disponibile solo sulle piattaforme AFF/ASA.
<a href="#">ONTAP Mediator 1,5 supporta la business continuity di SnapMirror</a>	ONTAP Mediator 1,5 è disponibile per il monitoring delle relazioni di SnapMirror Business Continuity (SM-BC).

Aggiornare	Descrizione
Miglioramenti alla continuità del business (SM-BC) di SnapMirror	SM-BC supporta il ripristino parziale del LUN da Snapshot. Inoltre, SM-BC estende la QoS ai volumi non nella relazione SM-BC.
Indicatore di ricostruzione del data warehouse per SnapMirror asincrono	SnapMirror Asynchronous fornisce un indicatore che mostra il tempo impiegato dalla ricostruzione di un data warehouse dopo una prova di disaster recovery, visualizzando la percentuale di completamento.
Opzione SnapLock per impostare il tempo di conservazione minimo "non specificato" assoluto	SnapLock include un'opzione per impostare un tempo di conservazione minimo quando il tempo di conservazione assoluto è impostato su "non specificato".
Copie Snapshot a prova di manomissione	Puoi bloccare una copia Snapshot su un volume non SnapLock per fornire protezione dagli attacchi ransomware. Il blocco delle copie Snapshot consente di evitare che vengano eliminate accidentalmente o in modo pericoloso.

## Protocolli di accesso ai file

Aggiornare	Descrizione
Disattivare i tipi di crittografia deboli per la comunicazione Kerberos	Una nuova opzione di protezione SMB consente di disattivare RC4 e DES a favore dei tipi di crittografia AES (Advanced Encryption Standard) per la comunicazione basata su Kerberos con il KDC Active Directory (ad).
Accesso client S3 ai dati NAS	I client S3 possono accedere agli stessi dati NAS dei client NFS e SMB senza riformattare, rendendo più semplice servire le applicazioni S3 che richiedono dati a oggetti.
Attributi estesi NFS	I server NFS abilitati per NFSv4,2 possono memorizzare e recuperare gli attributi estesi NFS (xattrs) dai client compatibili con xattr.
NFSv4,2 file sparse e supporto per la prenotazione dello spazio	Il client NFSv4,2 è in grado di riservare spazio per un file sparso. Lo spazio può anche essere deallocato e non prenotato da un file.

## MetroCluster

Aggiornare	Descrizione
ONTAP Mediator 1,5 è supportato in una configurazione MetroCluster IP	ONTAP Mediator 1,5 è disponibile per il monitoraggio delle configurazioni IP di MetroCluster.
Il supporto IPsec per il protocollo host front-end (ad esempio NFS e iSCSI) è disponibile nelle configurazioni MetroCluster IP e MetroCluster fabric-attached.	Il supporto IPsec per il protocollo host front-end (ad esempio NFS e iSCSI) è disponibile nelle configurazioni MetroCluster IP e MetroCluster fabric-attached.
"Funzione di switchover forzato automatico di MetroCluster in una configurazione IP di MetroCluster"	È possibile attivare la funzione di switchover forzato automatico di MetroCluster in una configurazione IP di MetroCluster. Questa funzione è un'estensione della funzione MAUSO (Mediator-Assisted Unplanned Switchover).

Aggiornare	Descrizione
"S3 su una SVM su un aggregato senza mirror in una configurazione IP di MetroCluster"	È possibile attivare la funzione di switchover forzato automatico di MetroCluster in una configurazione IP di MetroCluster. Questa funzione è un'estensione della funzione MAUSO (Mediator-Assisted Unplanned Switchover).

Per ulteriori informazioni sui miglioramenti della configurazione di piattaforme e switch per le configurazioni MetroCluster, vedere ["Note sulla versione di ONTAP 9"](#).

## Networking

Aggiornare	Descrizione
Servizi LIF	È possibile utilizzare <code>management-log-forwarding</code> Servizio per controllare le LIF che vengono utilizzate per inoltrare i registri di audit a un server syslog remoto

## Storage a oggetti S3

Aggiornare	Descrizione
Supporto esteso per S3 azioni	Sono supportate le seguenti azioni API Amazon S3: <ul style="list-style-type: none"> <li>• CopyObject</li> <li>• UploadPartCopy</li> <li>• BucketPolicy (GET, PUT, DELETE)</li> </ul>

## SAN

Aggiornare	Descrizione
Aumento delle dimensioni massime di LUN per le piattaforme AFF e FAS	A partire da ONTAP 9.12.1P2, le dimensioni massime supportate dei LUN sulle piattaforme AFF e FAS sono aumentate da 16 TB a 128 TB.
"Limiti NVMe aumentati"	Il protocollo NVMe supporta quanto segue: <ul style="list-style-type: none"> <li>• 8K sottosistemi in una singola macchina virtuale di storage e un singolo cluster</li> <li>• Cluster a 12 nodi NVMe/FC supporta 256 controller per porta, mentre NVMe/TCP supporta 2K controller per nodo.</li> </ul>
Supporto NVMe/TCP per l'autenticazione sicura	L'autenticazione sicura, unidirezionale e bidirezionale tra host e controller NVMe è supportata su NVMe/TCP utilizzando il protocollo di autenticazione DHMAC-CHAP.
Supporto IP MetroCluster per NVMe	Il protocollo NVMe/FC è supportato sulle configurazioni IP MetroCluster a 4 nodi.

## Sicurezza


Nell'ottobre 2022, NetApp ha implementato le modifiche per rifiutare le trasmissioni di messaggi AutoSupport non inviate da HTTPS con TLSv1,2 o SMTP protetto. Per ulteriori informazioni, vedere ["SU484: NetApp rifiuterà i messaggi AutoSupport trasmessi con una sicurezza di trasporto insufficiente"](#).

Funzione	Descrizione
<a href="#">Miglioramenti dell'interoperabilità della protezione autonoma dal ransomware</a>	La protezione autonoma dal ransomware è disponibile per queste configurazioni: <ul style="list-style-type: none"><li>• Volumi protetti con SnapMirror</li><li>• SVM protette con SnapMirror</li><li>• SVM abilitati per la migrazione (mobilità dei dati SVM)</li></ul>
<a href="#">Supporto Multifactor Authentication (MFA) per SSH con FIDO2 e PIV (entrambi utilizzati da Yubikey)</a>	SSH MFA può utilizzare lo scambio di chiavi pubbliche/private assistito da hardware con nome utente e password. Yubikey è un dispositivo token fisico collegato al client SSH per aumentare la sicurezza MFA.
<a href="#">Registrazione a prova di manomissione</a>	Per impostazione predefinita, tutti i log interni di ONTAP sono antimanomissione, garantendo che gli account amministratore compromessi non possano nascondere azioni dannose.
<a href="#">Trasporto TLS per eventi</a>	Gli eventi EMS possono essere inviati a un server syslog remoto utilizzando il protocollo TLS, migliorando in questo modo la protezione via cavo per il logging di audit esterno centrale.

## Efficienza dello storage

Aggiornare	Descrizione
<a href="#">Efficienza di conservazione sensibile alla temperatura</a>	L'efficienza dello storage sensibile alla temperatura è abilitata per impostazione predefinita sulle nuove piattaforme e volumi AFF C250, AFF C400, AFF C800. TSSE non è abilitato per impostazione predefinita sui volumi esistenti ma può essere abilitato manualmente utilizzando la CLI di ONTAP.
<a href="#">Aumento dello spazio utilizzabile dell'aggregato</a>	Per le piattaforme All Flash FAS (AFF) e FAS500f, la WAFL Reserve per gli aggregati superiori a 30TB TB viene ridotta dal 10% al 5%, con conseguente maggiore spazio utilizzabile nell'aggregato.
<a href="#">File System Analytics: Directory principali in base alla dimensione</a>	File System Analytics ora identifica le directory di un volume che consumano la maggior parte dello spazio.

## Miglioramenti alla gestione delle risorse dello storage

Aggiornare	Descrizione
Ribilanciamento FlexGroup	<p>Puoi abilitare il ribilanciamento automatico del volume FlexGroup senza interruzioni per ridistribuire i file tra componenti FlexGroup.</p> <div>  <p>Si consiglia di non utilizzare il ribilanciamento automatico di FlexGroup dopo una conversione da FlexVol a FlexGroup. È invece possibile utilizzare la funzione di spostamento dei file retroattivo e disagregativo disponibile in ONTAP 9.10.1 e versioni successive, immettendo il <code>volume rebalance file-move</code> comando. Per ulteriori informazioni e per la sintassi dei comandi, vedere <a href="#">"La Guida comandi ONTAP"</a>.</p> </div>
Supporto di SnapLock per SnapVault per FlexGroup Volumes	Supporto di SnapLock per SnapVault per FlexGroup Volumes

## Miglioramenti alla gestione delle SVM

Aggiornare	Descrizione
Miglioramenti alla mobilità dei dati delle SVM	<p>Gli amministratori del cluster possono spostare senza interruzioni una SVM da un cluster di origine a un cluster di destinazione utilizzando piattaforme FAS e AFF su aggregati ibridi.</p> <p>Sono stati aggiunti il supporto sia per il protocollo SMB con interruzioni che per la protezione autonoma dal ransomware.</p>

## System Manager

A partire da ONTAP 9.12.1, System Manager è integrato con BlueXP. Grazie a BlueXP, gli amministratori possono gestire l'infrastruttura di multicloud ibrido da un singolo pannello di controllo e conservare la familiare dashboard di System Manager. Quando effettui l'accesso a System Manager, gli amministratori hanno la possibilità di accedere all'interfaccia di System Manager in BlueXP o direttamente a System Manager. Scopri di più [Integrazione di System Manager con BlueXP](#).

Aggiornare	Descrizione
Supporto di System Manager per SnapLock	Le operazioni SnapLock, tra cui l'inizializzazione del clock di conformità, la creazione di volumi SnapLock e il mirroring del file WORM sono supportate in System Manager.
Visualizzazione hardware del cablaggio	Gli utenti di System Manager possono visualizzare informazioni sulla connettività relative al cablaggio tra i dispositivi hardware nel cluster per risolvere i problemi di connettività.
Supporto dell'autenticazione a più fattori con Cisco DUO durante l'accesso a System Manager	È possibile configurare Cisco DUO come provider di identità SAML (IdP), consentendo agli utenti di eseguire l'autenticazione utilizzando Cisco DUO quando accedono a System Manager.
Miglioramenti del networking di System Manager	System Manager offre un maggiore controllo sulla selezione della subnet e della porta home durante la creazione dell'interfaccia di rete. System Manager supporta anche la configurazione di connessioni NFS su RDMA.

Aggiornare	Descrizione
<a href="#">Temi di visualizzazione del sistema</a>	Gli utenti di System Manager possono selezionare un tema chiaro o scuro per la visualizzazione dell'interfaccia di System Manager. Possono anche scegliere di impostare il tema predefinito utilizzato per il sistema operativo o il browser. Questa funzionalità consente agli utenti di specificare un'impostazione più comoda per la lettura del display.
<a href="#">Miglioramenti ai dettagli sulla capacità dei Tier locali</a>	Gli utenti di System Manager possono visualizzare i dettagli relativi alla capacità di specifici livelli locali per determinare se lo spazio è sottoposto a overcommit, il che potrebbe indicare la necessità di aggiungere più capacità per garantire che il livello locale non esaurisca lo spazio disponibile.
<a href="#">Ricerca migliorata</a>	System Manager dispone di una funzionalità di ricerca migliorata che consente agli utenti di cercare e accedere a informazioni di supporto pertinenti e sensibili al contesto e a un documento di prodotto di System Manager dal sito di supporto NetApp direttamente attraverso l'interfaccia di System Manager. Ciò consente agli utenti di acquisire le informazioni necessarie per intraprendere le azioni appropriate senza dover cercare in varie posizioni sul sito di supporto.
<a href="#">Miglioramenti al provisioning di volumi</a>	Gli amministratori dello storage possono scegliere una policy di copia Snapshot durante la creazione di un volume con System Manager anziché utilizzare la policy predefinita.
<a href="#">Aumentare le dimensioni di un volume</a>	Gli amministratori dello storage possono vedere l'impatto sullo spazio dati e sulla riserva di copie Snapshot quando utilizzano System Manager per ridimensionare un volume.
<a href="#">Pool di storage e. Flash Pool gestione</a>	Gli amministratori dello storage possono utilizzare System Manager per aggiungere SSD a un pool di storage SSD, creare Tier locali Flash Pool (aggregato) con le unità di allocazione dei pool di storage SSD e creare Tier locali Flash Pool utilizzando SSD fisici.
<a href="#">Supporto NFS su RDMA in System Manager</a>	System Manager supporta le configurazioni delle interfacce di rete per NFS su RDMA e identifica le porte compatibili con RoCE.

## Novità di ONTAP 9.11.1


Scopri le nuove funzionalità disponibili in ONTAP 9.11.1.

Per informazioni dettagliate sulle versioni precedenti di ONTAP 9, sul supporto per piattaforme hardware e switch, sui problemi noti e sulle limitazioni, fare riferimento a ["Note sulla versione di ONTAP 9"](#). Per accedere alle *Note sulla versione di ONTAP 9*, è necessario accedere con il proprio account NetApp o creare un account NetApp.

Per eseguire l'aggiornamento alla versione più recente di ONTAP, vedere [Prepararsi all'aggiornamento di ONTAP](#).

## Protezione dei dati



Aggiornare	Descrizione
Server chiavi esterne in cluster	Il supporto dei server per la gestione delle chiavi esterne in cluster viene aggiunto per i partner NetApp che forniscono una soluzione server KMIP in cluster. In questo modo è possibile aggiungere server KMIP primari e secondari, impedendo la duplicazione dei dati delle chiavi di crittografia. Per i partner supportati, consultare la <a href="#">"Tool di matrice di interoperabilità"</a> .
Policy asincrona di SnapMirror in System Manager	<p>È possibile utilizzare System Manager per aggiungere criteri di mirroring e vault predefiniti e personalizzati, visualizzare criteri legacy e sovrascrivere le pianificazioni di trasferimento definite in un criterio di protezione quando si proteggono volumi e VM di storage. Puoi anche utilizzare System Manager per modificare le relazioni di protezione delle macchine virtuali per lo storage e il volume.</p> <div>  <p>Se si esegue ONTAP 9.8P12 o una versione successiva della patch di ONTAP 9,8, configurare SnapMirror utilizzando System Manager e pianificare l'aggiornamento a ONTAP 9.9.1 o ONTAP 9.10.1, utilizzare ONTAP 9,9.1P13 o versioni successive e ONTAP 9.10.1P10 o versioni successive della patch per l'aggiornamento.</p> </div>
Ripristino di una singola directory SnapMirror Cloud	Consente agli amministratori del cluster a livello di privilegi amministrativi di eseguire un'operazione di ripristino di una singola directory da un endpoint cloud. È necessario fornire l'UUID dell'endpoint di origine per identificare l'endpoint di backup da cui si sta eseguendo il ripristino. Perché più backup possono utilizzare lo stesso <code>cloud_endpoint_name</code> Come destinazione, deve essere fornito l'UUID associato al backup per il comando di ripristino. È possibile utilizzare <code>snapmirror show command</code> per ottenere <code>source_endpoint_uuid</code> .
Supporto avanzato per SnapMirror Business Continuity (SM-BC)	<ul style="list-style-type: none"> <li>• SM-BC supporta AIX come host</li> <li>• SM-BC supporta SnapRestore a file singolo, consentendo il ripristino di una LUN singola o di un file normale in una configurazione SM-BC.</li> </ul>
Risincronizzazione rapida della replica dei dati delle SVM	La risincronizzazione rapida della replica dei dati delle SVM offre agli amministratori dello storage la possibilità di bypassare la ricostruzione di un intero data warehouse e di eseguire il ripristino più rapidamente dopo una prova di disaster recovery.
Supporto della replica dei dati delle SVM con MetroCluster	L'origine SVM-DR è supportata su entrambi i lati di una configurazione MetroCluster.
Creazione di copie Snapshot di un gruppo di coerenza in due fasi	Nell'API REST, i gruppi di coerenza supportano una procedura Snapshot in due fasi, che consente di eseguire un controllo preliminare prima di salvare la Snapshot.

## Protocolli di accesso ai file

Aggiornare	Descrizione
Supporto TLSv1,3	ONTAP supporta TLS 1,3 per HTTPS e protocolli di gestione API REST. TLS 1,3 non è supportato con SP/BMC o con crittografia di peering cluster.



Aggiornare	Descrizione
<a href="#">Supporto bind veloce LDAP</a>	Se supportato dal server LDAP, è possibile utilizzare l'associazione rapida LDAP per autenticare gli utenti amministrativi ONTAP in modo rapido e semplice.

## MetroCluster

Aggiornare	Descrizione
<a href="#">Supporto ONTAP Mediator 1,4</a>	Il software ONTAP Mediator versione 1,4 è supportato nelle configurazioni MetroCluster IP.
<a href="#">Supporto del gruppo di coerenza</a>	I gruppi di coerenza sono supportati nelle configurazioni MetroCluster.
<a href="#">"Transizione da una configurazione FC MetroCluster a una configurazione IP MetroCluster AFF A250 o FAS500f"</a>	È possibile passare da una configurazione FC MetroCluster a una configurazione IP AFF A250 o FAS500f MetroCluster.

Per ulteriori informazioni sui miglioramenti della configurazione di piattaforme e switch per le configurazioni MetroCluster, vedere ["Note sulla versione di ONTAP 9"](#).

## Networking

Aggiornare	Descrizione
<a href="#">LLDP (link Layer Discovery Protocol)</a>	La rete del cluster supporta LLDP per consentire a ONTAP di funzionare con switch del cluster che non supportano il protocollo di rilevamento Cisco (CDP).
<a href="#">Servizi LIF</a>	I nuovi servizi LIF lato client offrono un maggiore controllo sulle LIF utilizzate per le richieste ad, DNS, LDAP e NIS in uscita.

## Storage a oggetti S3

Aggiornare	Descrizione
<a href="#">Supporto aggiuntivo per le azioni oggetto S3</a>	Le seguenti azioni sono supportate dalle API ONTAP: CreateBucket, DeleteBucket, DeleteObjects. Inoltre, ONTAP S3 supporta la versione oggetto e le azioni associate con PutBucketVersioning, GetBucketVersioning, ListBucketVersions.

## SAN

Aggiornare	Descrizione
<a href="#">Failover LIF iSCSI</a>	La nuova funzione di failover LIF iSCSI supporta la migrazione automatica e manuale delle LIF iSCSI in un failover di partner SFO e in un failover locale. Il failover LIF iSCSI è disponibile su tutte le piattaforme SAN Array (ASA).

Aggiornare	Descrizione
Migrazione non distruttiva da LUN a namespace NVMe e da namespace NVMe a LUN	Utilizzare l'interfaccia CLI di ONTAP per convertire sul posto un <a href="#">LUN esistente su un namespace NVMe</a> o un <a href="#">Namespace NVMe esistente in una LUN</a> .

## Sicurezza

Aggiornare	Descrizione
<a href="#">Miglioramenti alla protezione autonoma dal ransomware (ARP)</a>	L'algoritmo di rilevamento ARP è stato migliorato per rilevare ulteriori minacce malware. Inoltre, viene utilizzata una nuova chiave di licenza per attivare la protezione autonoma da ransomware. Per gli aggiornamenti dei sistemi ONTAP da ONTAP 9.10.1, la chiave di licenza precedente offre comunque la stessa funzionalità.
<a href="#">Verifica multi-admin</a>	Quando la verifica con amministratori multipli è abilitata, determinate operazioni, come l'eliminazione di volumi o copie Snapshot, possono essere eseguite solo dopo le approvazioni da parte di amministratori designati. In questo modo si evita che gli amministratori compromessi, dannosi o inesperti apportino modifiche indesiderate o eliminino dati.

## Efficienza dello storage

Aggiornare	Descrizione
<a href="#">Visualizzare i risparmi dell'ingombro fisico</a>	Quando su un volume è attivata l'efficienza dello storage sensibile alla temperatura, è possibile utilizzare il comando volume show-footprint per visualizzare i risparmi in termini di impatto fisico.
<a href="#">Supporto SnapLock per FlexGroup Volumes</a>	SnapLock include il supporto per i dati archiviati su FlexGroup Volumes. Il supporto per i volumi FlexGroup è disponibile con le modalità SnapLock Compliance e SnapLock Enterprise.
<a href="#">Mobilità dei dati SVM</a>	Aumenta a tre il numero di array AFF supportati e aggiunge il supporto per relazioni SnapMirror quando l'origine e la destinazione eseguono ONTAP 9.11.1 o versioni successive. È stata introdotta anche la gestione esterna delle chiavi (KMIP), disponibile per le installazioni cloud e on-premise.

## Miglioramenti alla gestione delle risorse dello storage


Aggiornare	Descrizione
<a href="#">Tracciamento dell'attività a livello di SVM in file System Analytics</a>	Il tracciamento delle attività viene aggregato a livello della SVM, monitorando gli IOPS in lettura/scrittura e i throughput per fornire informazioni istantanee e fruibili sui dati.
<a href="#">Abilitare gli aggiornamenti dei tempi di accesso al file</a>	Quando questa opzione è attivata, il tempo di accesso viene aggiornato sul volume di origine FlexCache solo se l'età del tempo di accesso corrente è superiore alla durata specificata dall'utente.


Aggiornare	Descrizione
<a href="#">Eliminazione asincrona delle directory</a>	L'eliminazione asincrona è disponibile per i client NFS e SMB quando l'amministratore dello storage concede loro diritti sul volume. Quando l'eliminazione asincrona è attivata, i client Linux possono utilizzare il comando mv e i client Windows possono utilizzare il comando Rinomina per eliminare una directory e spostarla in un file nascosto .ontaptrashbin directory.
<a href="#">Supporto SnapLock per FlexGroup Volumes</a>	SnapLock include il supporto per i dati archiviati su FlexGroup Volumes. Il supporto per i volumi FlexGroup è disponibile con le modalità SnapLock Compliance e SnapLock Enterprise. SnapLock non supporta le seguenti operazioni su FlexGroup Volumes: SnapLock per SnapVault, conservazione basata sugli eventi e conservazione a fini giudiziari.

## Miglioramenti alla gestione delle SVM

Aggiornare	Descrizione
<a href="#">Mobilità dei dati SVM</a>	Aumenta a tre il numero di array AFF supportati e aggiunge il supporto per relazioni SnapMirror quando l'origine e la destinazione eseguono ONTAP 9.11.1 o versioni successive. È anche introdotta la gestione esterna delle chiavi (KMIP), disponibile per le installazioni cloud e on-premise.

## System Manager

Aggiornare	Descrizione
<a href="#">Gestire le policy asincrone di SnapMirror</a>	<p>Utilizzare System Manager per aggiungere criteri di mirroring e vault predefiniti e personalizzati, visualizzare criteri legacy e sovrascrivere le pianificazioni di trasferimento definite in un criterio di protezione quando si proteggono volumi e VM di storage. Puoi anche utilizzare System Manager per modificare le relazioni di protezione delle macchine virtuali per lo storage e il volume.</p> <div>  <p>Se si utilizza ONTAP 9.8P12 o una versione successiva della patch per ONTAP 9,8 e si configura SnapMirror utilizzando System Manager e si intende eseguire l'aggiornamento a ONTAP 9.9.1 o ONTAP 9.10.1, si consiglia di utilizzare ONTAP 9,9.1P13 o versioni successive e ONTAP 9.10.1P10 o versioni successive della patch per l'aggiornamento.</p> </div>
<a href="#">Visualizzazione hardware</a>	La funzionalità di visualizzazione hardware in Gestione sistema supporta tutte le piattaforme AFF e FAS correnti.
<a href="#">Informazioni sull'analisi dei sistemi</a>	Nella pagina Insights, System Manager ti aiuta a ottimizzare il sistema visualizzando ulteriori informazioni sulla capacità e sulla sicurezza e nuovi approfondimenti sulla configurazione dei cluster e delle macchine virtuali storage.

Aggiornare	Descrizione
Miglioramenti dell'usabilità	<ul style="list-style-type: none"> <li>• <a href="#">I volumi appena creati non sono condivisibili per impostazione predefinita</a>. Gli utenti possono invece specificare le autorizzazioni di accesso predefinite, ad esempio l'esportazione tramite NFS o la condivisione tramite SMB/CIFS e il livello di autorizzazione.</li> <li>• <a href="#">Semplificazione SAN</a> - Quando si aggiunge o si modifica un gruppo iniziatore, gli utenti di System Manager possono visualizzare lo stato di connessione degli iniziatori nel gruppo e assicurarsi che gli iniziatori connessi siano inclusi nel gruppo in modo da poter accedere ai dati LUN.</li> </ul>
<a href="#">Operazioni avanzate sui Tier locali (aggregati)</a>	<p>Gli amministratori di System Manager possono specificare la configurazione di un livello locale se non desiderano accettare il suggerimento da System Manager. Inoltre, gli amministratori possono modificare la configurazione RAID di un livello locale esistente.</p> <div>  <p>Se si utilizza ONTAP 9.8P12 o una versione successiva della patch per ONTAP 9,8 e si configura SnapMirror utilizzando System Manager e si intende eseguire l'aggiornamento a ONTAP 9.9.1 o ONTAP 9.10.1, si consiglia di utilizzare ONTAP 9,9.1P13 o versioni successive e ONTAP 9.10.1P10 o versioni successive della patch per l'aggiornamento.</p> </div>
<a href="#">Gestire i registri di controllo</a>	Puoi utilizzare System Manager per visualizzare e gestire i log di audit di ONTAP.

## Novità di ONTAP 9.10.1

Scopri le nuove funzionalità disponibili in ONTAP 9.10.1.

Per informazioni dettagliate sulle versioni precedenti di ONTAP 9, sul supporto per piattaforme hardware e switch, sui problemi noti e sulle limitazioni, fare riferimento a ["Note sulla versione di ONTAP 9"](#). Per accedere alle *Note sulla versione di ONTAP 9*, è necessario accedere con il proprio account NetApp o creare un account NetApp.

Per aggiornare ONTAP, vedere [Prepararsi all'aggiornamento di ONTAP](#).

### Protezione dei dati

Aggiornare	Descrizione
<a href="#">Impostare il periodo di conservazione SnapLock fino a 100 anni</a>	Nelle versioni precedenti a ONTAP 9.10.1, il tempo di conservazione massimo supportato è il 19 gennaio 2071. A partire da ONTAP 9.10.1, SnapLock Enterprise e Compliance supportano un tempo di conservazione fino al 26 ottobre 3058 e un periodo di conservazione fino a 100 anni. Le policy precedenti vengono convertite automaticamente all'estensione delle date di conservazione.
<a href="#">Possibilità di creare volumi SnapLock e non SnapLock nello stesso aggregato</a>	A partire da ONTAP 9.10.1, volumi SnapLock e non possono esistere sullo stesso aggregato, pertanto non è più necessario creare un aggregato SnapLock separato per i volumi SnapLock.

Aggiornare	Descrizione
<a href="#">Gruppi di coerenza</a>	Organizzare volumi e LUN in gruppi di coerenza per gestire le policy di data Protection e garantire la fedeltà di ordine di scrittura dei carichi di lavoro su più volumi di storage.
<a href="#">Archiviare i backup con il cloud pubblico</a>	SnapMirror Cloud supporta il tiering dei backup ONTAP in classi di storage a oggetti su cloud pubblico a costi minori in AWS e MS Azure per la conservazione a lungo termine.
<a href="#">Supporto AES per la comunicazione protetta del canale Netlogon</a>	Se si effettua la connessione ai controller di dominio Windows utilizzando il servizio di autenticazione Netlogon, è possibile utilizzare AES (Advanced Encryption Standard) per le comunicazioni del canale protetto.
<a href="#">Kerberos per l'autenticazione con tunnel di dominio SMB</a>	Oltre a NTLM, l'autenticazione Kerberos è disponibile per le autenticazioni del tunnel di dominio per la gestione di ONTAP. Ciò consente di accedere in modo più sicuro alla CLI di ONTAP e alla GUI di Gestione del sistema utilizzando le credenziali di Active Directory.

## Protocolli di accesso ai file

Aggiornare	Descrizione
<a href="#">NFS su RDMA (solo NVIDIA)</a>	NFS su RDMA utilizza adattatori RDMA, che consentono di copiare i dati direttamente tra la memoria del sistema di storage e la memoria del sistema host, eludendo le interruzioni della CPU e il sovraccarico. NFS su RDMA consente l'utilizzo di NVIDIA GPUDirect Storage per workload con accelerazione GPU su host con GPU NVIDIA supportate.

## MetroCluster

Aggiornare	Descrizione
<a href="#">"Configurazione dell'indirizzo IP MetroCluster di livello 3 nelle configurazioni IP MetroCluster"</a>	In una configurazione di livello 3, è possibile modificare l'indirizzo IP, la netmask e il gateway della MetroCluster.
<a href="#">"Aggiornamento semplificato del controller dei nodi in una configurazione MetroCluster FC"</a>	La procedura di upgrade per il processo di upgrade che utilizza switchover e switchback è stata semplificata.

Per ulteriori informazioni sui miglioramenti della configurazione di piattaforme e switch per le configurazioni MetroCluster, vedere ["Note sulla versione di ONTAP 9"](#).

## Networking

Aggiornare	Descrizione
<a href="#">Interconnessione del cluster RDMA</a>	Con il sistema storage A400 o ASA A400 e una NIC del cluster X1151A puoi accelerare i carichi di lavoro dalle performance elevate in un cluster multi-nodo che sfrutta RDMA per il traffico intra-cluster

Aggiornare	Descrizione
È necessaria una conferma prima di impostare lo stato admin su inattivo per una LIF in una SVM di sistema	In questo modo ti proteggerai da errori LIF fondamentali per il corretto funzionamento del cluster. Se si dispone di script che richiamano questo comportamento all'interfaccia CLI, è necessario aggiornarli per tenere conto del passaggio di conferma.
<a href="#">Suggerimenti per il rilevamento e la riparazione automatici dei problemi di cablaggio di rete</a>	Quando viene rilevato un problema di raggiungibilità della porta, Gestione sistema di ONTAP consiglia un'operazione di riparazione per risolvere il problema.
<a href="#">Certificati IPsec (Internet Protocol Security)</a>	I criteri IPsec supportano le chiavi precondivise (PSK) oltre ai certificati per l'autenticazione.
<a href="#">Politiche di servizio LIF</a>	Le policy del firewall sono obsolete e sostituite con quelle del servizio LIF. È stata aggiunta anche una nuova policy di servizio NTP per fornire un maggiore controllo sulle LIF che vengono utilizzate per le richieste NTP in uscita.

## Storage a oggetti S3

Aggiornare	Descrizione
<a href="#">Protezione di dati a oggetti S3, backup e disaster recovery</a>	S3 SnapMirror offre servizi di protezione dei dati per lo storage a oggetti ONTAP S3, inclusi bucket di mirroring nelle configurazioni ONTAP S3 e backup bucket in destinazioni NetApp e non NetApp.
<a href="#">Verifica S3</a>	Puoi controllare i dati e gli eventi di gestione negli ambienti ONTAP S3. La funzionalità di audit S3 è simile alle funzionalità di auditing NAS esistenti e l'auditing S3 e NAS può coesistere in un cluster.

## SAN

Aggiornare	Descrizione
<a href="#">Namespace NVMe</a>	È possibile utilizzare l'interfaccia CLI di ONTAP per aumentare o diminuire le dimensioni di uno spazio dei nomi. Puoi utilizzare System Manager per aumentare le dimensioni di un namespace.
<a href="#">Supporto del protocollo NVMe per TCP</a>	Il protocollo NVMe (non-volatile Memory Express) è disponibile per gli ambienti SAN su una rete TCP.

## Sicurezza

Aggiornare	Descrizione
<a href="#">Protezione ransomware autonoma</a>	Tramite l'analisi dei workload negli ambienti NAS, la protezione autonoma contro il ransomware ti avvisa in caso di attività anomale che potrebbero indicare un attacco ransomware. Protezione autonoma contro il ransomware crea inoltre backup automatici di Snapshot quando viene rilevato un attacco, oltre alla protezione esistente di copie Snapshot pianificate.
<a href="#">Gestione delle chiavi di crittografia</a>	Utilizza Azure Key Vault e il servizio di gestione delle chiavi di Google Cloud Platform per memorizzare, proteggere e utilizzare le chiavi ONTAP, semplificando la gestione e l'accesso delle chiavi.

## Efficienza dello storage

Aggiornare	Descrizione
<a href="#">Efficienza di conservazione sensibile alla temperatura</a>	Puoi abilitare l'efficienza dello storage sensibile alla temperatura utilizzando la modalità "predefinita" o "efficiente" su volumi AFF nuovi o esistenti.
<a href="#">Possibilità di spostare le SVM senza interruzioni tra i cluster</a>	È possibile spostare le SVM tra cluster fisici AFF, da un'origine a una destinazione, per il bilanciamento del carico, il miglioramento delle performance, gli upgrade delle apparecchiature e le migrazioni del data center.

## Miglioramenti alla gestione delle risorse dello storage

Aggiornare	Descrizione
<a href="#">Monitoraggio delle attività per gli oggetti hot con file System Analytics (FSA)</a>	Per migliorare la valutazione delle prestazioni del sistema, FSA è in grado di identificare gli oggetti hot: File, directory, utenti e client con il maggior numero di traffico e throughput.
<a href="#">Blocco globale della lettura dei file</a>	Abilitare un blocco di lettura da un singolo punto in tutte le cache e nell'origine; articolo interessato nella migrazione.
<a href="#">Supporto NFSv4 per FlexCache</a>	I volumi FlexCache supportano il protocollo NFSv4.
<a href="#">Creazione di cloni da volumi FlexGroup esistenti</a>	Puoi creare un volume FlexClone usando i volumi FlexGroup esistenti.
<a href="#">Converti un volume FlexVol in un FlexGroup in un'origine di disaster recovery della SVM</a>	Puoi convertire FlexVol Volumes in FlexGroup Volumes in un'origine di disaster recovery SVM.

## Miglioramenti alla gestione delle SVM

Aggiornare	Descrizione
<a href="#">Possibilità di spostare le SVM senza interruzioni tra i cluster</a>	È possibile spostare le SVM tra cluster fisici AFF, da un'origine a una destinazione, per il bilanciamento del carico, il miglioramento delle performance, gli upgrade delle apparecchiature e le migrazioni del data center.

## System Manager

Aggiornare	Descrizione
<a href="#">Abilitare il logging della telemetria delle performance nei log di System Manager</a>	Gli amministratori possono abilitare il logging telemetrico in caso di problemi di performance con System Manager, quindi contattare il supporto per analizzare il problema.
<a href="#">File di licenza NetApp</a>	Tutte le chiavi di licenza vengono fornite come file di licenza NetApp invece di chiavi di licenza singole di 28 caratteri, rendendo possibile la licenza di più funzioni utilizzando un unico file.
<a href="#">Aggiornamento automatico del firmware</a>	Gli amministratori di System Manager possono configurare ONTAP in modo che aggiorni automaticamente il firmware.

Aggiornare	Descrizione
Esaminare le raccomandazioni di mitigazione dei rischi e riconoscere i rischi segnalati da Active IQ	Gli utenti di System Manager possono vedere i rischi segnalati da Active IQ e rivedere i consigli sulla loro riduzione. A partire dalla versione 9.10.1, gli utenti possono anche riconoscere i rischi.
Configurare la ricezione da parte dell'amministratore delle notifiche degli eventi EMS	Gli amministratori di System Manager possono configurare il modo in cui le notifiche degli eventi del sistema di gestione degli eventi EMS (Event Management System) vengono inviate in modo che vengano informate dei problemi del sistema che richiedono la loro attenzione.
Gestire i certificati	Gli amministratori di System Manager possono gestire le autorità di certificazione attendibili, i certificati client/server e le autorità di certificazione locali (integrate).
Utilizza System Manager per visualizzare lo storico utilizzo della capacità e per prevedere le future esigenze di capacità	L'integrazione tra Active IQ e System Manager consente agli amministratori di visualizzare i dati sui trend storici nell'utilizzo della capacità per i cluster.
Utilizzare Gestione sistema per eseguire il backup dei dati su StorageGRID utilizzando Cloud Backup Service	In qualità di amministratore Cloud Backup Service, puoi effettuare il backup su StorageGRID se hai implementato Cloud Manager on-premise. Puoi anche archiviare oggetti utilizzando Cloud Backup Service con AWS o Azure.
Miglioramenti dell'usabilità	<p>A partire da ONTAP 9.10.1, puoi:</p> <ul style="list-style-type: none"> <li>• Assegna policy di QoS ai LUN invece del volume principale (VMware, Linux, Windows)</li> <li>• Modificare il gruppo di criteri QoS LUN</li> <li>• Spostare un LUN</li> <li>• Portare un LUN offline</li> <li>• Eseguire un aggiornamento dell'immagine Rolling ONTAP</li> <li>• Creare un set di porte e associarlo a un igroup</li> <li>• Suggerimenti per il rilevamento e la riparazione automatici dei problemi di cablaggio di rete</li> <li>• Attivare o disattivare l'accesso del client alla directory di copia Snapshot</li> <li>• Calcola lo spazio recuperabile prima di eliminare le copie Snapshot</li> <li>• Accesso alle modifiche sul campo continuamente disponibili nelle condivisioni SMB</li> <li>• Visualizzare le misurazioni della capacità utilizzando unità di visualizzazione più accurate</li> <li>• Gestire utenti e gruppi specifici per host per Windows e Linux</li> <li>• Gestire le impostazioni AutoSupport</li> <li>• Ridimensionare i volumi come azione separata</li> </ul>



# Novità di ONTAP 9.9.1

Ulteriori informazioni sulle nuove funzionalità disponibili in ONTAP 9.9.1.

Per informazioni dettagliate sulle versioni precedenti di ONTAP 9, sul supporto per piattaforme hardware e switch, sui problemi noti e sulle limitazioni, fare riferimento a ["Note sulla versione di ONTAP 9"](#). Per accedere alle *Note sulla versione di ONTAP 9*, è necessario accedere con il proprio account NetApp o creare un account NetApp.

Per eseguire l'aggiornamento alla versione più recente di ONTAP, vedere [Prepararsi all'aggiornamento di ONTAP](#).

## Protezione dei dati

Aggiornare	Descrizione
<a href="#">"Supporto dell'efficienza dello storage su volumi e aggregati SnapLock"</a>	Le funzionalità per l'efficienza dello storage per i volumi SnapLock e gli aggregati sono state estese per includere la compaction dei dati, la deduplica tra volumi, la compressione adattiva e TSSE (efficienza dello storage sensibile alla temperatura), permettendo di ottenere risparmi di spazio maggiori per i dati WORM.
<a href="#">"Supporto per la configurazione di policy Snapshot diverse sull'origine e sulla destinazione del disaster recovery di SVM"</a>	Le configurazioni DR SVM possono utilizzare la Mirror-Vault Policy per configurare diverse policy Snapshot sull'origine e sulla destinazione. Le policy sulla destinazione non vengono sovrascritte da quelle sull'origine.
<a href="#">"Supporto di System Manager per SnapMirror Cloud"</a>	SnapMirror Cloud è ora supportato in System Manager.
<a href="#">SVM abilitate all'audit</a>	È stato aumentato da 50 a 400 il numero massimo di SVM abilitate all'audit supportate in un cluster.
<a href="#">SnapMirror sincrono</a>	Il numero massimo di endpoint sincroni SnapMirror supportati per coppia ha è aumentato da 80 a 160.
<a href="#">Topologia di SnapMirror di FlexGroup</a>	I volumi FlexGroup supportano due o più relazioni fanout; ad esempio A→B, A→C. Come per FlexVol Volumes, il fan-out FlexGroup supporta un massimo di 8 moduli fanout e la cascata fino a due livelli; ad esempio, A→B→C.

## Protocolli di accesso ai file

Aggiornare	Descrizione
<a href="#">"Miglioramenti alla ricerca delle referenze LDAP"</a>	La ricerca di riferimenti LDAP è supportata con firma e sigillatura LDAP, connessioni TLS crittografate e comunicazioni sulla porta LDAPS 636.
<a href="#">"Supporto LDAPS su qualsiasi porta"</a>	LDAPS può essere configurato su qualsiasi porta; la porta 636 rimane l'impostazione predefinita.
<a href="#">"Versioni NFSv4.x attivate per impostazione predefinita"</a>	NFSv4,0, NFSv4,1 e NFSv4,2 sono attivati per impostazione predefinita.

Aggiornare	Descrizione
"Supporto etichettato NFSv4,2"	L'opzione MAC (Mandatory Access Control) con etichetta NFS è supportata quando NFSv4,2 è attivato. Con questa funzionalità, i server NFS ONTAP sono compatibili con MAC, memorizzano e recuperano <code>sec_label</code> attributi inviati dai client.

## MetroCluster

Aggiornare	Descrizione
"Supporto IP per il collegamento condiviso nel livello 3"	Le configurazioni IP di MetroCluster possono essere implementate con connessioni back-end con routing IP (livello 3).
"Supporto per cluster a 8 nodi"	I cluster permanenti a 8 nodi sono supportati nelle configurazioni IP e fabric-attached. Inoltre, le piattaforme AFF ASA supportano le configurazioni IP MCC a 8 nodi.

Per ulteriori informazioni sui miglioramenti della configurazione di piattaforme e switch per le configurazioni MetroCluster, vedere ["Note sulla versione di ONTAP 9"](#).

## Networking

Aggiornare	Descrizione
"Resilienza del cluster"	<ul style="list-style-type: none"> <li>Monitoraggio e prevenzione delle porte per cluster senza switch a due nodi (precedentemente disponibili solo in configurazioni con switch)</li> <li>Failover automatico dei nodi quando un nodo non è in grado di fornire dati attraverso la rete cluster</li> <li>Nuovi strumenti per visualizzare i percorsi cluster in cui si verificano perdite di pacchetti</li> </ul>
"Estensione LIF IP virtuale (VIP)"	<ul style="list-style-type: none"> <li>Il numero di sistema autonomo (ASN) per il protocollo BGP (Border gateway Protocol) supporta un intero non negativo a 4 byte.</li> <li>Il discriminatore a uscite multiple (MED) consente di selezionare le rotte avanzate con il supporto della prioritizzazione dei percorsi. Il FARMACO è un attributo facoltativo nel messaggio di aggiornamento BGP.</li> <li>VIP BGP offre l'automazione del percorso predefinita utilizzando il raggruppamento peer BGP per semplificare la configurazione.</li> </ul>

## Storage a oggetti S3

Aggiornare	Descrizione
"Supporto di tag e metadati S3"	Il server ONTAP S3 offre funzionalità di automazione migliorate per client e applicazioni S3 con supporto per metadati di oggetti definiti dall'utente e tagging di oggetti.

## SAN

Aggiornare	Descrizione
Importazione di LUN esterne (FLI)	È possibile utilizzare l'app SAN LUN Migrate sul sito di supporto NetApp per qualificare un array esterno non elencato nella matrice di interoperabilità FLI.
Accesso al percorso remoto NVMe-of	Se durante il failover si perde l'accesso diretto al percorso, l'i/o remoto consente al sistema di eseguire il failover in un percorso remoto e continuare l'accesso ai dati.
Supporto per cluster a 12 nodi su ASA	I cluster a 12 nodi sono supportati per le configurazioni AFF ASA. I cluster ASA possono includere un mix di vari tipi di sistema ASA.
Protocollo NVMe-of su ASA	Il supporto del protocollo NVMe-of è disponibile anche con un sistema AFF ASA.
	<ul style="list-style-type: none"><li>• È possibile creare un igroup composto da igroup esistenti.</li><li>• È possibile aggiungere una descrizione a un igroup o agli iniziatori host che funge da alias per igroup o iniziatore host.</li><li>• È possibile mappare gli igroup a due o più LUN contemporaneamente.</li></ul>
Miglioramento delle performance di una singola LUN	Le prestazioni di una singola LUN per AFF sono state notevolmente migliorate, il che la rende ideale per la semplificazione delle implementazioni in ambienti virtuali. Ad esempio, A800 può fornire fino al 400% di IOPS di lettura casuale in più.

## Sicurezza

Aggiornare	Descrizione
Supporto dell'autenticazione a più fattori con Cisco DUO durante l'accesso a System Manager	A partire da ONTAP 9.9.1P3, è possibile configurare Cisco DUO come provider di identità SAML (IdP), consentendo agli utenti di eseguire l'autenticazione utilizzando Cisco DUO quando accedono a System Manager.

## Efficienza dello storage

Aggiornare	Descrizione
"Impostare il numero massimo di file per il volume"	Automatizza i valori massimi dei file con il parametro del volume <code>-files -set-maximum</code> , eliminando la necessità di monitorare i limiti dei file.

## Miglioramenti alla gestione delle risorse dello storage

Aggiornare	Descrizione
Miglioramenti alla gestione di file System Analytics (FSA) in System Manager	FSA offre funzionalità aggiuntive di System Manager per la ricerca e il filtraggio e per l'azione sui suggerimenti FSA.

Aggiornare	Descrizione
<a href="#">Supporto per cache di ricerca negativa</a>	Memorizza nella cache un errore "file non trovato" sul volume FlexCache per ridurre il traffico di rete causato dalle chiamate all'origine.
<a href="#">Disaster recovery FlexCache</a>	Consente la migrazione senza interruzioni dei client da una cache all'altra.
<a href="#">Supporto di SnapMirror in cascata e fan-out per volumi FlexGroup</a>	Fornisce supporto per relazioni di SnapMirror a cascata e fan-out per volumi FlexGroup.
<a href="#">Supporto del disaster recovery SVM per FlexGroup Volumes</a>	Il supporto di disaster recovery SVM per i volumi FlexGroup offre ridondanza utilizzando SnapMirror per replicare e sincronizzare la configurazione e i dati di una SVM.
<a href="#">Supporto di reporting e applicazione dello spazio logico per i volumi FlexGroup</a>	È possibile visualizzare e limitare la quantità di spazio logico utilizzata dagli utenti di volumi FlexGroup.
<a href="#">Supporto dell'accesso SMB in qtree</a>	L'accesso SMB è supportato per i qtree in volumi FlexVol e FlexGroup con SMB abilitato.

## System Manager

Aggiornare	Descrizione
<a href="#">System Manager visualizza i rischi segnalati da Active IQ</a>	Utilizza System Manager per il collegamento a NetApp Active IQ, che segnala le opportunità per ridurre i rischi e migliorare le performance e l'efficienza del tuo ambiente di storage.
<a href="#">Assegnare manualmente i livelli locali</a>	Gli utenti di System Manager possono assegnare manualmente un Tier locale durante la creazione e l'aggiunta di volumi e LUN.
<a href="#">Eliminazione rapida della directory</a>	Le directory possono essere eliminate in System Manager con la funzionalità di eliminazione rapida delle directory a bassa latenza.
<a href="#">Genera Playbook Ansible</a>	Gli utenti di System Manager possono generare Playbook Ansible dall'interfaccia utente per alcuni workflow selezionati e possono utilizzarli in un tool di automazione per aggiungere o modificare ripetutamente volumi o LUN.
<a href="#">Visualizzazione hardware</a>	Introdotta per la prima volta in ONTAP 9,8, la funzione di visualizzazione hardware supporta ora tutte le piattaforme AFF.
<a href="#">Integrazione di Active IQ</a>	Gli utenti di System Manager possono vedere i casi di supporto associati al cluster e scaricarli. Inoltre, potranno copiare i dettagli del cluster richiesti per l'invio di nuovi casi di supporto sul sito NetApp Support. Gli utenti di System Manager possono ricevere avvisi da Active IQ per informarli della disponibilità di nuovi aggiornamenti del firmware. Quindi, possono scaricare l'immagine del firmware e caricarla tramite System Manager.
<a href="#">Integrazione di Cloud Manager</a>	Gli utenti di System Manager possono configurare la protezione per il backup dei dati su endpoint di cloud pubblico utilizzando Cloud Backup Service.
<a href="#">Miglioramenti al workflow di provisioning di data Protection</a>	Gli utenti di System Manager possono assegnare manualmente un nome igroup e una destinazione SnapMirror durante la configurazione della data Protection.

Aggiornare	Descrizione
Migliore gestione delle porte di rete	La pagina delle interfacce di rete dispone di funzionalità migliorate per la visualizzazione e la gestione delle interfacce sulle porte home.
Miglioramenti alla gestione del sistema	<ul style="list-style-type: none"> <li>• <a href="#">Supporto per igroup nidificati</a></li> <li>• <a href="#">Mappare più LUN a un igroup in una singola attività e può utilizzare un alias WWPN per il filtraggio durante il processo.</a></li> <li>• <a href="#">Durante la creazione della LIF NVMe-of, non hai più bisogno di selezionare porte identiche su entrambi i controller.</a></li> <li>• <a href="#">Disattivare le porte FC con un pulsante di attivazione/disattivazione per ciascuna porta.</a></li> </ul>
Visualizzazione migliorata in System Manager delle informazioni sulle copie Snapshot	<ul style="list-style-type: none"> <li>• Gli utenti di System Manager possono vedere le dimensioni delle copie Snapshot e l'etichetta SnapMirror.</li> <li>• Le riserve di copie Snapshot sono impostate su zero se le copie Snapshot sono disattivate.</li> </ul>
Visualizzazione migliorata in System Manager delle informazioni sulla capacità e sulla posizione dei Tier di storage	<ul style="list-style-type: none"> <li>• <a href="#">Una nuova colonna <b>livelli</b> identifica i livelli locali (aggregati) in cui risiede ciascun volume.</a></li> <li>• <a href="#">System Manager mostra la capacità fisica e la capacità logica utilizzate a livello del cluster e anche a livello del Tier locale (aggregato).</a></li> <li>• <a href="#">I nuovi campi di visualizzazione della capacità consentono di monitorare la capacità, tenendo traccia dei volumi che si stanno avvicinando alla capacità o che sono sottoutilizzati.</a></li> </ul>
Visualizzazione in System Manager degli avvisi di emergenza EMS e di altri errori e avvisi	Il numero di avvisi EMS ricevuti in 24 ore, così come altri errori e avvisi, vengono visualizzati nella scheda integrità di System Manager.

# Integrazione di System Manager con BlueXP

A partire da ONTAP 9.12.1, System Manager è completamente integrato con BlueXP. Con BlueXP, puoi gestire la tua infrastruttura multicloud ibrida da un singolo piano di controllo mantenendo la familiare dashboard di System Manager.

BlueXP consente di creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP), utilizzare i servizi dati di NetApp (ad esempio, backup cloud) e controllare molti dispositivi storage on-premise e edge.

Per utilizzare System Manager in BlueXP, attenersi alla seguente procedura:

## Fasi

1. Aprire un browser Web e inserire l'indirizzo IP dell'interfaccia di rete per la gestione del cluster.

Se il cluster dispone della connettività a BlueXP, viene visualizzato un prompt di accesso.

2. Fare clic su **Continue to BlueXP** (continua con BlueXP\*) per seguire il link a BlueXP.



Se le impostazioni del sistema hanno bloccato le reti esterne, non sarà possibile accedere a BlueXP. Per accedere a System Manager utilizzando BlueXP, devi assicurarti che il sistema possa accedere all'indirizzo "cloudmanager.cloud.netapp.com". In caso contrario, quando richiesto, è possibile scegliere di utilizzare la versione di Gestione sistema installata con il sistema ONTAP.

3. Nella pagina di accesso a BlueXP, selezionare **Accedi con le credenziali del sito di supporto NetApp** e immettere le credenziali.

Se hai già utilizzato BlueXP e disponi di un account di accesso utilizzando un'e-mail e una password, dovrai continuare a utilizzare l'opzione di accesso.

["Scopri di più sull'accesso a BlueXP"](#).

4. Se richiesto, immettere un nome per il nuovo account BlueXP.

Nella maggior parte dei casi, BlueXP crea automaticamente un account in base ai dati del cluster.

5. Immettere le credenziali di amministratore del cluster per il cluster.

## Risultato

System Manager viene visualizzato ed è ora possibile gestire il cluster da BlueXP.

## Scopri i tuoi cluster direttamente da BlueXP

BlueXP offre due modi per rilevare e gestire i cluster:

- Rilevamento diretto per la gestione tramite System Manager

Si tratta della stessa opzione di rilevamento descritta nella sezione precedente con cui si segue il reindirizzamento.

- Rilevamento attraverso un connettore

Il connettore è un software installato nel tuo ambiente che ti consente di accedere alle funzioni di gestione tramite System Manager e ai servizi cloud BlueXP che offrono funzionalità come replica dei dati, backup e recovery, classificazione dei dati, tiering dei dati e molto altro ancora.

Accedere alla "[Documentazione BlueXP](#)" per ulteriori informazioni su queste opzioni di rilevamento e gestione.

## Scopri di più su BlueXP

- "[Panoramica di BlueXP](#)"
- "[Gestisci i tuoi sistemi NetApp AFF e FAS tramite BlueXP](#)"

# Introduzione e concetti

## Concetti di ONTAP

### Panoramica dei concetti

I seguenti concetti informano il software di gestione dei dati ONTAP, inclusi storage in cluster, alta disponibilità, virtualizzazione, protezione dei dati, Efficienza dello storage, sicurezza e FabricPool. Prima di configurare la soluzione di storage, è necessario conoscere la gamma completa di funzionalità e vantaggi di ONTAP.

Per ulteriori informazioni, consultare quanto segue:

- ["Amministrazione di cluster e SVM"](#)
- ["Coppie ad alta disponibilità \(ha\)"](#)
- ["Gestione di rete e LIF"](#)
- ["Gestione di dischi e aggregati"](#)
- ["FlexVol Volumes, tecnologia FlexClone e funzionalità di efficienza dello storage"](#)
- ["Provisioning host SAN"](#)
- Accesso al file NAS
  - ["Gestione NFS"](#)
  - ["Gestione delle PMI"](#)
- ["Disaster recovery e archiviazione"](#)

### Piattaforme ONTAP

Il software per la gestione dei dati ONTAP offre storage unificato per le applicazioni che leggono e scrivono i dati su protocolli di accesso a blocchi o file, in configurazioni storage che spaziano dalla flash ad alta velocità, ai supporti rotanti a basso prezzo, allo storage a oggetti basato sul cloud.

Le implementazioni di ONTAP vengono eseguite su piattaforme FAS, AFF A-Series e C-Series e All-SAN Flash Array ASA, oltre che su commodity hardware (ONTAP Select) e in cloud privati, pubblici o ibridi (Cloud Volumes ONTAP). Un'implementazione specializzata offre un'infrastruttura convergente Best-in-class (data center FlexPod).

Insieme, queste implementazioni formano il framework di base del *data fabric NetApp*, con un approccio comune software-defined alla gestione dei dati e una replica rapida ed efficiente tra le piattaforme.

### Storage in cluster

L'attuale iterazione di ONTAP è stata originariamente sviluppata per l'architettura storage scale-out di NetApp. Questa è l'architettura che di solito si trova nelle implementazioni dei data center di ONTAP. Poiché questa implementazione esercita la maggior parte delle funzionalità di ONTAP, è un buon punto di partenza per comprendere i concetti che



informano la tecnologia ONTAP.

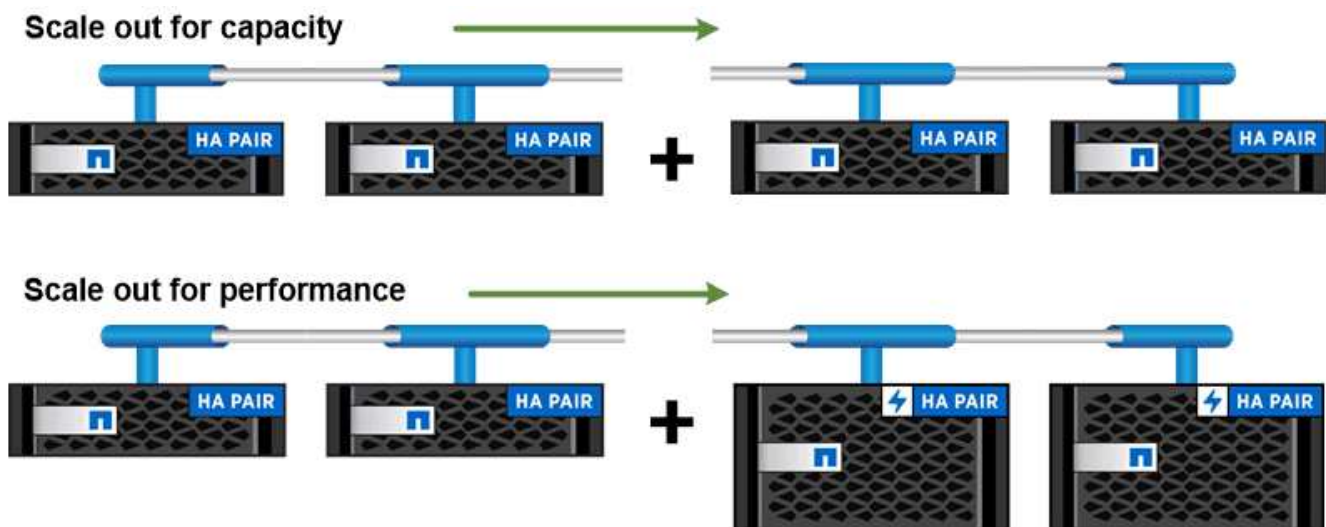
Le architetture dei data center in genere implementano controller FAS o AFF dedicati che eseguono il software di gestione dei dati ONTAP. Ciascun controller, il relativo storage, la connettività di rete e l'istanza di ONTAP in esecuzione sul controller sono denominati *node*.

I nodi sono accoppiati per l'alta disponibilità (ha). Insieme, queste coppie (fino a 12 nodi per SAN, fino a 24 nodi per NAS) comprendono il cluster. I nodi comunicano tra loro tramite un'interconnessione cluster dedicata privata.

A seconda del modello di controller, lo storage a nodi è costituito da dischi flash, dischi di capacità o entrambi. Le porte di rete sul controller forniscono l'accesso ai dati. Le risorse di storage fisico e di connettività di rete sono virtualizzate, visibili solo agli amministratori del cluster, non ai client NAS o agli host SAN.

I nodi di una coppia ha devono utilizzare lo stesso modello di array di storage. In caso contrario, è possibile utilizzare qualsiasi combinazione di controller supportata. Puoi scalare in base alla capacità aggiungendo nodi con modelli di storage array simili o per le performance aggiungendo nodi con storage array di fascia superiore.

Naturalmente è possibile scalare in alto anche in tutti i modi tradizionali, aggiornando dischi o controller in base alle esigenze. L'infrastruttura di storage virtualizzata di ONTAP semplifica lo spostamento dei dati senza interruzioni, consentendoti di scalare verticalmente o orizzontalmente senza downtime.



*You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.*

## Coppie ad alta disponibilità

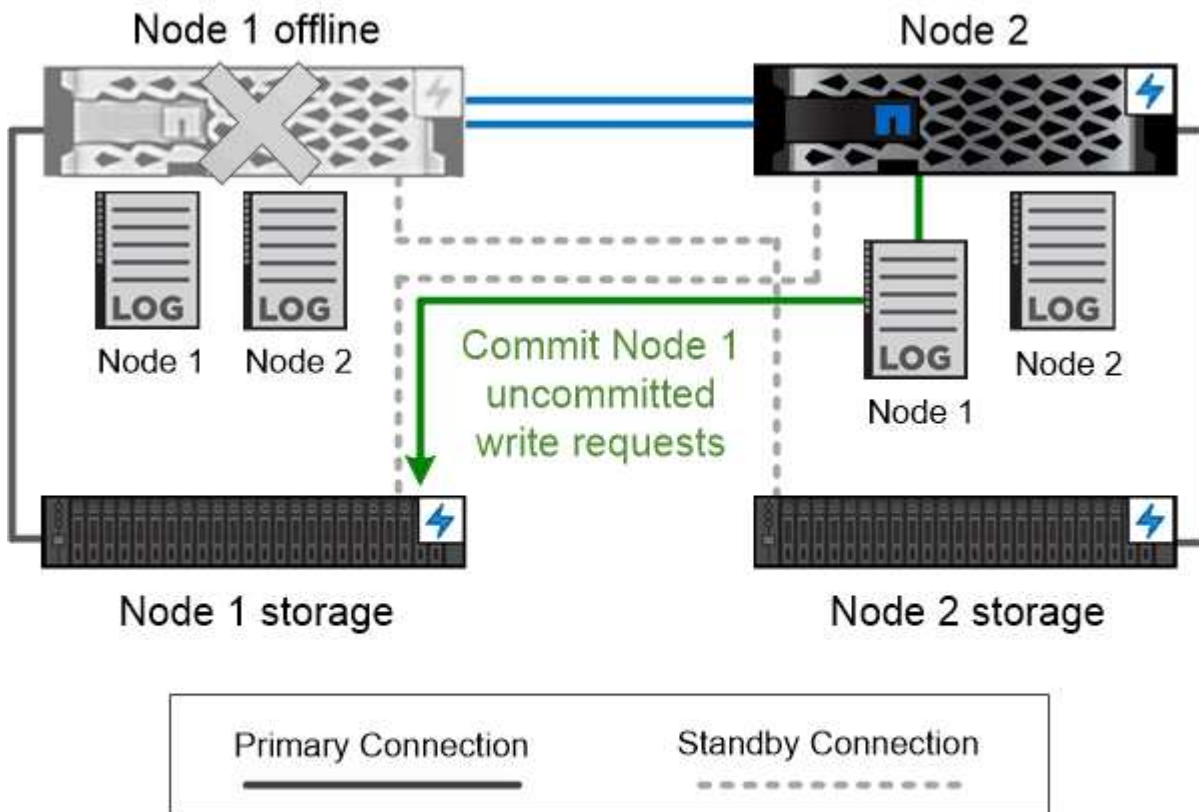
I nodi del cluster sono configurati in *coppie ad alta disponibilità (ha)* per la fault tolerance e le operazioni senza interruzioni. Se un nodo si guasta o se è necessario interrompere un nodo per la manutenzione ordinaria, il partner può *assumere* il proprio storage e continuare a fornire i dati da esso. Il partner *restituisce* lo storage quando il nodo viene riportato in linea.

Le coppie HA sono sempre costituite da modelli di controller simili. In genere, i controller risiedono nello stesso chassis con alimentatori ridondanti.

Le coppie hanno nodi con tolleranza agli errori in grado di comunicare tra loro in modi diversi per consentire a ciascun nodo di verificare continuamente se il proprio partner funziona e di mirrorare i dati di registro per la memoria non volatile dell'altro. Quando una richiesta di scrittura viene effettuata a un nodo, viene registrata nella NVRAM su entrambi i nodi prima che una risposta venga rinviata al client o all'host. In caso di failover, il partner superstite impegna le richieste di scrittura non assegnate del nodo guasto sul disco, garantendo la coerenza dei dati.

Le connessioni ai supporti di storage dell'altro controller consentono a ciascun nodo di accedere allo storage dell'altro in caso di takeover. I meccanismi di failover del percorso di rete garantiscono che client e host continuino a comunicare con il nodo esistente.

Per garantire la disponibilità, è necessario mantenere l'utilizzo della capacità delle performance su entrambi i nodi al 50% per adattarsi al carico di lavoro aggiuntivo nel caso di failover. Per lo stesso motivo, è possibile configurare non più del 50% del numero massimo di interfacce di rete virtuale NAS per un nodo.



*On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.*

#### **Takeover e giveback nelle implementazioni virtualizzate di ONTAP**

Lo storage non viene condiviso tra nodi in implementazioni ONTAP virtualizzate "hared-nothing `s`" come Cloud Volumes ONTAP per AWS o ONTAP Select. Quando un nodo non funziona, il suo partner continua a fornire i dati da una copia sincrona dei dati del nodo con mirroring. Non prende il controllo dello storage del nodo, ma solo della funzione di data serving.

## Consulente digitale AutoSupport e Active IQ

ONTAP offre il monitoraggio e il reporting dei sistemi basati sull'intelligenza artificiale attraverso un portale web e un'app mobile. Il componente AutoSupport di ONTAP invia la telemetria che viene analizzata dal consulente digitale Active IQ.

Active IQ ti consente di ottimizzare la tua infrastruttura dati nel tuo cloud ibrido globale offrendo analisi predittive e supporto proattivo attraverso un portale basato sul cloud e un'app mobile. Le informazioni e i consigli di Active IQ basati sui dati sono disponibili per tutti i clienti NetApp con un contratto SupportEdge attivo (le funzionalità variano in base al prodotto e al livello di supporto).

Ecco alcune cose che puoi fare con Active IQ:

- Pianificare gli aggiornamenti. Active IQ identifica i problemi dell'ambiente che possono essere risolti eseguendo l'aggiornamento a una versione più recente di ONTAP e il componente preparazione aggiornamento consente di pianificare un aggiornamento corretto.
- Visualizza lo stato di salute del sistema. La dashboard di Active IQ segnala eventuali problemi relativi allo stato di salute e ti aiuta a correggerli. Monitorare la capacità del sistema per assicurarsi di non esaurire mai lo spazio di storage.
- Gestire le performance. Active IQ mostra le performance del sistema in un periodo più lungo di quello che puoi vedere in Gestione sistema. Identificare i problemi di configurazione e di sistema che influiscono sulle performance.
- Massimizza l'efficienza. Visualizza le metriche di efficienza dello storage e identifica i modi per memorizzare più dati in meno spazio.
- Visualizza l'inventario e la configurazione. Active IQ visualizza l'inventario completo e le informazioni di configurazione software e hardware. Verificare la scadenza dei contratti di servizio per garantire la garanzia di una copertura.

### Informazioni correlate

["Documentazione NetApp: Consulente digitale Active IQ"](#)

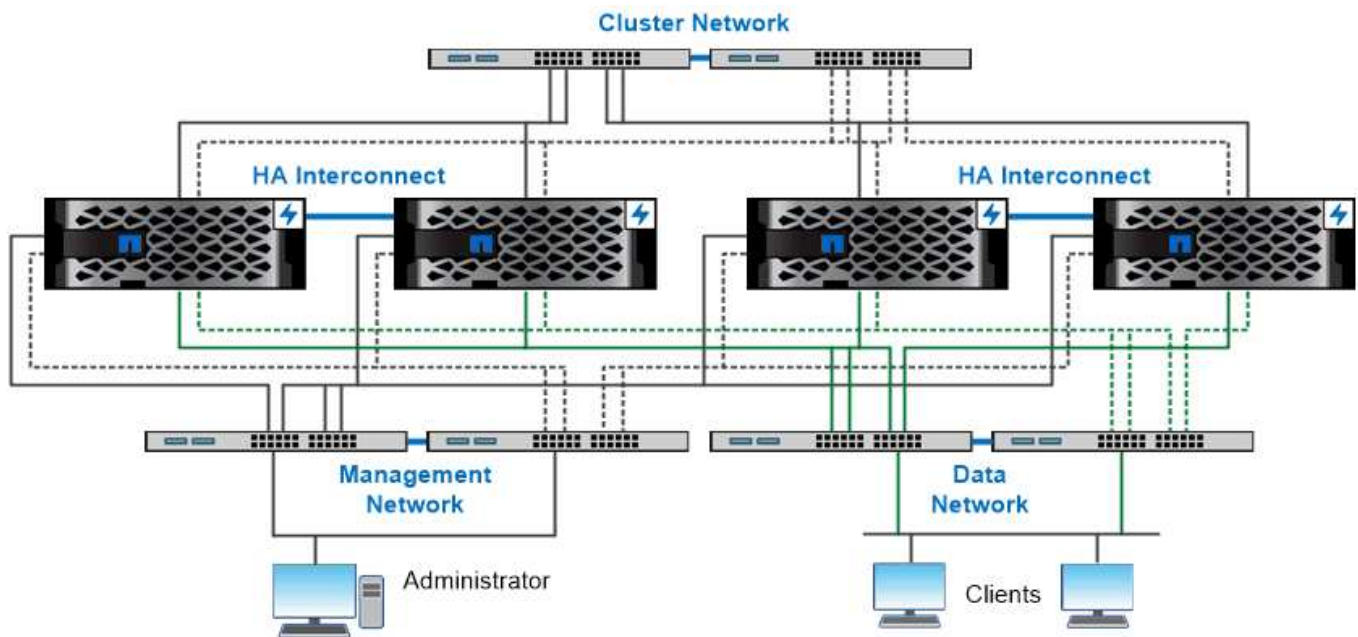
["Avviare Active IQ"](#)

["Servizi SupportEdge"](#)

## Architettura di rete

### Panoramica dell'architettura di rete

L'architettura di rete per un'implementazione di un data center ONTAP in genere è costituita da un'interconnessione cluster, una rete di gestione per l'amministrazione del cluster e una rete dati. Le schede di interfaccia di rete (NIC) forniscono porte fisiche per le connessioni Ethernet. Gli HBA (host bus adapter) forniscono porte fisiche per le connessioni FC.



*The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.*

## Porte logiche

Oltre alle porte fisiche fornite su ciascun nodo, è possibile utilizzare *porte logiche* per gestire il traffico di rete. Le porte logiche sono gruppi di interfacce o VLAN.

## Gruppi di interfacce

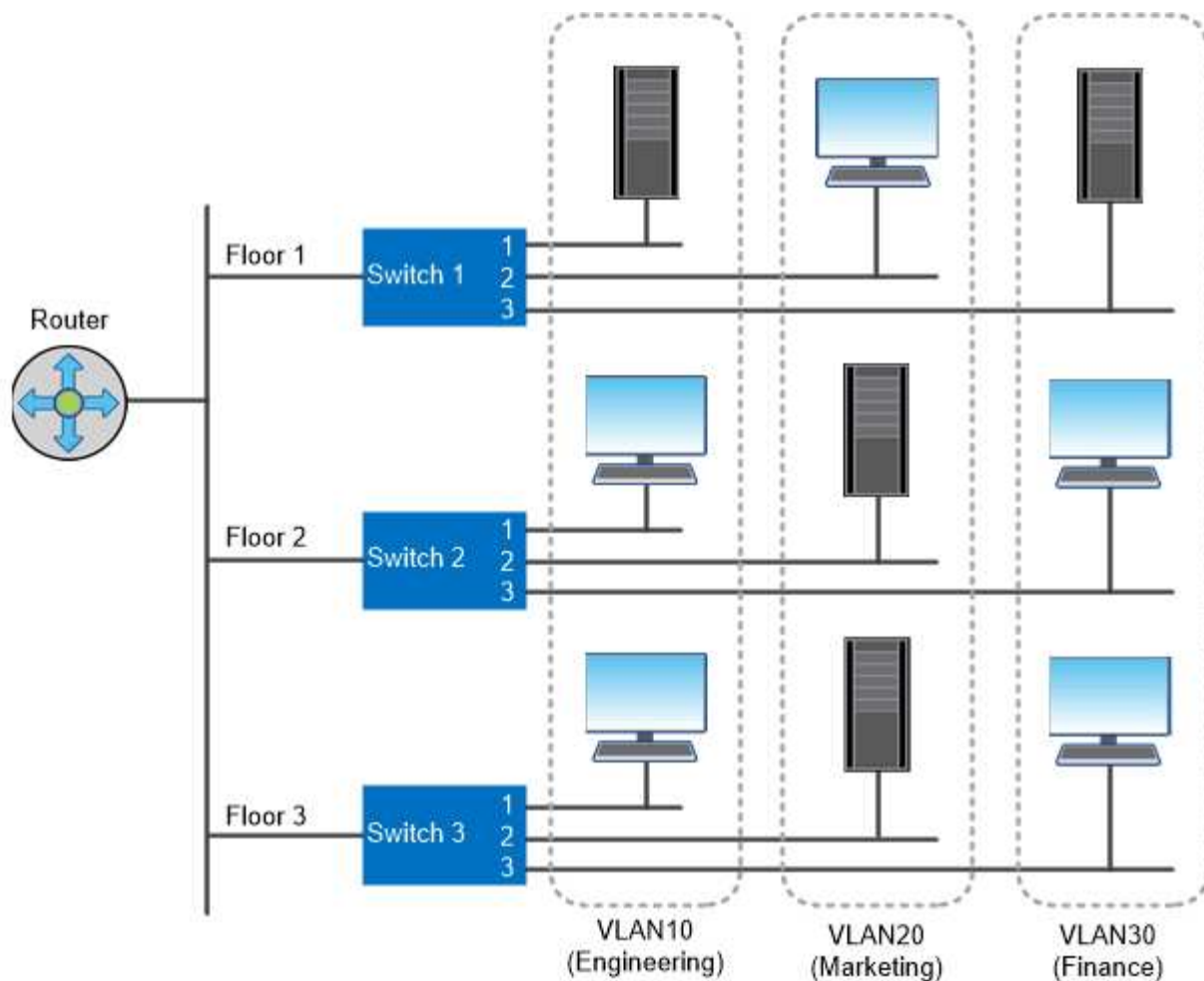
*Gruppi di interfacce* combina più porte fisiche in una singola “porta trunk” logica. È possibile creare un gruppo di interfacce costituito da porte provenienti da NIC in slot PCI diversi per evitare un errore di slot che riduce il traffico business-critical.

Un gruppo di interfacce può essere monomodale, multimodale o multimodale dinamica. Ogni modalità offre diversi livelli di tolleranza agli errori. Per bilanciare il carico del traffico di rete, è possibile utilizzare entrambi i tipi di gruppo di interfacce multimodali.

## VLAN

*VLAN* separa il traffico da una porta di rete (che potrebbe essere un gruppo di interfacce) in segmenti logici definiti in base alla porta dello switch, piuttosto che in base ai confini fisici. Le *stazioni finali* appartenenti a una VLAN sono correlate in base alla funzione o all'applicazione.

È possibile raggruppare le stazioni finali per reparto, ad esempio Engineering and Marketing, o per progetto, ad esempio release1 e release2. Poiché la prossimità fisica delle stazioni finali è irrilevante in una VLAN, le stazioni finali possono essere geograficamente remote.



*You can use VLANs to segregate traffic by department.*

### Supporto per tecnologie di rete standard di settore

ONTAP supporta tutte le principali tecnologie di rete standard di settore. Le tecnologie chiave includono IPspaces, bilanciamento del carico DNS e trap SNMP.

I domini di broadcast, i gruppi di failover e le subnet sono descritti nella [Failover del percorso NAS](#).

### IPspaces

È possibile utilizzare un *IPSpace* per creare uno spazio di indirizzi IP distinto per ciascun server di dati virtuale in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

Un provider di servizi, ad esempio, potrebbe configurare diversi spazi IP per i tenant utilizzando gli stessi indirizzi IP per accedere a un cluster.

### Bilanciamento del carico DNS

È possibile utilizzare *bilanciamento del carico DNS* per distribuire il traffico di rete degli utenti tra le porte disponibili. Un server DNS seleziona dinamicamente un'interfaccia di rete per il traffico in base al numero di client montati sull'interfaccia.

## Trap SNMP

È possibile utilizzare *trap SNMP* per controllare periodicamente la presenza di soglie operative o errori. I trap SNMP catturano le informazioni di monitoraggio del sistema inviate in modo asincrono da un agente SNMP a un gestore SNMP.

## Conformità FIPS

ONTAP è conforme agli standard federali sull'elaborazione delle informazioni (FIPS) 140-2 per tutte le connessioni SSL. È possibile attivare e disattivare la modalità SSL FIPS, impostare i protocolli SSL a livello globale e disattivare le crittografie deboli come RC4.

## Panoramica di RDMA

Le offerte Remote Direct Memory Access (RDMA) di ONTAP supportano carichi di lavoro sensibili alla latenza e a elevata larghezza di banda. RDMA consente di copiare i dati direttamente tra la memoria del sistema di storage e la memoria del sistema host, eludendo le interruzioni della CPU e l'overhead.

## NFS su RDMA

A partire da ONTAP 9.10.1, è possibile eseguire la configurazione ["NFS su RDMA"](#) Per consentire l'utilizzo dello storage NVIDIA GPUDirect per carichi di lavoro con accelerazione GPU su host con GPU NVIDIA supportate.

## Interconnessione del cluster RDMA

L'interconnessione del cluster RDMA riduce la latenza, riduce i tempi di failover e accelera la comunicazione tra i nodi di un cluster.

A partire da ONTAP 9.10.1, cluster Interconnect RDMA è supportato per determinati sistemi hardware, se utilizzato con le schede di rete del cluster X1151A. A partire da ONTAP 9.13.1, le schede di rete X91153A supportano anche la interconnessione in cluster RDMA. Consultare la tabella per sapere quali sistemi sono supportati nelle diverse versioni di ONTAP.

Sistemi	Versioni di ONTAP supportate
<ul style="list-style-type: none"><li>• R400</li><li>• ASA A400</li></ul>	ONTAP 9.10.1 e versioni successive
<ul style="list-style-type: none"><li>• AFF A900</li><li>• ASA A900</li><li>• FAS9500</li></ul>	ONTAP 9.13.1 e versioni successive

Data l'impostazione appropriata del sistema di storage, non è necessaria alcuna configurazione aggiuntiva per utilizzare l'interconnessione RDMA.

## Protocolli client

ONTAP supporta tutti i principali protocolli client standard di settore: NFS, SMB, FC, FCoE, iSCSI, NVMe/FC e S3.



## **NFS**

NFS è il protocollo di accesso ai file tradizionale per i sistemi UNIX e LINUX. I client possono accedere ai file in volumi ONTAP utilizzando i seguenti protocolli.

- NFSv3
- NFSv4
- NFSv4.2
- NFSv4.1
- PNFS

È possibile controllare l'accesso ai file utilizzando permessi di stile UNIX, permessi di stile NTFS o una combinazione di entrambi.

I client possono accedere agli stessi file utilizzando i protocolli NFS e SMB.

## **PMI**

SMB è il protocollo di accesso ai file tradizionale per i sistemi Windows. I client possono accedere ai file nei volumi ONTAP utilizzando i protocolli SMB 2.0, SMB 2.1, SMB 3.0 e SMB 3.1.1. Come per NFS, sono supportati diversi stili di permesso.

SMB 1.0 è disponibile ma disattivato per impostazione predefinita in ONTAP 9.3 e versioni successive.

## **FC**

Fibre Channel è il protocollo a blocchi di rete originale. Al posto dei file, un protocollo a blocchi presenta un intero disco virtuale a un client. Il protocollo FC tradizionale utilizza una rete FC dedicata con switch FC specializzati e richiede che il computer client disponga di interfacce di rete FC.

Un LUN rappresenta il disco virtuale e uno o più LUN vengono memorizzati in un volume ONTAP. È possibile accedere allo stesso LUN attraverso i protocolli FC, FCoE e iSCSI, ma più client possono accedere allo stesso LUN solo se fanno parte di un cluster che impedisce collisioni in scrittura.

## **FCoE**

FCoE è fondamentalmente lo stesso protocollo di FC, ma utilizza una rete Ethernet di livello datacenter al posto del trasporto FC tradizionale. Il client richiede ancora un'interfaccia di rete specifica per FCoE.

## **iSCSI**

iSCSI è un protocollo a blocchi che può essere eseguito su reti Ethernet standard. La maggior parte dei sistemi operativi client offre un iniziatore software che viene eseguito su una porta Ethernet standard. iSCSI è una buona scelta quando è necessario un protocollo a blocchi per una particolare applicazione, ma non è disponibile una rete FC dedicata.

## **NVMe/FC**

Il più recente protocollo a blocchi, NVMe/FC, è progettato specificamente per funzionare con lo storage basato su flash. Offre sessioni scalabili, una significativa riduzione della latenza e un aumento del parallelismo, il che lo rende ideale per applicazioni a bassa latenza e throughput elevato, come database in-memory e analytics.

A differenza di FC e iSCSI, NVMe non utilizza LUN. Utilizza invece spazi dei nomi, memorizzati in un volume

ONTAP. È possibile accedere agli spazi dei nomi NVMe solo tramite il protocollo NVMe.

### S3

A partire da ONTAP 9.8, è possibile attivare un server S3 (Simple Storage Service) di ONTAP in un cluster ONTAP, consentendo di fornire i dati nello storage a oggetti utilizzando i bucket S3.

ONTAP supporta due scenari di casi d'utilizzo on-premise per il servizio dello storage a oggetti S3:

- Tier FabricPool per un bucket su cluster locale (Tier to a local bucket) o cluster remoto (Tier cloud).
- Accesso dell'applicazione client S3 a un bucket sul cluster locale o su un cluster remoto.



ONTAP S3 è adatto per le funzionalità S3 sui cluster esistenti senza hardware e gestione aggiuntivi. Per implementazioni superiori a 300 TB, il software NetApp StorageGRID continua a essere la soluzione di punta per lo storage a oggetti. Scopri di più ["StorageGRID"](#).

## Dischi e aggregati

=  
:allow-uri-read:

### Tier locali (aggregati) e gruppi RAID

Le moderne tecnologie RAID proteggono dai guasti dei dischi ricostruendo i dati di un disco guasto su un disco spare. Il sistema confronta le informazioni di indice su un “disco di parità” con i dati sui dischi integri rimanenti per ricostruire i dati mancanti, il tutto senza downtime o costi significativi per le performance.

Un Tier locale (aggregato) è costituito da uno o più *gruppi RAID*. Il *tipo RAID* del livello locale determina il numero di dischi di parità nel gruppo RAID e il numero di guasti simultanei dei dischi da cui la configurazione RAID protegge.

Il tipo RAID predefinito, RAID-DP (RAID-Double Parity), richiede due dischi di parità per gruppo RAID e protegge dalla perdita di dati in caso di guasto di due dischi contemporaneamente. Per RAID-DP, la dimensione del gruppo RAID consigliata è compresa tra 12 e 20 HDD e tra 20 e 28 SSD.

È possibile distribuire il costo di overhead dei dischi di parità creando gruppi RAID all'estremità più alta della raccomandazione di dimensionamento. Questo vale soprattutto per gli SSD, che sono molto più affidabili dei dischi con capacità. Per i Tier locali che utilizzano HDD, è necessario bilanciare la necessità di massimizzare lo storage su disco rispetto a fattori compensativi come il tempo di ricostruzione più lungo richiesto per gruppi RAID più grandi.

### Tier locali mirrorati e senza mirror (aggregati)

ONTAP dispone di una funzionalità opzionale denominata *SyncMirror* che è possibile utilizzare per eseguire il mirroring sincrono dei dati del Tier locale (aggregato) nelle copie, o *plex*, memorizzate in diversi gruppi RAID. I plex garantiscono la protezione contro la perdita di dati in caso di guasti di più dischi rispetto al tipo RAID o in caso di perdita di connettività ai dischi del gruppo RAID.

Quando si crea un Tier locale con System Manager o utilizzando la CLI, è possibile specificare che il Tier

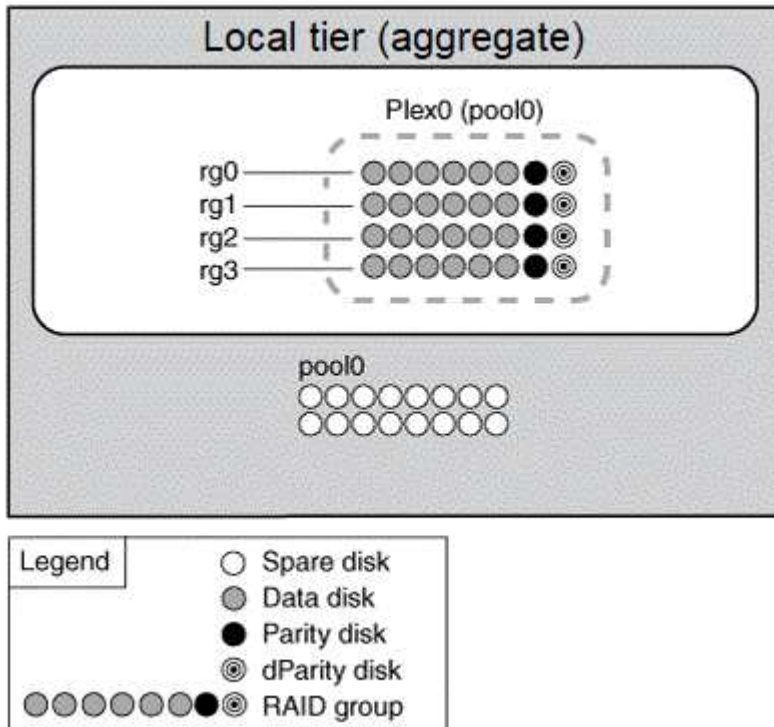


locale sia mirrorato o senza mirror.

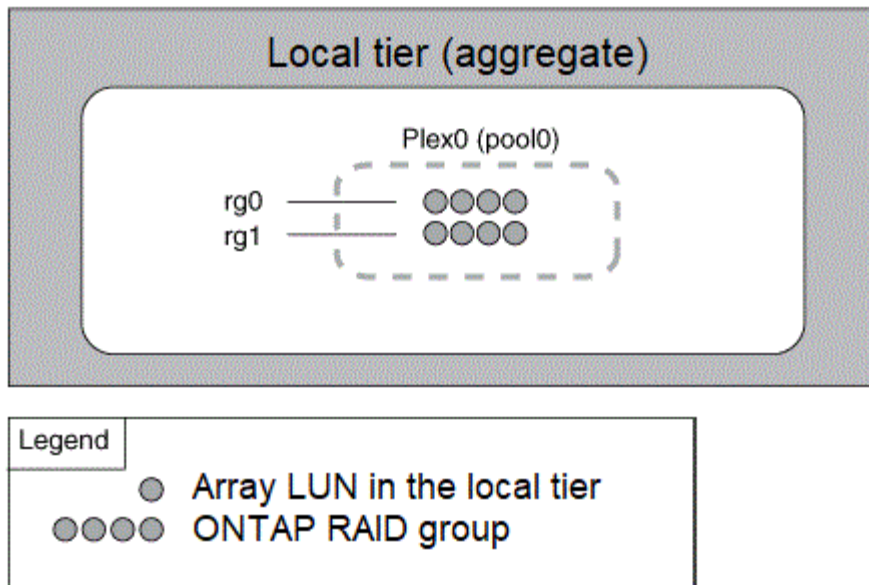
### Come funzionano i Tier locali senza mirror (aggregati)

Se non si specifica il mirroring dei Tier locali, questi vengono creati come Tier locali senza mirror (aggregati). I Tier locali senza mirror dispongono di un solo *plex* (una copia dei dati), che contiene tutti i gruppi RAID appartenenti a quel Tier locale.

Il diagramma seguente mostra un Tier locale senza mirror composto da dischi, con il suo unico plex. Il Tier locale dispone di quattro gruppi RAID: Rg0, rg1, rg2 e rg3. Ciascun gruppo RAID dispone di sei dischi dati, un disco di parità e un disco di parità doppia. Tutti i dischi utilizzati dal Tier locale provengono dallo stesso pool, “pool0”.



Il seguente diagramma mostra un Tier locale senza mirror con LUN di array, con un unico plex. Ha due gruppi RAID, rg0 e rg1. Tutte le LUN degli array utilizzate dal Tier locale provengono dallo stesso pool, “pool0”.



### Come funzionano i Tier locali mirrorati (aggregati)

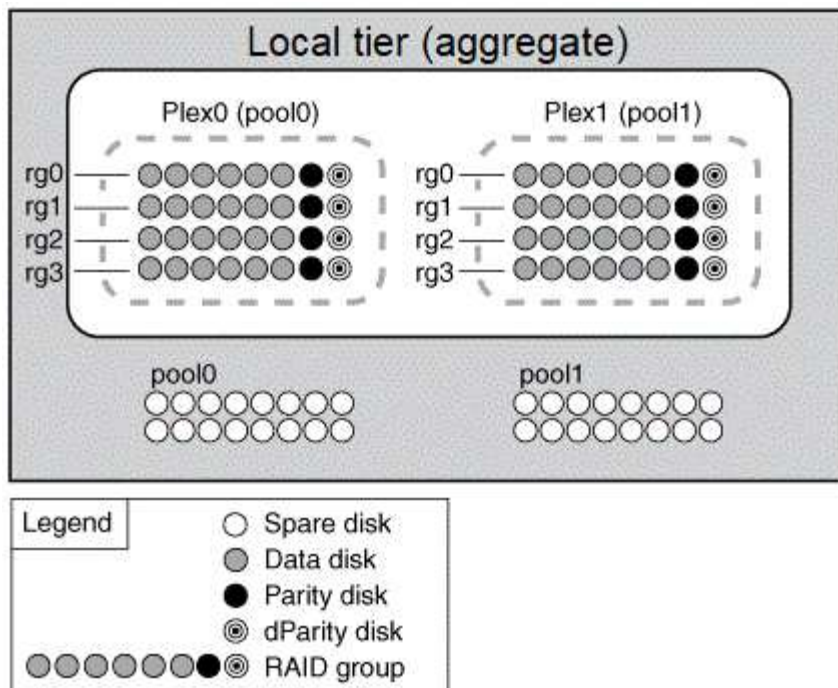
Gli aggregati mirrorati hanno due *plex* (copie dei dati), che utilizzano la funzionalità SyncMirror per duplicare i dati e fornire ridondanza.

Quando si crea un Tier locale, è possibile specificare che si tratta di un Tier locale mirrorato. Inoltre, è possibile aggiungere un secondo plex a un Tier locale senza mirror esistente per renderlo un Tier mirrorato. Utilizzando la funzionalità SyncMirror, ONTAP copia i dati nel plesso originale (plex0) nel nuovo plesso (plex1). I plex sono fisicamente separati (ogni plesso ha i propri gruppi RAID e il proprio pool) e i plex vengono aggiornati simultaneamente.

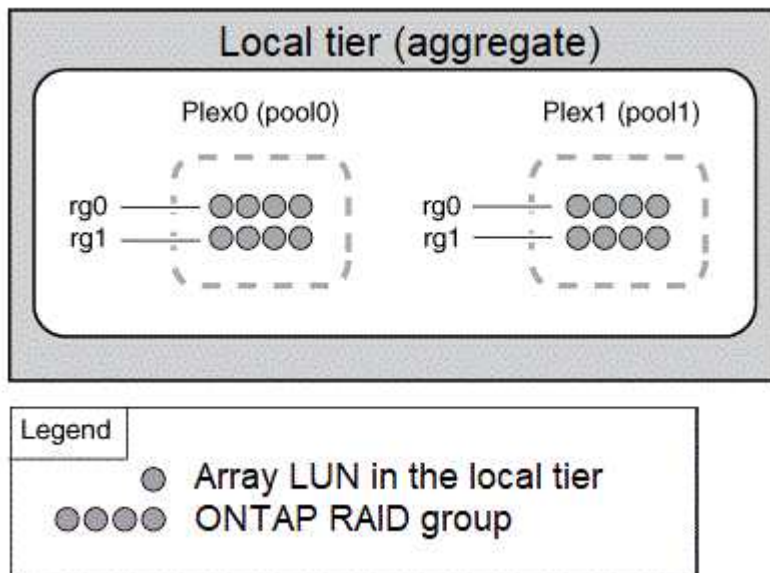
Questa configurazione offre una protezione aggiuntiva contro la perdita di dati in caso di guasti di più dischi rispetto al livello RAID dell'aggregato, in quanto il plex non interessato continua a fornire dati mentre si corregge la causa dell'errore. Una volta risolto il problema, i due plessi risincronizzano e ristabiliscono la relazione di mirroring.

I dischi e le LUN degli array sul sistema sono divisi in due pool: "pool0" e "pool1". Plex0 ottiene lo storage dal pool0 e Plex1 lo ottiene dal pool1.

Il seguente diagramma mostra un Tier locale composto da dischi con la funzionalità SyncMirror attivata e implementata. È stato creato un secondo plex per il Tier locale, "plex1". I dati in plex1 sono una copia dei dati in plex0 e anche i gruppi RAID sono identici. I 32 dischi spare vengono allocati al pool 0 o pool1 utilizzando 16 dischi per ciascun pool.



Il diagramma seguente mostra un Tier locale composto da LUN array con la funzionalità SyncMirror attivata e implementata. È stato creato un secondo plex per il Tier locale, "plex1". Plex1 è una copia di plex0 e anche i gruppi RAID sono identici.



Si consiglia di mantenere almeno il 20% di spazio libero per gli aggregati con mirroring, per performance e disponibilità dello storage ottimali. Sebbene il suggerimento sia del 10% per gli aggregati non speculari, il 10% di spazio aggiuntivo può essere utilizzato dal filesystem per assorbire le modifiche incrementali. I cambiamenti incrementali aumentano l'utilizzo dello spazio per gli aggregati con mirroring grazie all'architettura copy-on-write basata su Snapshot di ONTAP. Il mancato rispetto di queste Best practice può avere un impatto negativo sulle prestazioni.

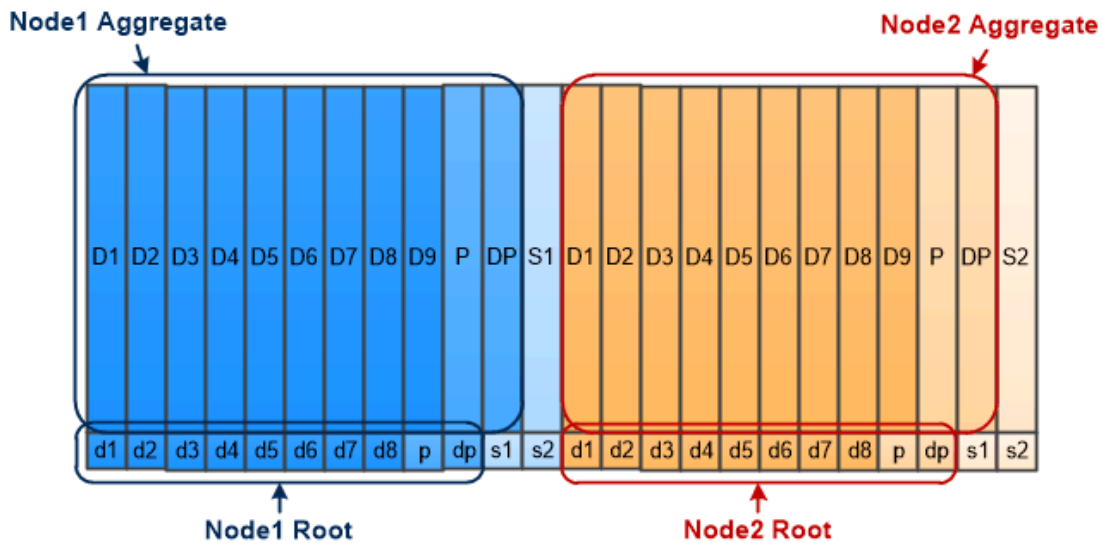
## Partizione dei dati root

Ogni nodo deve disporre di un aggregato root per i file di configurazione del sistema storage. L'aggregato root ha il tipo RAID dell'aggregato di dati.

System Manager non supporta la partizione root-data o root-data-data.

Un aggregato root di tipo RAID-DP è generalmente costituito da un disco dati e da due dischi di parità. Si tratta di una "tassa di parità" significativa da pagare per i file del sistema di storage, quando il sistema sta già riservando due dischi come dischi di parità per ciascun gruppo RAID nell'aggregato.

*Partizione dei dati root* riduce la tassa di parità suddividendo l'aggregato root tra le partizioni del disco, riservando una piccola partizione su ciascun disco come partizione root e una grande partizione per i dati.



*Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.*

Come suggerisce l'illustrazione, maggiore è il numero di dischi utilizzati per memorizzare l'aggregato root, minore è la partizione root. Questo è anche il caso di una forma di partizione dei dati root denominata *root-data-data partitioning*, che crea una partizione piccola come partizione root e due partizioni più grandi e di pari dimensioni per i dati.



*Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.*

Entrambi i tipi di partizione dei dati root fanno parte della funzione di *partizione avanzata dei dischi (ADP)* di ONTAP. Entrambi sono configurati in fabbrica: Partizione dei dati root per sistemi entry-level FAS2xxx, FAS9000, FAS8200, FAS80xx e AFF, partizione dei dati root solo per sistemi AFF.

Scopri di più ["Partizione avanzata dei dischi"](#).

#### Dischi partizionati e utilizzati per l'aggregato root

I dischi partizionati per l'utilizzo nell'aggregato root dipendono dalla configurazione del sistema.

Conoscere il numero di dischi utilizzati per l'aggregato root consente di determinare la quantità di capacità dei dischi riservata alla partizione root e la quantità disponibile per l'utilizzo in un aggregato di dati.

La funzionalità di partizione dei dati root è supportata per piattaforme entry-level, piattaforme All Flash FAS e piattaforme FAS con solo SSD collegati.

Per le piattaforme entry-level, vengono partizionati solo i dischi interni.

Per tutte le piattaforme Flash FAS e FAS con solo SSD collegati, tutti i dischi collegati al controller al momento dell'inizializzazione del sistema vengono partizionati, fino a un limite di 24 per nodo. Le unità aggiunte dopo la configurazione del sistema non vengono partizionate.

## Volumi, qtree, file e LUN

ONTAP fornisce dati a client e host da container logici denominati *volumi FlexVol*. poiché questi volumi sono solo accoppiati in modo lasco con il loro aggregato contenente, offrono una maggiore flessibilità nella gestione dei dati rispetto ai volumi tradizionali.

È possibile assegnare più volumi FlexVol a un aggregato, ciascuno dedicato a un'applicazione o servizio diverso. È possibile espandere e contrarre un volume FlexVol, spostare un volume FlexVol ed eseguire copie efficienti di un volume FlexVol. È possibile utilizzare *qtree* per partizionare un volume FlexVol in unità più gestibili e *quote* per limitare l'utilizzo delle risorse dei volumi.

I volumi contengono file system in un ambiente NAS e LUN in un ambiente SAN. Un LUN (Logical Unit

Number) è un identificatore di un dispositivo chiamato *unità logica* indirizzato da un protocollo SAN.

I LUN sono l'unità di storage di base in una configurazione SAN. L'host Windows vede le LUN del sistema storage come dischi virtuali. È possibile spostare le LUN in volumi diversi senza interruzioni in base alle esigenze.

Oltre ai volumi di dati, è necessario conoscere alcuni volumi speciali:

- Un *volume root del nodo* (in genere "vol0") contiene le informazioni di configurazione del nodo e i registri.
- Un *volume root SVM* funge da punto di ingresso allo spazio dei nomi fornito da SVM e contiene informazioni sulla directory dello spazio dei nomi.
- I *volumi di sistema* contengono metadati speciali come i registri di audit del servizio.

Non è possibile utilizzare questi volumi per memorizzare i dati.



*Volumes contain files in a NAS environment and LUNs in a SAN environment.*

### **volumi FlexGroup**

In alcune aziende, un singolo namespace potrebbe richiedere petabyte di storage, superando di gran lunga anche la capacità di 100 TB di un volume FlexVol.

Un *volume FlexGroup* supporta fino a 400 miliardi di file con 200 volumi membri costitutivi che lavorano in modo collaborativo per bilanciare dinamicamente l'allocazione di carico e spazio in modo uniforme tra tutti i membri.

Con un volume FlexGroup non è necessario alcun overhead di gestione o manutenzione. È sufficiente creare il volume FlexGroup e condividerlo con i client NAS. ONTAP fa il resto.

## **Virtualizzazione dello storage**



## Panoramica sulla virtualizzazione dello storage

Utilizzate *macchine virtuali storage (SVM)* per fornire dati a client e host. Come una macchina virtuale in esecuzione su un hypervisor, una SVM è un'entità logica che astratta le risorse fisiche. I dati a cui si accede tramite SVM non sono legati a una posizione nello storage. L'accesso di rete alla SVM non è vincolato a una porta fisica.



In precedenza, le SVM erano chiamate "vserver". L'interfaccia della riga di comando di ONTAP utilizza ancora il termine "vserver".

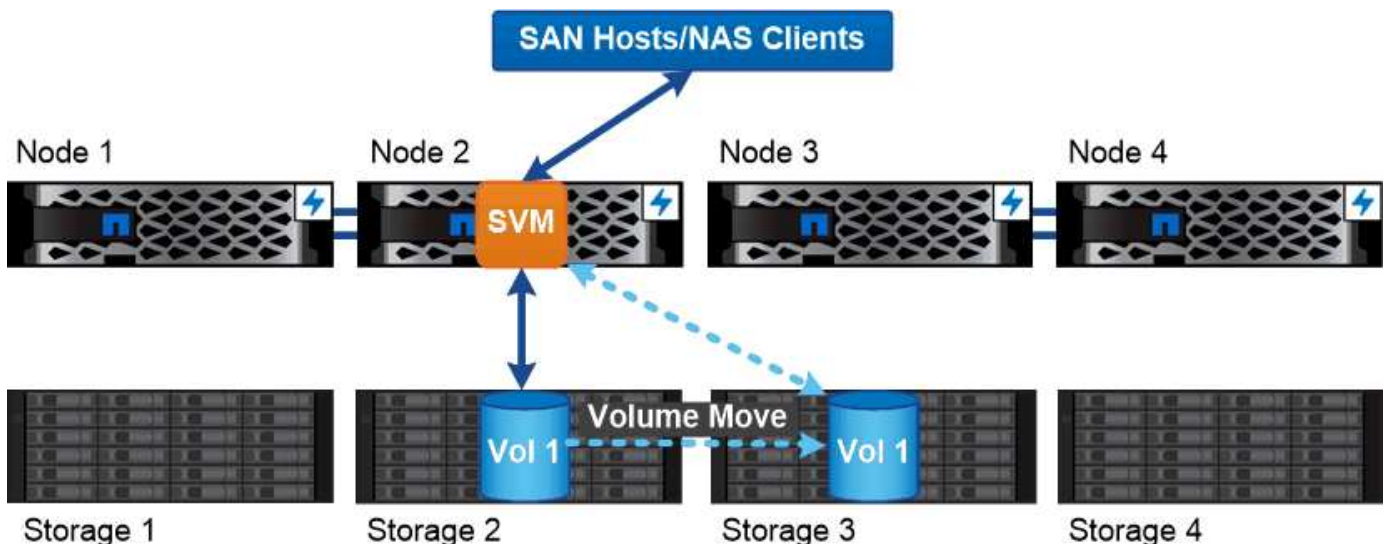
Una SVM fornisce i dati a client e host da uno o più volumi, attraverso una o più *interfacce logiche (LIF)* di rete. I volumi possono essere assegnati a qualsiasi aggregato di dati nel cluster. Le LIF possono essere ospitate da qualsiasi porta fisica o logica. Sia i volumi che le LIF possono essere spostati senza interrompere il servizio dati, sia che tu stia eseguendo aggiornamenti hardware, aggiungendo nodi, bilanciando le performance o ottimizzando la capacità tra gli aggregati.

La stessa SVM può avere una LIF per il traffico NAS e una LIF per il traffico SAN. Per accedere a SVM, i client e gli host necessitano solo dell'indirizzo LIF (indirizzo IP per NFS, SMB o iSCSI; WWPN per FC). I LIF mantengono i propri indirizzi mentre si spostano. Le porte possono ospitare più LIF. Ogni SVM dispone di sicurezza, amministrazione e spazio dei nomi propri.

Oltre alle SVM dei dati, ONTAP implementa speciali SVM per l'amministrazione:

- Una *SVM amministrativa* viene creata quando il cluster viene configurato.
- Un *nodo SVM* viene creato quando un nodo si unisce a un cluster nuovo o esistente.
- Viene creata automaticamente una *SVM di sistema* per le comunicazioni a livello di cluster in un IPspace.

Non è possibile utilizzare queste SVM per la distribuzione dei dati. Esistono inoltre LIF speciali per il traffico all'interno e tra i cluster e per la gestione di cluster e nodi.



*Data accessed through an SVM is not bound to a physical storage location. You can move a volume without disrupting data service.*

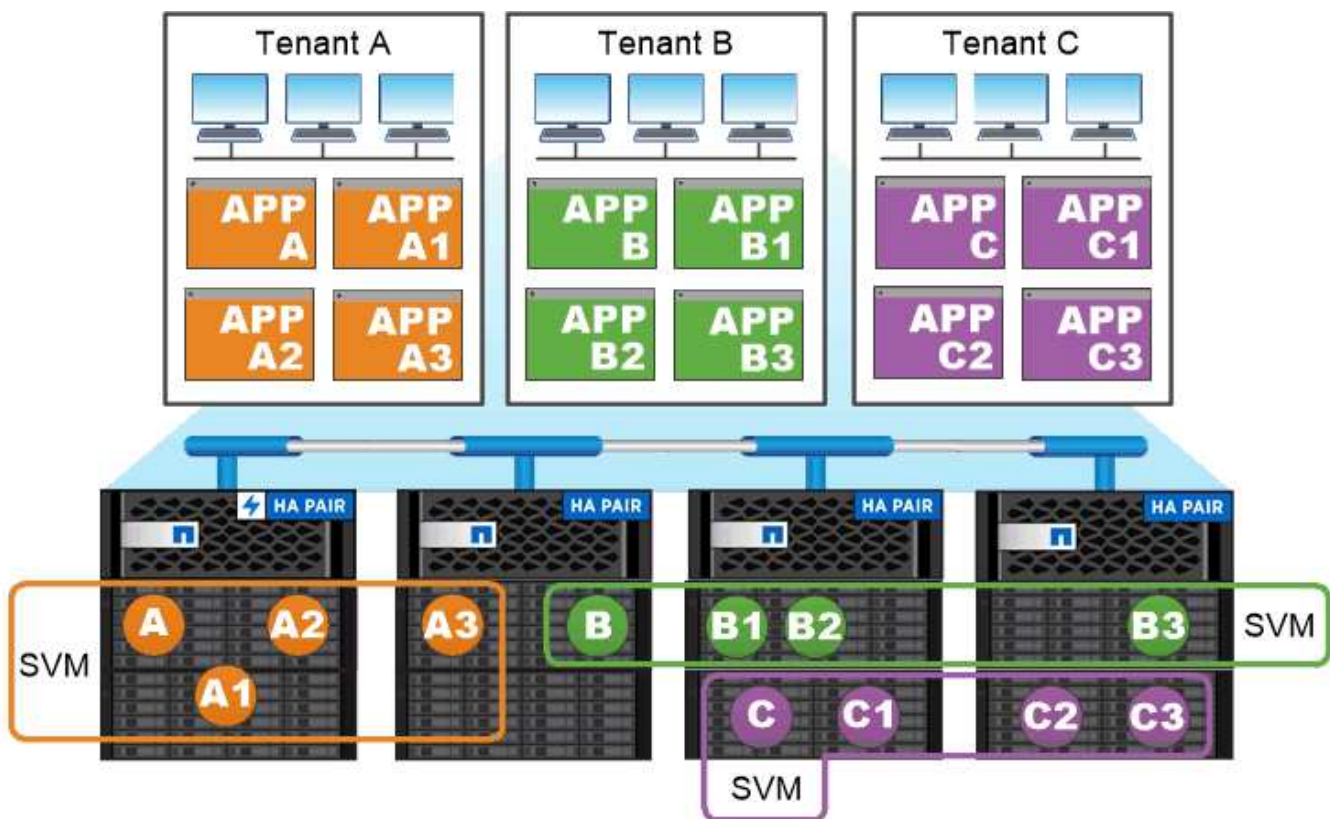
## Perché ONTAP è come il middleware

Gli oggetti logici utilizzati da ONTAP per le attività di gestione dello storage soddisfano gli obiettivi familiari di un pacchetto middleware ben progettato: Proteggere l'amministratore dai dettagli di implementazione di basso livello e isolare la configurazione dalle modifiche delle caratteristiche fisiche come nodi e porte. L'idea di base è che l'amministratore dovrebbe essere in grado di spostare facilmente volumi e LIF, riconfigurando alcuni campi piuttosto che l'intera infrastruttura di storage.

## Casi di utilizzo di SVM

I service provider utilizzano le SVM in accordi di multi-tenancy sicuri per isolare i dati di ciascun tenant, fornire a ciascun tenant la propria autenticazione e amministrazione e semplificare il chargeback. È possibile assegnare più LIF alla stessa SVM per soddisfare le diverse esigenze dei clienti e utilizzare la QoS per proteggere dai carichi di lavoro dei tenant "bullismo" dei carichi di lavoro degli altri tenant.

Gli amministratori utilizzano le SVM per scopi simili all'interno dell'azienda. È possibile separare i dati da diversi reparti o mantenere i volumi di storage a cui accedono gli host in una SVM e i volumi di condivisione utente in un'altra. Alcuni amministratori mettono LUN iSCSI/FC e datastore NFS in una condivisione SVM e SMB in un'altra.



*Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.*

## Amministrazione di cluster e SVM

Un amministratore del cluster accede alla SVM amministrativa per il cluster. La SVM



amministrativa e un amministratore del cluster con il nome riservato `admin` vengono creati automaticamente quando viene configurato il cluster.

Un amministratore del cluster con l'impostazione predefinita `admin` il ruolo può amministrare l'intero cluster e le relative risorse. L'amministratore del cluster può creare ulteriori amministratori del cluster con ruoli diversi in base alle esigenze.

Un *amministratore SVM* accede a una SVM di dati. L'amministratore del cluster crea gli amministratori SVM e SVM dei dati in base alle necessità.

Agli amministratori di SVM viene assegnato il `vsadmin` ruolo per impostazione predefinita. L'amministratore del cluster può assegnare ruoli diversi agli amministratori SVM in base alle esigenze.

### **RBAC (role-based Access Control)**

Il *ruolo* assegnato a un amministratore determina i comandi a cui l'amministratore ha accesso. Il ruolo viene assegnato quando si crea l'account per l'amministratore. È possibile assegnare un ruolo diverso o definire ruoli personalizzati in base alle esigenze.

### **Spazi dei nomi e punti di giunzione**

Un *namespace* NAS è un raggruppamento logico di volumi Uniti in *punti di giunzione* per creare una singola gerarchia di file system. Un client con autorizzazioni sufficienti può accedere ai file nello spazio dei nomi senza specificare la posizione dei file nello storage. I volumi Junctioned possono risiedere in qualsiasi punto del cluster.

Invece di montare ogni volume contenente un file di interesse, i client NAS montano un NFS *export* o accedono a una *share*. SMB. L'esportazione o la condivisione rappresenta l'intero namespace o una posizione intermedia all'interno dello spazio dei nomi. Il client accede solo ai volumi montati sotto il proprio access point.

È possibile aggiungere volumi allo spazio dei nomi in base alle esigenze. È possibile creare punti di giunzione direttamente sotto una giunzione di un volume padre o in una directory all'interno di un volume. Il percorso di una giunzione di volume per un volume denominato "vol3" potrebbe essere `/vol1/vol2/vol3`, o `/vol1/dir2/vol3`, o persino `/dir1/dir2/vol3`. Il percorso è chiamato *percorso di giunzione*.

Ogni SVM dispone di uno spazio dei nomi univoco. Il volume root SVM è il punto di ingresso della gerarchia dello spazio dei nomi.



Per garantire che i dati rimangano disponibili in caso di interruzione o failover di un nodo, è necessario creare una copia *mirror per la condivisione del carico* per il volume root SVM.



*A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.*

### Esempio

Nell'esempio riportato di seguito viene creato un volume denominato "home4" situato su SVM vs1 con un percorso di giunzione /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

## Failover del percorso

### Panoramica del failover del percorso

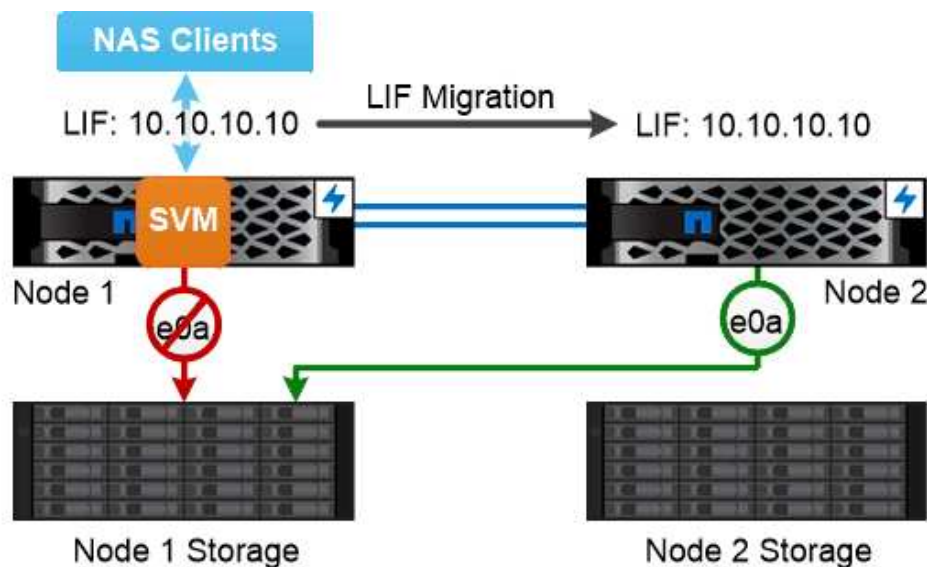
Esistono importanti differenze nel modo in cui ONTAP gestisce il failover del percorso nelle topologie NAS e SAN. Una LIF NAS esegue automaticamente la migrazione a una porta di rete diversa dopo un errore di collegamento. Un LIF SAN non esegue la migrazione (a meno che non venga spostato manualmente dopo l'errore). Invece, la tecnologia multipathing sull'host devia il traffico verso una LIF diversa, sulla stessa SVM, ma accede a una porta di rete diversa.

## Failover del percorso NAS

Un LIF NAS esegue automaticamente la migrazione a una porta di rete esistente dopo un errore di collegamento sulla porta corrente. La porta alla quale LIF migra deve essere membro del *gruppo di failover* per LIF. La *policy di gruppo di failover* restringe le destinazioni di failover per un LIF di dati alle porte sul nodo che possiede i dati e il suo partner ha.

Per comodità amministrativa, ONTAP crea un gruppo di failover per ogni *dominio di trasmissione* nell'architettura di rete. I domini di broadcast raggruppano le porte appartenenti alla stessa rete Layer 2. Se, ad esempio, si utilizzano VLAN per separare il traffico in base al reparto (Engineering, Marketing, Finance e così via), ogni VLAN definisce un dominio di trasmissione separato. Il gruppo di failover associato al dominio di trasmissione viene aggiornato automaticamente ogni volta che si aggiunge o rimuove una porta del dominio di trasmissione.

È quasi sempre consigliabile utilizzare un dominio di broadcast per definire un gruppo di failover per garantire che il gruppo di failover rimanga aggiornato. Talvolta, tuttavia, è possibile definire un gruppo di failover non associato a un dominio di broadcast. Ad esempio, è possibile che si desideri eseguire il failover delle LIF solo sulle porte di un sottoinsieme delle porte definite nel dominio di trasmissione.



*A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.*

### **subnet**

Una *subnet* riserva un blocco di indirizzi IP in un dominio di trasmissione. Questi indirizzi appartengono alla stessa rete Layer 3 e vengono allocati alle porte nel dominio di trasmissione quando si crea una LIF. In genere, quando si definisce un indirizzo LIF, è più semplice e meno soggetto a errori specificare un nome di subnet che specificare un indirizzo IP e una maschera di rete.

## Failover del percorso SAN

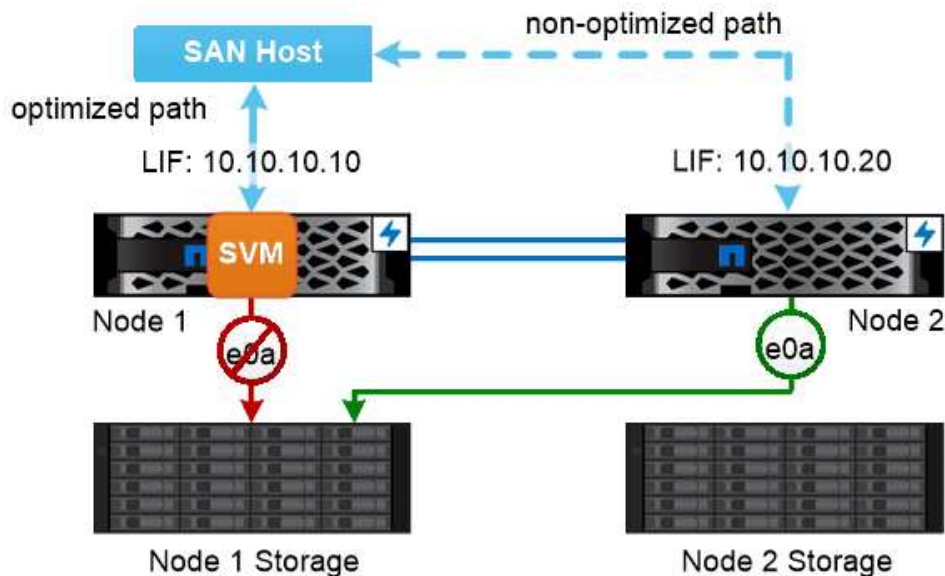
Un host SAN utilizza ALUA (Asymmetric Logical Unit Access) e MPIO (Multipath i/o) per

reindirizzare il traffico a una LIF sopravvissuta dopo un errore di collegamento. I percorsi predefiniti determinano i possibili percorsi verso il LUN serviti da SVM.

In un ambiente SAN, gli host sono considerati *iniziatori* di richieste a LUN *targets*. MPIO consente percorsi multipli dagli iniziatori alle destinazioni. ALUA identifica i percorsi più diretti, denominati *percorsi ottimizzati*.

In genere, si configurano più percorsi ottimizzati per le LIF sul nodo proprietario del LUN e più percorsi non ottimizzati per le LIF sul partner ha. In caso di guasto di una porta sul nodo proprietario, l'host instrada il traffico verso le porte sopravvissute. Se tutte le porte si guastano, l'host instrada il traffico sui percorsi non ottimizzati.

Per impostazione predefinita, la mappa LUN selettiva (SLM) di ONTAP limita il numero di percorsi dall'host a un LUN. Un LUN appena creato è accessibile solo attraverso i percorsi verso il nodo proprietario del LUN o del suo partner ha. È inoltre possibile limitare l'accesso a un LUN configurando i LIF in un *set di porte* per l'iniziatore.



*A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.*

### **spostamento di volumi in ambienti SAN**

Per impostazione predefinita, ONTAP *Selective LUN Map (SLM)* limita il numero di percorsi a un LUN da un host SAN. Un LUN appena creato è accessibile solo attraverso i percorsi al nodo proprietario del LUN o del suo partner ha, i *nodi di reporting* per il LUN.

Ciò significa che quando si sposta un volume in un nodo di un'altra coppia ha, è necessario aggiungere nodi di reporting per la coppia ha di destinazione alla mappatura LUN. È quindi possibile specificare i nuovi percorsi nella configurazione di MPIO. Una volta completato lo spostamento del volume, è possibile eliminare i nodi di reporting per la coppia ha di origine dalla mappatura.

## **Bilanciamento del carico**

Le performance dei carichi di lavoro iniziano ad essere influenzate dalla latenza quando la quantità di lavoro su un nodo supera le risorse disponibili. È possibile gestire un nodo sovraccarico aumentando le risorse disponibili (aggiornamento di dischi o CPU) o

riducendo il carico (spostamento di volumi o LUN in nodi diversi in base alle necessità).

È inoltre possibile utilizzare ONTAP *qualità del servizio (QoS) dello storage* per garantire che le performance dei carichi di lavoro critici non vengano degradate da carichi di lavoro concorrenti:

- È possibile impostare un *soffitto* di throughput QoS su un carico di lavoro concorrente per limitarne l'impatto sulle risorse di sistema (QoS Max).
- È possibile impostare un *floor* di throughput QoS per un carico di lavoro critico, garantendo che soddisfi gli obiettivi di throughput minimi indipendentemente dalla domanda mediante carichi di lavoro concorrenti (QoS min).
- È possibile impostare un tetto e un piano QoS per lo stesso carico di lavoro.

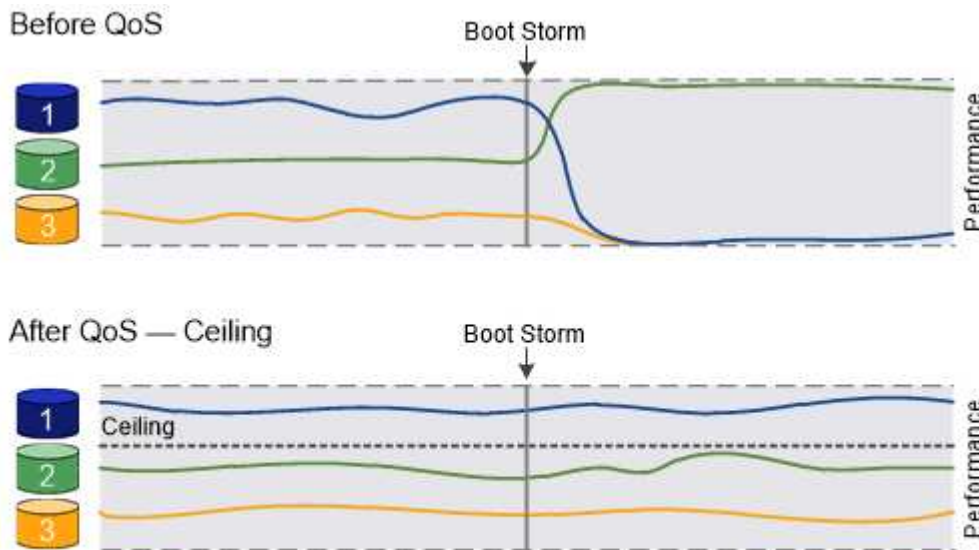
## Limiti di throughput

Un limite massimo di throughput limita il throughput per un carico di lavoro a un numero massimo di IOPS o MB/s. Nella figura seguente, il limite massimo di throughput per il carico di lavoro 2 garantisce che non vengano utilizzati i carichi di lavoro 1 e 3 "bully".

Un *gruppo di policy* definisce il limite massimo di throughput per uno o più carichi di lavoro. Un carico di lavoro rappresenta le operazioni di i/o per un *oggetto storage*: volume, file o LUN o tutti i volumi, file o LUN di una SVM. È possibile specificare il limite massimo quando si crea il gruppo di criteri oppure attendere che i carichi di lavoro vengano monitorati per specificarlo.



Il throughput per i carichi di lavoro potrebbe superare il limite massimo specificato fino al 10%, soprattutto se un carico di lavoro subisce rapidi cambiamenti nel throughput. Il limite massimo potrebbe essere superato fino al 50% per gestire i burst.



*The throughput ceiling for workload 2 ensures that it does not "bully" workloads 1 and 3.*

## Piani di throughput

Un piano di throughput garantisce che il throughput per un carico di lavoro non scenda al di sotto di un numero minimo di IOPS. Nella figura riportata di seguito, i livelli di throughput per il carico di lavoro 1 e il carico di lavoro 3 garantiscono il raggiungimento degli obiettivi di throughput minimi, indipendentemente dalla domanda



per carico di lavoro 2.

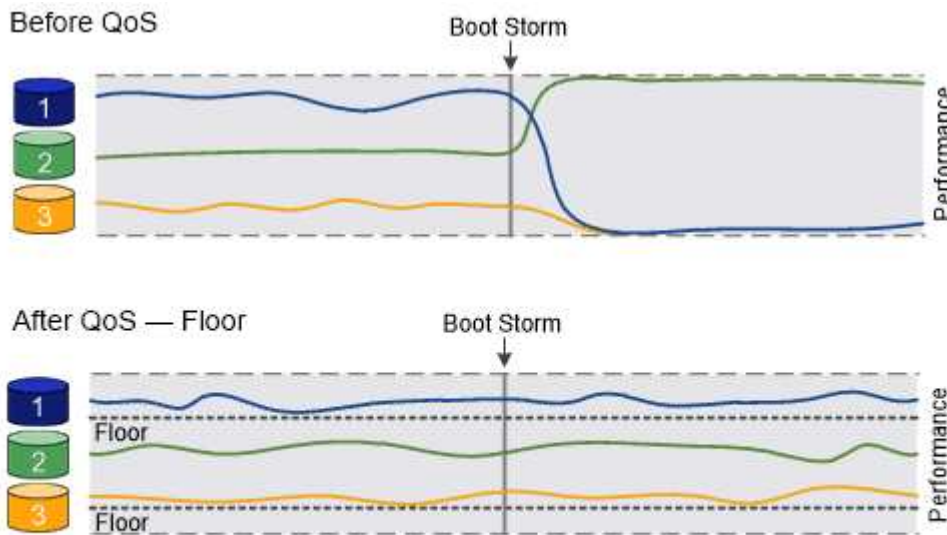


Come suggeriscono gli esempi, un limite di throughput rallenta direttamente il throughput. Un piano di throughput rallenta indirettamente il throughput, dando priorità ai carichi di lavoro per i quali è stato impostato il piano.

Un carico di lavoro rappresenta le operazioni di i/o di un volume, LUN o, a partire da ONTAP 9.3, file. Un gruppo di criteri che definisce un piano di throughput non può essere applicato a una SVM. È possibile specificare il piano di lavoro quando si crea il gruppo di policy oppure attendere fino a quando non si monitorano i carichi di lavoro per specificarlo.



Il throughput di un carico di lavoro potrebbe scendere al di sotto del piano specificato se la capacità delle performance (spazio di crescita) sul nodo o sull'aggregato è insufficiente o durante operazioni critiche come `volume move trigger-cutover`. Anche quando è disponibile una capacità sufficiente e non si svolgono operazioni critiche, il throughput di un workload potrebbe scendere al di sotto del piano specificato fino al 5%.



*The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.*

### QoS adattiva

Normalmente, il valore del gruppo di criteri assegnato a un oggetto di storage è fisso. È necessario modificare il valore manualmente quando la dimensione dell'oggetto di storage cambia. Un aumento della quantità di spazio utilizzata su un volume, ad esempio, richiede solitamente un aumento corrispondente del limite di throughput specificato per il volume.

QoS *adattiva* scala automaticamente il valore del gruppo di policy in base alle dimensioni del carico di lavoro, mantenendo il rapporto tra IOPS e TB|GB in base alle dimensioni del carico di lavoro. Si tratta di un vantaggio significativo quando si gestiscono centinaia o migliaia di carichi di lavoro in un'implementazione di grandi dimensioni.

In genere, si utilizza la QoS adattiva per regolare i limiti di throughput, ma è anche possibile utilizzarla per gestire i piani di throughput (quando le dimensioni del carico di lavoro aumentano). La dimensione del carico di lavoro viene espressa come spazio allocato per l'oggetto di storage o come spazio utilizzato dall'oggetto di storage.



Lo spazio utilizzato è disponibile per i piani di throughput in ONTAP 9.5 e versioni successive. Non è supportato per i piani di throughput in ONTAP 9.4 e versioni precedenti.

A partire da ONTAP 9.13.1, è possibile utilizzare la QoS adattiva per impostare i livelli e i limiti di throughput a livello di SVM.

- Una policy di *spazio allocato* mantiene il rapporto IOPS/TB|GB in base alle dimensioni nominali dell'oggetto di storage. Se il rapporto è di 100 IOPS/GB, un volume da 150 GB avrà un limite di throughput di 15,000 IOPS, a condizione che il volume rimanga tale. Se il volume viene ridimensionato a 300 GB, la QoS adattiva regola il limite di throughput a 30,000 IOPS.
- Una policy *used space* (predefinita) mantiene il rapporto IOPS/TB|GB in base alla quantità di dati effettivi memorizzati prima dell'efficienza dello storage. Se il rapporto è di 100 IOPS/GB, un volume da 150 GB con 100 GB di dati memorizzati avrebbe un limite massimo di throughput di 10,000 IOPS. Man mano che la quantità di spazio utilizzato cambia, la QoS adattiva regola il limite di throughput in base al rapporto.

## Replica

### Copie Snapshot

Tradizionalmente, le tecnologie di replica di ONTAP servivano per il disaster recovery (DR) e l'archiviazione dei dati. Con l'avvento dei servizi cloud, la replica di ONTAP è stata adattata al trasferimento dei dati tra endpoint nel data fabric NetApp. La base per tutti questi utilizzi è la tecnologia Snapshot di ONTAP.

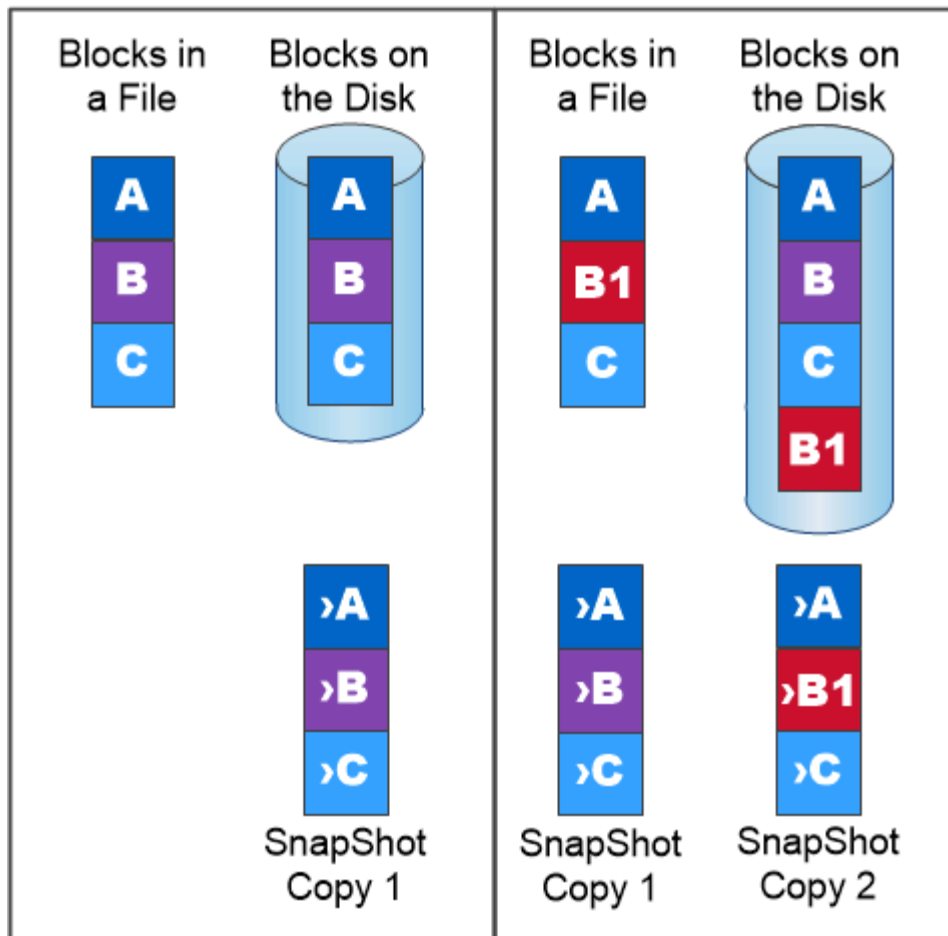
Una *copia Snapshot* è un'immagine point-in-time di sola lettura di un volume. Dopo aver creato una copia Snapshot, il file system attivo e la copia Snapshot puntano agli stessi blocchi di disco; pertanto, la copia Snapshot non utilizza spazio su disco aggiuntivo. Con il passare del tempo, l'immagine consuma uno spazio di storage minimo e subisce un overhead delle performance trascurabile in quanto registra solo le modifiche ai file dall'ultima copia Snapshot.

Le copie Snapshot devono la loro efficienza alla tecnologia di virtualizzazione dello storage di base di ONTAP, il suo *Write Anywhere file Layout (WAFL)*. come un database, WAFL utilizza i metadati per puntare ai blocchi di dati effettivi sul disco. Tuttavia, a differenza di un database, WAFL non sovrascrive i blocchi esistenti. Scrive i dati aggiornati in un nuovo blocco e cambia i metadati.

Le copie Snapshot sono efficienti perché, al contrario, vengono utilizzati blocchi di dati di copia, mentre ONTAP fa riferimento ai metadati durante la creazione di una copia Snapshot. In questo modo si eliminano sia il tempo di ricerca che altri sistemi incorrono nell'individuazione dei blocchi da copiare, sia il costo della copia stessa.

È possibile utilizzare una copia Snapshot per ripristinare singoli file o LUN o per ripristinare l'intero contenuto di un volume. ONTAP confronta le informazioni del puntatore nella copia Snapshot con i dati su disco per ricostruire l'oggetto mancante o danneggiato, senza downtime o costi di performance significativi.

Una *policy Snapshot* definisce il modo in cui il sistema crea le copie Snapshot dei volumi. Il criterio specifica quando creare le copie Snapshot, quante copie conservare, come assegnarle un nome e come etichettarle per la replica. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti, chiamarle "daily" (con data e ora) ed etichettarle "daily" per la replica.



*A SnapShot copy records only changes to the active file system since the last SnapShot copy.*

#### Disaster recovery e trasferimento dei dati SnapMirror

*SnapMirror* è una tecnologia di disaster recovery progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. Come suggerisce il nome, SnapMirror crea una replica, o *mirror*, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di disastro nel sito primario.

I dati vengono mirrorati a livello di volume. La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene chiamata *relazione di protezione dei dati*. I cluster in cui risiedono i volumi e le SVM che servono i dati dei volumi devono essere *peering*. Una relazione peer consente lo scambio di cluster e SVM dati in modo sicuro.



È inoltre possibile creare una relazione di protezione dei dati tra le SVM. In questo tipo di relazione, viene replicata tutta o parte della configurazione di SVM, dalle esportazioni NFS e dalle condivisioni SMB a RBAC, nonché i dati nei volumi di proprietà di SVM.

A partire da ONTAP 9.10.1, è possibile creare relazioni di protezione dei dati tra i bucket S3 utilizzando S3 SnapMirror. I bucket di destinazione possono essere su sistemi ONTAP locali o remoti o su sistemi non ONTAP come StorageGRID e AWS.



La prima volta che si richiama SnapMirror, esegue un *trasferimento baseline* dal volume di origine al volume di destinazione. Il trasferimento della linea di base in genere prevede i seguenti passaggi:

- Creare una copia Snapshot del volume di origine.
- Trasferire la copia Snapshot e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.
- Trasferire le copie Snapshot rimanenti, meno recenti, sul volume di origine al volume di destinazione per l'utilizzo in caso di danneggiamento del mirror "Active".

Una volta completato il trasferimento di riferimento, SnapMirror trasferisce solo le nuove copie Snapshot nel mirror. Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. La conservazione rispecchia la policy Snapshot sull'origine. È possibile attivare il volume di destinazione con interruzioni minime in caso di disastro nel sito primario e riattivare il volume di origine quando il servizio viene ripristinato.

Poiché SnapMirror trasferisce solo le copie Snapshot dopo la creazione della linea di base, la replica è rapida e senza interruzioni. Come implica il caso di utilizzo del failover, i controller sul sistema secondario devono essere equivalenti o quasi equivalenti ai controller sul sistema primario per fornire i dati in modo efficiente dallo storage mirrorato.



*A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.*

#### **utilizzo di SnapMirror per il trasferimento dei dati**

È inoltre possibile utilizzare SnapMirror per replicare i dati tra endpoint nel data fabric NetApp. Quando si crea il criterio SnapMirror, è possibile scegliere tra replica singola o ricorrente.

#### **Backup di SnapMirror Cloud nello storage a oggetti**

*SnapMirror Cloud* è una tecnologia di backup e recovery progettata per gli utenti ONTAP che desiderano trasferire i propri flussi di lavoro di data Protection nel cloud. Le organizzazioni che si allontanano dalle architetture di backup su nastro legacy possono utilizzare lo storage a oggetti come repository alternativo per la conservazione e l'archiviazione dei dati a lungo termine. SnapMirror Cloud offre la replica dello storage

## ONTAP-to-object come parte di una strategia di backup incrementale per sempre.

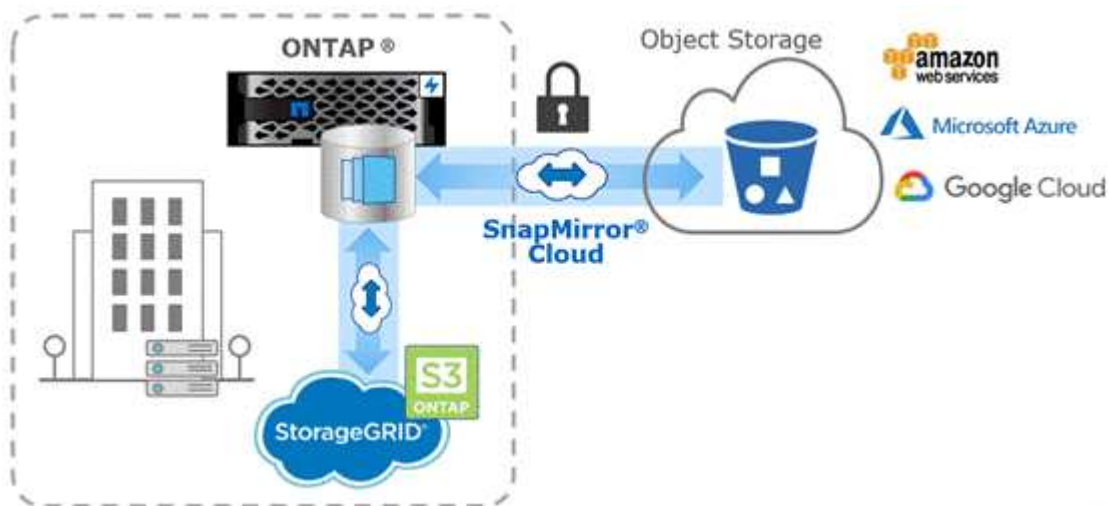
SnapMirror Cloud è stato introdotto in ONTAP 9.8 come estensione della famiglia di tecnologie di replica SnapMirror. Mentre SnapMirror viene spesso utilizzato per i backup da ONTAP a ONTAP, SnapMirror Cloud utilizza lo stesso motore di replica per trasferire le copie Snapshot per ONTAP ai backup dello storage a oggetti compatibili con S3.

Destinato ai casi di utilizzo del backup, SnapMirror Cloud supporta sia la conservazione a lungo termine che i flussi di lavoro di archiviazione. Come per SnapMirror, il backup iniziale di SnapMirror Cloud esegue un trasferimento di riferimento di un volume. Per i backup successivi, SnapMirror Cloud genera una copia snapshot del volume di origine e trasferisce la copia snapshot con solo i blocchi di dati modificati a una destinazione di storage a oggetti.

Le relazioni cloud di SnapMirror possono essere configurate tra sistemi ONTAP e destinazioni di storage a oggetti on-premise e cloud pubblico selezionate, tra cui Amazon S3, Google Cloud Storage e Microsoft Azure Blob Storage. Ulteriori destinazioni di storage a oggetti on-premise includono StorageGRID e ONTAP S3.

La replica cloud di SnapMirror è una funzionalità ONTAP concessa in licenza e richiede un'applicazione approvata per orchestrare i flussi di lavoro di protezione dei dati. Sono disponibili diverse opzioni di orchestrazione per la gestione dei backup di SnapMirror Cloud:

- Diversi partner di backup di terze parti che offrono supporto per la replica di SnapMirror Cloud. I vendor partecipanti sono disponibili su ["Blog di NetApp"](#).
- Backup e ripristino BlueXP per una soluzione nativa NetApp per ambienti ONTAP
- API per lo sviluppo di software personalizzato per i flussi di lavoro di data Protection o l'utilizzo di strumenti di automazione



### Archiviazione SnapVault

La licenza SnapMirror viene utilizzata per supportare le relazioni SnapVault per il backup e le relazioni SnapMirror per il disaster recovery. A partire da ONTAP 9,3, le licenze SnapVault sono obsolete e le licenze SnapMirror possono essere utilizzate per configurare relazioni di vault, mirror e mirror-and-vault. La replica di SnapMirror viene utilizzata per la replica da ONTAP a ONTAP delle copie Snapshot, supportando i casi di utilizzo di backup e disaster recovery.

*SnapVault* è una tecnologia di archiviazione, progettata per la replica delle copie Snapshot disk-to-disk per la

conformità agli standard e altri scopi correlati alla governance. A differenza di una relazione SnapMirror, in cui la destinazione contiene di solito solo le copie Snapshot attualmente nel volume di origine, una destinazione SnapVault conserva in genere le copie Snapshot point-in-time create in un periodo molto più lungo.

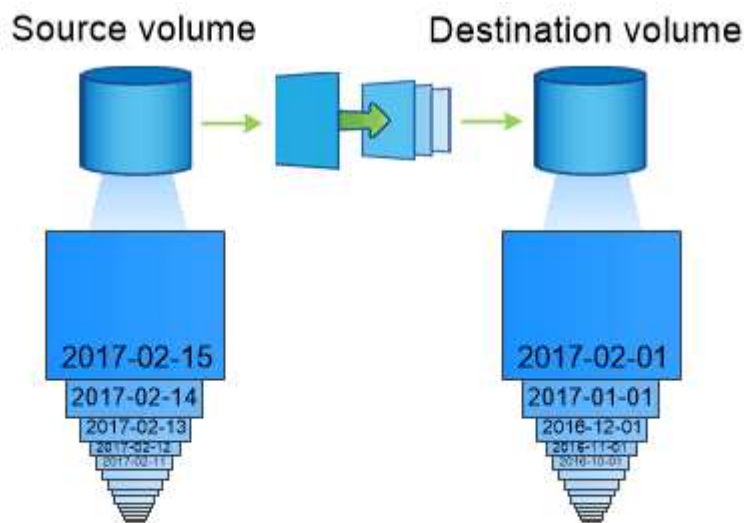
È possibile conservare copie Snapshot mensili dei dati per un periodo di 20 anni, ad esempio per rispettare le normative contabili governative per la propria azienda. Poiché non è necessario fornire dati dallo storage del vault, è possibile utilizzare dischi più lenti e meno costosi sul sistema di destinazione.

Come con SnapMirror, SnapVault esegue un trasferimento di riferimento la prima volta che lo si richiama. Esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e i blocchi di dati a cui fa riferimento al volume di destinazione. A differenza di SnapMirror, SnapVault non include copie Snapshot precedenti nella linea di base.

Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. Le regole definite nella policy per la relazione identificano quali nuove copie Snapshot includere negli aggiornamenti e quante copie conservare. Le etichette definite nella policy ("monthly," ad esempio) devono corrispondere a una o più etichette definite nella policy Snapshot sull'origine. In caso contrario, la replica non riesce.



SnapMirror e SnapVault condividono la stessa infrastruttura di comando. Specificare il metodo da utilizzare per la creazione di un criterio. Entrambi i metodi richiedono cluster peered e SVM peered.



*A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.*

### Backup nel cloud e supporto per backup tradizionali

Oltre alle relazioni di protezione dei dati SnapMirror e SnapVault, che erano disk-to-disk solo per ONTAP 9,7 e versioni precedenti, oggi esistono diverse soluzioni di backup che offrono un'alternativa meno costosa per la conservazione dei dati a lungo termine.

Numerose applicazioni di protezione dei dati di terze parti offrono il backup tradizionale per i dati gestiti da ONTAP. Veeam, Veritas e CommVault, tra gli altri, offrono backup integrato per i sistemi ONTAP.

A partire da ONTAP 9.8, SnapMirror Cloud offre la replica asincrona delle copie Snapshot dalle istanze di

ONTAP agli endpoint dello storage a oggetti. La replica di SnapMirror Cloud richiede un'applicazione con licenza per l'orchestrazione e la gestione dei flussi di lavoro per la protezione dei dati. Le relazioni cloud di SnapMirror sono supportate dai sistemi ONTAP per selezionare obiettivi di storage a oggetti per il cloud pubblico e on-premise, tra cui AWS S3, la piattaforma di storage cloud di Google o lo storage Blob di Microsoft Azure, che offrono una maggiore efficienza con il software di backup del vendor. Contatta il tuo rappresentante NetApp per un elenco delle applicazioni certificate supportate e dei vendor di storage a oggetti.

Se sei interessato alla protezione dei dati nativa del cloud, BlueXP può essere utilizzato per configurare le relazioni di SnapMirror o SnapVault tra volumi on-premise e istanze di Cloud Volumes ONTAP nel cloud pubblico.

BlueXP fornisce inoltre backup delle istanze di Cloud Volumes ONTAP utilizzando un modello SaaS (Software as a Service). Gli utenti possono eseguire il backup delle istanze di Cloud Volumes ONTAP su storage a oggetti cloud pubblico compatibile con S3 e S3 utilizzando il backup cloud disponibile su NetApp Cloud Central.

["Risorse per la documentazione di Cloud Volumes ONTAP e BlueXP"](#)

["NetApp Cloud Central"](#)

### **Disponibilità continua di MetroCluster**

Le configurazioni MetroCluster proteggono i dati implementando due cluster fisicamente separati con mirroring. Ciascun cluster replica in modo sincrono i dati e la configurazione SVM dell'altro. In caso di disastro in un sito, un amministratore può attivare la SVM mirrorata e iniziare a fornire i dati dal sito sopravvissuto.

- Le configurazioni *Fabric-attached MetroCluster* supportano cluster a livello metropolitano.
- Le configurazioni *stretch MetroCluster* supportano cluster a livello di campus.

In entrambi i casi, i cluster devono essere peering.

MetroCluster utilizza una funzionalità di ONTAP denominata *SyncMirror* per eseguire il mirroring sincrono dei dati aggregati per ciascun cluster nelle copie, o *plex*, nello storage dell'altro cluster. Se si verifica uno switchover, il plex remoto sul cluster in uso viene online e la SVM secondaria inizia a fornire i dati.



*When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.*

**utilizzo di SyncMirror in implementazioni non MetroCluster** è possibile utilizzare SyncMirror in un'implementazione non MetroCluster per proteggere dalla perdita di dati in caso di guasti di più dischi rispetto a quelli protetti dal tipo RAID o in caso di perdita di connettività ai dischi del gruppo RAID. La funzione è disponibile solo per le coppie ha.

I dati aggregati vengono mirrorati in plessi memorizzati su diversi shelf di dischi. Se uno degli shelf non è disponibile, il plesso non interessato continua a fornire dati mentre si corregge la causa del guasto.

Tenere presente che un aggregato mirrorato utilizzando SyncMirror richiede il doppio dello storage rispetto a un aggregato senza mirror. Ogni plex richiede un numero di dischi pari a quello del plex che esegue il mirroring. Per eseguire il mirroring di un aggregato da 1,440 GB, ad esempio 1,440 GB per ciascun plex, sono necessari 2,880 GB di spazio su disco.

Con SyncMirror, si consiglia di mantenere almeno il 20% di spazio libero per gli aggregati con mirroring, per ottenere performance e disponibilità dello storage ottimali. Sebbene il suggerimento sia del 10% per gli aggregati non speculari, il 10% di spazio aggiuntivo può essere utilizzato dal filesystem per assorbire le modifiche incrementali. I cambiamenti incrementali aumentano l'utilizzo dello spazio per gli aggregati con mirroring grazie all'architettura copy-on-write basata su Snapshot di ONTAP. Il mancato rispetto di queste Best practice può avere un impatto negativo sulle performance di risincronizzazione del SyncMirror, che influisce indirettamente sui flussi di lavoro operativi come NDU per le implementazioni di cloud non condivisi e lo switchback per le implementazioni di MetroCluster.



SyncMirror è disponibile anche per le implementazioni della virtualizzazione FlexArray.

## Efficienza dello storage

### Panoramica dell'efficienza dello storage di ONTAP

L'efficienza dello storage misura la efficacia con cui un sistema storage utilizza lo spazio disponibile ottimizzando le risorse di storage, riducendo lo spazio sprecato e riducendo l'impatto fisico dei dati scritti. Una maggiore efficienza dello storage consente di memorizzare la quantità massima di dati nel minor spazio possibile al minor costo possibile. Ad esempio, utilizzando tecnologie per l'efficienza dello storage che rilevano ed eliminano blocchi di dati duplicati e blocchi di dati pieni di zero, si riduce la quantità complessiva di storage fisico necessario e si riduce il costo complessivo.

ONTAP offre una vasta gamma di tecnologie per l'efficienza dello storage che riducono la quantità di hardware fisico o di cloud storage consumato dai dati e che forniscono anche miglioramenti significativi alle performance di sistema, tra cui letture dei dati più rapide, copie dei set di dati più rapide e un provisioning più rapido delle macchine virtuali.

**Le tecnologie per l'efficienza dello storage di ONTAP includono:**

- **Thin provisioning**

**Thin provisioning** Consente di allocare lo storage in un volume o LUN in base alle necessità, anziché riservarlo in anticipo. Questo riduce la quantità di storage fisico necessario consentendo di allocare in eccesso i volumi o le LUN in base a un potenziale utilizzo, senza riservare spazio non attualmente in uso.

- **Deduplica**

**Deduplica** riduce la quantità di storage fisico necessaria per un volume in tre modi distinti.



- **Deduplicazione a blocchi zero**

La deduplica zero block rileva ed elimina i blocchi di dati riempiti con tutti gli zero e aggiorna solo i metadati. Viene quindi salvato il 100% dello spazio tipicamente utilizzato dai blocchi zero. La deduplica zero block è abilitata per impostazione predefinita su tutti i volumi deduplicati.

- **Deduplicazione inline**

La deduplica inline rileva i blocchi di dati duplicati e li sostituisce con dei riferimenti a un blocco condiviso univoco prima che i dati vengano scritti sul disco. La deduplica inline accelera il provisioning delle macchine virtuali del 20-30%. A seconda della versione di ONTAP in uso e della piattaforma in uso, la deduplica inline è disponibile a livello di volume o aggregato. È abilitato per impostazione predefinita nei sistemi AFF e ASA. È necessario abilitare manualmente la deduplica inline su sistemi FAS.

- **Deduplicazione in background**

La deduplica in background rileva anche i blocchi di dati duplicati e li sostituisce con dei riferimenti a un blocco condiviso unico, ma migliora ulteriormente l'efficienza dello storage dopo che i dati sono stati scritti sul disco. È possibile impostare la deduplica in background in modo che venga eseguita quando vengono soddisfatti determinati criteri sul sistema di storage. Ad esempio, è possibile abilitare la deduplica in background quando il volume raggiunge un utilizzo del 10%. È inoltre possibile attivare manualmente la deduplica in background o impostarla per l'esecuzione su una pianificazione specifica. È abilitato per impostazione predefinita nei sistemi AFF e ASA. È necessario abilitare manualmente la deduplica in background sui sistemi FAS.

La deduplica è supportata sia all'interno dei volumi che tra i volumi di un aggregato. Le letture dei dati deduplicati non comportano in genere alcun costo per le prestazioni.

- **Compressione**

**Compressione** riduce la quantità di storage fisico necessaria per un volume combinando blocchi di dati in gruppi di compressione, ciascuno dei quali viene memorizzato come un singolo blocco. Quando viene ricevuta una richiesta di lettura o sovrascrittura, viene letto solo un piccolo gruppo di blocchi, non l'intero file. Questo processo ottimizza le prestazioni di lettura e sovrascrittura e consente una maggiore scalabilità nelle dimensioni dei file compressi.

La compressione può essere eseguita inline o post-process. La compressione inline genera risparmi di spazio immediati grazie alla compressione dei dati in memoria prima che vengano scritti sul disco. La compressione post-elaborazione scrive prima i blocchi su disco come non compressi, quindi, in un momento pianificato, comprime i dati. È necessario attivare manualmente la compressione.

- **Compattazione**

La tecnologia di compaction riduce la quantità di storage fisico richiesta per un volume prelevando porzioni di dati memorizzate in blocchi da 4 KB, ma di dimensioni inferiori a 4 KB e combinandole in un singolo blocco. La tecnologia di compaction avviene mentre i dati sono ancora in memoria, in modo da non consumare spazio non necessario sui dischi. È abilitato per impostazione predefinita nei sistemi AFF e ASA. Devi attivare manualmente la compaction sui sistemi FAS.

- **Volumi, file e LUN di FlexClone**

**Tecnologia FlexClone** Sfrutta i metadati Snapshot per creare copie scrivibili point-in-time di un volume, file o LUN. Le copie condividono i blocchi di dati con i genitori, senza consumare storage tranne ciò che è necessario per i metadati fino a quando le modifiche non vengono scritte in una copia o nella relativa copia

padre. Quando viene scritta una modifica, viene memorizzato solo il delta.

Se le copie tradizionali dei set di dati richiedono pochi minuti o anche ore per la creazione, la tecnologia FlexClone consente di copiare quasi istantaneamente anche i set di dati più estesi.

- **Efficienza di stoccaggio sensibile alla temperatura**

ONTAP offre "efficienza dello storage sensibile alla temperatura" i vantaggi, valutando la frequenza di accesso ai dati del volume ed eseguendo la mappatura di tale frequenza al grado di compressione applicato a tali dati. Per i dati cold a cui si accede raramente, i blocchi di dati più grandi vengono compressi, mentre per i dati hot, a cui si accede frequentemente e che vengono sovrascritti più spesso, i blocchi di dati più piccoli vengono compressi, rendendo il processo più efficiente.

L'efficienza dello storage sensibile alla temperatura (TSSE) viene introdotta in ONTAP 9.8 e attivata automaticamente sui volumi AFF appena creati con thin provisioning.

Puoi realizzare il vantaggio di queste tecnologie nelle tue operazioni quotidiane con il minimo sforzo. Ad esempio, si supponga di dover fornire a 5.000 utenti lo spazio di archiviazione per le home directory e si stimi che lo spazio massimo necessario a qualsiasi utente sia di 1 GB. È possibile riservare in anticipo un aggregato da 5 TB per soddisfare la potenziale esigenza di storage totale. Tuttavia, è anche noto che i requisiti di capacità delle home directory variano notevolmente a seconda dell'organizzazione. Invece di riservare 5 TB di spazio totale all'organizzazione, è possibile creare un aggregato da 2 TB. Quindi è possibile utilizzare il thin provisioning per assegnare nominalmente 1 GB di storage a ciascun utente, ma allocare lo storage solo in base alle necessità. È possibile monitorare attivamente l'aggregato nel tempo e aumentare le dimensioni fisiche effettive in base alle necessità.

Un altro esempio potrebbe essere l'utilizzo di una VDI (Virtual Desktop Infrastructure) con una grande quantità di dati duplicati tra i virtual desktop. La deduplica riduce l'utilizzo dello storage eliminando automaticamente i blocchi di informazioni duplicati nell'infrastruttura di desktop virtuale, sostituendoli con un puntatore al blocco originale. Altre tecnologie per l'efficienza dello storage di ONTAP, come la compressione, possono essere eseguite in background senza alcun intervento da parte dell'utente.

La tecnologia di partizione dei dischi di ONTAP offre anche una maggiore efficienza dello storage. La tecnologia RAID DP protegge da guasti a due unità disco senza sacrificare le prestazioni o aggiungere overhead del mirroring del disco. La partizione avanzata dei dischi a stato solido con ONTAP 9 aumenta la capacità utilizzabile di quasi il 20%.

NetApp offre le stesse funzionalità di efficienza dello storage disponibili con ONTAP on-premise nel cloud. Durante la migrazione dei dati da ONTAP on-premise al cloud, l'efficienza dello storage esistente viene preservata. Ad esempio, supponiamo di disporre di un database SQL contenente dati business-critical da spostare da un sistema on-premise nel cloud. Puoi utilizzare la replica dei dati in BlueXP per migrare i tuoi dati e, come parte del processo di migrazione, puoi abilitare la tua policy on-premise più recente per le copie Snapshot nel cloud.

## **Thin provisioning**

ONTAP offre un'ampia gamma di tecnologie per l'efficienza dello storage oltre alle copie Snapshot. Le tecnologie chiave includono thin provisioning, deduplica, compressione e volumi FlexClone, file, E LUN. Come le copie Snapshot, tutte sono basate sul layout di file Write Anywhere (WAFL) di ONTAP.

Un volume o LUN *con thin provisioning* è un volume per il quale lo storage non è riservato in anticipo. Invece, lo storage viene allocato in modo dinamico, in base alle esigenze. Lo spazio libero viene nuovamente rilasciato nel sistema di storage quando i dati nel volume o nel LUN vengono cancellati.



Supponiamo che la tua organizzazione debba fornire a 5,000 utenti lo storage per le home directory. Si stima che le home directory più grandi consumeranno 1 GB di spazio.

In questa situazione, è possibile acquistare 5 TB di storage fisico. Per ogni volume che memorizza una home directory, si dovrebbe riservare spazio sufficiente per soddisfare le esigenze dei consumatori più grandi.

Tuttavia, come aspetto pratico, sai anche che i requisiti di capacità della home directory variano notevolmente in tutta la community. Per ogni grande utente dello storage, sono dieci i clienti che consumano poco o niente spazio.

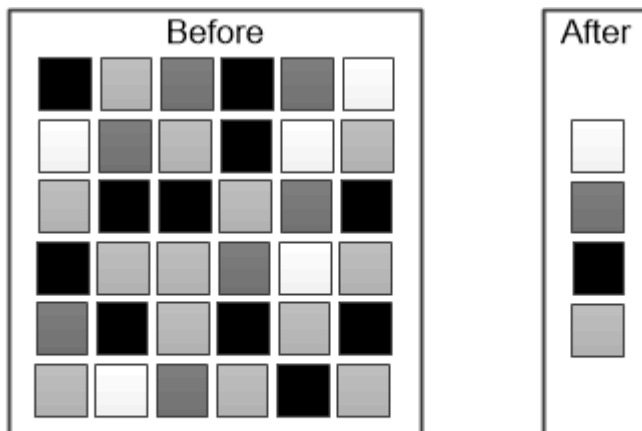
Il thin provisioning ti consente di soddisfare le esigenze dei grandi consumatori di storage senza dover acquistare storage che potresti non utilizzare mai. Poiché lo spazio di storage non viene allocato fino a quando non viene consumato, è possibile “assegnare in eccesso” un aggregato di 2 TB assegnando nominalmente una dimensione di 1 GB a ciascuno dei 5,000 volumi contenuti nell’aggregato.

Se hai ragione, il rapporto tra utenti leggeri e utenti pesanti è di 10:1 e se assumi un ruolo attivo nel monitoraggio dello spazio libero sull’aggregato, puoi essere sicuro che le scritture dei volumi non falliscono a causa della mancanza di spazio.

## Deduplica

*Deduplica* riduce la quantità di storage fisico richiesta per un volume (o per tutti i volumi in un aggregato AFF) eliminando i blocchi duplicati e sostituendoli con riferimenti a un singolo blocco condiviso. Le letture dei dati deduplicati non comportano in genere alcun costo per le prestazioni. Le scritture comportano un costo trascurabile, tranne che per i nodi sovraccarichi.

Quando i dati vengono scritti durante il normale utilizzo, WAFL utilizza un processo batch per creare un catalogo di *firme a blocchi*. dopo l’avvio della deduplica, ONTAP confronta le firme nel catalogo per identificare i blocchi duplicati. Se esiste una corrispondenza, viene eseguito un confronto byte per byte per verificare che i blocchi candidati non siano stati modificati dalla creazione del catalogo. Solo se tutti i byte corrispondono, il blocco duplicato viene scartato e il relativo spazio su disco viene recuperato.



*Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.*

## Compressione

*Compressione* riduce la quantità di storage fisico richiesta per un volume combinando i

blocchi di dati in *gruppi di compressione*, ciascuno dei quali viene memorizzato come un singolo blocco. Le letture dei dati compressi sono più veloci rispetto ai metodi di compressione tradizionali, poiché ONTAP decompime solo i gruppi di compressione che contengono i dati richiesti, non un intero file o LUN.

È possibile eseguire la compressione inline o post-processo, separatamente o in combinazione:

- *Compressione inline* comprime i dati in memoria prima che vengano scritti su disco, riducendo significativamente la quantità di i/o di scrittura su un volume, ma potenzialmente degradando le prestazioni di scrittura. Le operazioni che richiedono prestazioni elevate vengono posticipate fino alla successiva operazione di compressione post-processo, se presente.
- *Compressione post-processo* comprime i dati dopo la scrittura su disco, secondo la stessa pianificazione della deduplica.

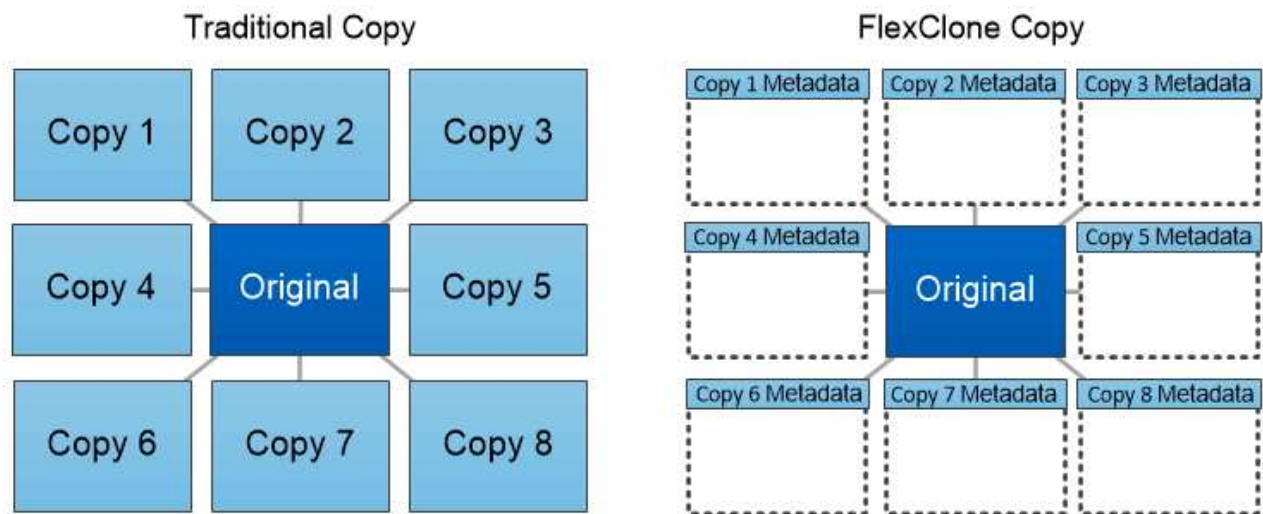
***Inline data compaction*** i file di piccole dimensioni o i/o con zeri vengono memorizzati in un blocco di 4 KB, indipendentemente dal fatto che richiedano o meno 4 KB di storage fisico. *Inline data compaction* combina blocchi di dati che normalmente consumerebbero più blocchi da 4 KB in un singolo blocco da 4 KB su disco. La compattazione avviene quando i dati sono ancora in memoria, quindi è più adatta ai controller più veloci.

## Volumi, file e LUN FlexClone

La tecnologia *FlexClone* fa riferimento ai metadati Snapshot per creare copie scrivibili point-in-time di un volume. Le copie condividono i blocchi di dati con i genitori, senza consumare storage, ad eccezione di quanto richiesto per i metadati fino a quando le modifiche non vengono scritte nella copia. I file FlexClone e le LUN FlexClone utilizzano una tecnologia identica, tranne per il fatto che non è necessaria una copia Snapshot di backup.

Il software FlexClone consente di copiare quasi istantaneamente anche i set di dati più grandi, anche se le copie tradizionali richiedono pochi minuti o persino ore. Ciò lo rende ideale per le situazioni in cui sono necessarie più copie di set di dati identici (ad esempio, un'implementazione di desktop virtuale) o copie temporanee di un set di dati (test di un'applicazione rispetto a un set di dati di produzione).

È possibile clonare un volume FlexClone esistente, clonare un volume contenente cloni LUN o clonare dati di mirroring e vault. È possibile *separare* un volume FlexClone dal relativo volume padre, nel qual caso la copia viene allocata al proprio storage.



*FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.*

### Misurazioni della capacità in System Manager

La capacità del sistema può essere misurata come spazio fisico o spazio logico. A partire da ONTAP 9.7, System Manager fornisce misurazioni della capacità fisica e logica.

Le differenze tra le due misurazioni sono spiegate nelle seguenti descrizioni:

- **Capacità fisica:** Lo spazio fisico si riferisce ai blocchi fisici di storage utilizzati nel volume o nel Tier locale. Il valore della capacità fisica utilizzata è in genere inferiore al valore della capacità logica utilizzata a causa della riduzione dei dati dalle funzionalità di efficienza dello storage (come deduplica e compressione).
- **Capacità logica:** Lo spazio logico si riferisce allo spazio utilizzabile (i blocchi logici) in un volume o in un Tier locale. Lo spazio logico si riferisce al modo in cui lo spazio teorico può essere utilizzato, senza tenere conto dei risultati della deduplica o della compressione. Il valore dello spazio logico utilizzato deriva dalla quantità di spazio fisico utilizzato e dai risparmi derivanti dalle funzionalità di efficienza dello storage (come deduplica e compressione) configurate. Questa misurazione appare spesso più grande della capacità fisica utilizzata perché include copie Snapshot, cloni e altri componenti e non riflette la compressione dei dati e altre riduzioni dello spazio fisico. Pertanto, la capacità logica totale potrebbe essere superiore allo spazio fornito.



In System Manager, le rappresentazioni della capacità non tengono conto delle capacità del Tier storage root (aggregato).

### Misurazioni della capacità utilizzata

Le misurazioni della capacità utilizzata vengono visualizzate in modo diverso a seconda della versione di System Manager in uso, come illustrato nella seguente tabella:

Versione di System Manager	Termine utilizzato per la capacità	Tipo di capacità a cui si fa riferimento
----------------------------	------------------------------------	--

9.9.1 e versioni successive	Logica utilizzata	Spazio logico utilizzato se sono state attivate le impostazioni di efficienza dello storage)
9.7 e 9.8	Utilizzato	Spazio logico utilizzato (se sono state attivate le impostazioni di efficienza dello storage)
9.5 e 9.6 (visualizzazione classica)	Utilizzato	Spazio fisico utilizzato

### Termini di misurazione della capacità

Quando si descrive la capacità, vengono utilizzati i seguenti termini:

- **Capacità allocata:** Quantità di spazio allocato per i volumi in una VM di storage.
- **Available:** La quantità di spazio fisico disponibile per memorizzare i dati o per eseguire il provisioning dei volumi in una VM di storage o su un Tier locale.
- **Capacità tra volumi:** La somma dello storage utilizzato e dello storage disponibile di tutti i volumi su una VM di storage.
- **Dati del client:** Quantità di spazio utilizzata dai dati del client (fisici o logici).
  - A partire da ONTAP 9.13.1, la capacità utilizzata dai dati del client viene definita **uso logico** e la capacità utilizzata dalle copie Snapshot viene visualizzata separatamente.
  - In ONTAP 9.12.1 e versioni precedenti, la capacità utilizzata dai dati del client aggiunta alla capacità utilizzata dalle copie Snapshot viene definita **logica utilizzata**.
- **Impegnato:** Quantità di capacità impegnata per un Tier locale.
- **Riduzione dei dati:**
  - A partire da ONTAP 9.13.1, i rapporti di riduzione dei dati vengono visualizzati come segue:
    - Il valore di riduzione dei dati visualizzato sul pannello **Capacity** è il rapporto tra lo spazio logico utilizzato e lo spazio fisico utilizzato senza considerare le riduzioni significative ottenute utilizzando le funzionalità di efficienza dello storage, come le copie Snapshot.
    - Quando si visualizza il pannello dei dettagli, vengono visualizzati sia il rapporto visualizzato nel pannello di panoramica che il rapporto complessivo di tutto lo spazio logico utilizzato rispetto allo spazio fisico utilizzato. Definito **con copie Snapshot**, questo valore include i benefici derivanti dall'utilizzo di copie Snapshot e altre funzionalità di efficienza dello storage.
  - In ONTAP 9.12.1 e versioni precedenti, i rapporti di riduzione dei dati vengono visualizzati come segue:
    - Il valore di riduzione dei dati visualizzato sul pannello **Capacity** è il rapporto complessivo di tutto lo spazio logico utilizzato rispetto allo spazio fisico utilizzato e include i benefici derivanti dall'utilizzo di copie Snapshot e altre funzionalità di efficienza dello storage.
    - Quando si visualizza il pannello dei dettagli, vengono visualizzati il rapporto **complessivo** visualizzato nel pannello di panoramica e il rapporto dello spazio logico utilizzato solo dai dati del client rispetto allo spazio fisico utilizzato solo dai dati del client, denominato **senza copie Snapshot e cloni**.
- **Logica utilizzata:**
  - A partire da ONTAP 9.13.1, la capacità utilizzata dai dati del client viene definita **uso logico** e la

capacità utilizzata dalle copie Snapshot viene visualizzata separatamente.

- In ONTAP 9.12.1 e versioni precedenti, la capacità utilizzata dai dati client aggiunti alla capacità utilizzata dalle copie Snapshot viene definita **logica utilizzata**.

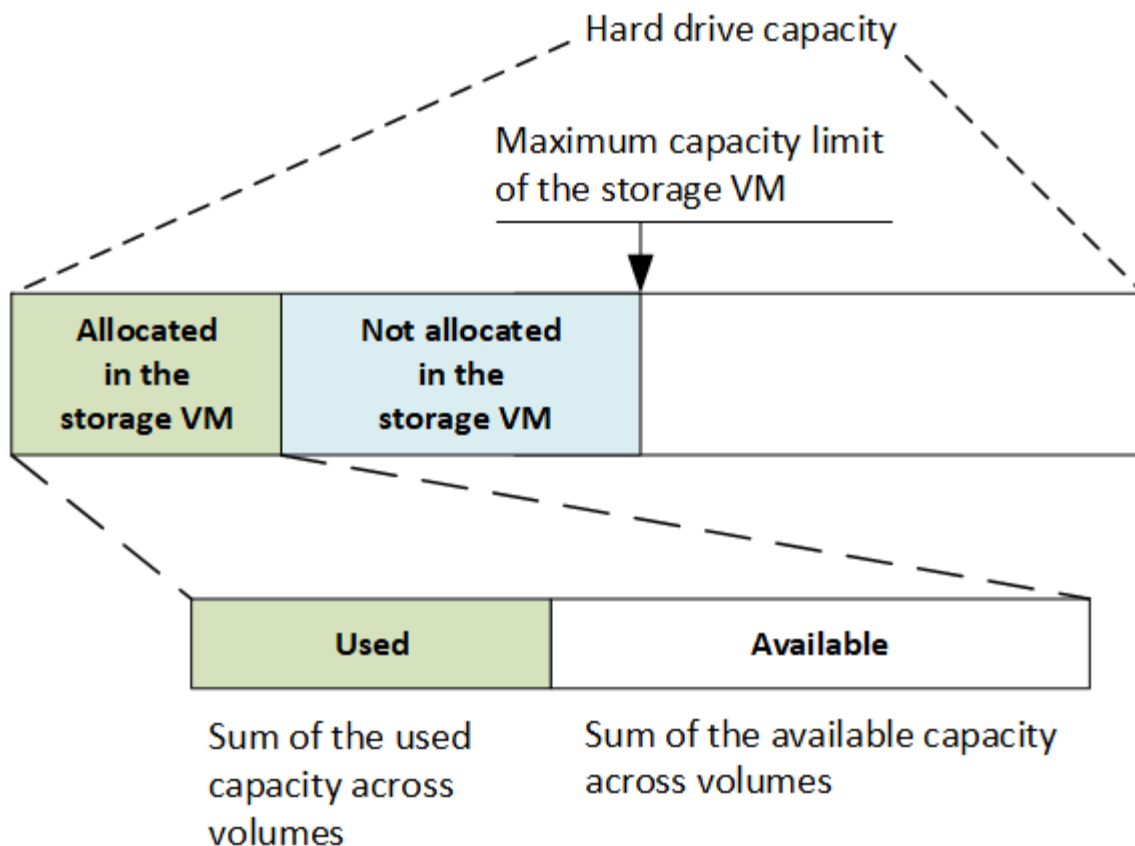
- **Logical used %**: Percentuale della capacità logica utilizzata corrente rispetto alle dimensioni fornite, escluse le riserve Snapshot. Questo valore può essere superiore al 100%, perché include risparmi di efficienza nel volume.
- **Capacità massima**: Quantità massima di spazio allocato per i volumi su una VM di storage.
- **Fisico utilizzato**: La quantità di capacità utilizzata nei blocchi fisici di un volume o di un Tier locale.
- **Physical used %**: Percentuale di capacità utilizzata nei blocchi fisici di un volume rispetto alle dimensioni del provisioning.
- **Capacità di provisioning**: Un file system (volume) allocato da un sistema Cloud Volumes ONTAP ed pronto per l'archiviazione dei dati dell'utente o dell'applicazione.
- **Reserved**: Quantità di spazio riservato ai volumi già sottoposti a provisioning in un Tier locale.
- **Used**: Quantità di spazio che contiene dati.
- **Utilizzato e riservato**: La somma dello spazio fisico utilizzato e riservato.

#### Capacità di una VM storage

La capacità massima di una VM di storage è determinata dallo spazio allocato totale per i volumi più lo spazio non allocato rimanente.

- Lo spazio allocato per i volumi è la somma della capacità utilizzata e della capacità disponibile di volumi FlexVol, FlexGroup e FlexCache.
- La capacità dei volumi viene inclusa nelle somme, anche quando sono limitate, offline o nella coda di ripristino dopo l'eliminazione.
- Se i volumi sono configurati con la crescita automatica, il valore massimo di dimensionamento automatico del volume viene utilizzato nelle somme. Senza la crescita automatica, la capacità effettiva del volume viene utilizzata nelle somme.

Il grafico seguente spiega come la misurazione della capacità tra i volumi si riferisce al limite massimo di capacità.



A partire da ONTAP 9.13.1, gli amministratori del cluster possono farlo ["Abilitare un limite massimo di capacità per una VM di storage"](#). Tuttavia, non è possibile impostare limiti di storage per una VM di storage che contiene volumi per la protezione dei dati, in una relazione SnapMirror o in una configurazione MetroCluster. Inoltre, le quote non possono essere configurate in modo da superare la capacità massima di una VM di storage.

Una volta impostato il limite massimo di capacità, non è possibile modificarlo in una dimensione inferiore alla capacità attualmente allocata.

Quando una VM di storage raggiunge il limite massimo di capacità, alcune operazioni non possono essere eseguite. System Manager fornisce suggerimenti per le fasi successive di ["Insights"](#).

#### Unità di misura della capacità

System Manager calcola la capacità dello storage in base a unità binarie di 1024 ( $2^{10}$ ) byte.

- A partire da ONTAP 9.10.1, le unità di capacità dello storage vengono visualizzate in Gestione sistemi come KiB, MiB, GiB, TiB e PiB.
- In ONTAP 9.10.0 e versioni precedenti, queste unità vengono visualizzate in Gestione sistema come KB, MB, GB, TB e PB.



Le unità utilizzate in Gestione sistema per il throughput continuano a essere KB/s, MB/s, GB/s, TB/s e PB/s per tutte le release di ONTAP.

Unità di capacità visualizzata in Gestore di sistema per ONTAP 9.10.0 e versioni precedenti	Unità di capacità visualizzata in Gestore di sistema per ONTAP 9.10.1 e versioni successive	Calcolo	Valore in byte
KB	KiB	1024	1024 byte
MB	MiB	1024 * 1024	1,048,576 byte
GB	GiB	1024 * 1024 * 1024	1,073,741,824 byte
TB	TiB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 byte
PB	PiB	1024 * 1024 * 1024 * 1024 * 1024	1,125,899,906,842,624 byte

### Informazioni correlate

["Monitorare la capacità in System Manager"](#)

["Creazione di report e applicazione dello spazio logico per i volumi"](#)

### Panoramica dell'efficienza dello storage sensibile alla temperatura

ONTAP offre vantaggi in termini di efficienza dello storage sensibili alla temperatura, valutando la frequenza di accesso ai dati del volume e mappando tale frequenza al grado di compressione applicato a tali dati. Per i dati cold a cui si accede raramente, i blocchi di dati più grandi vengono compressi, mentre per i dati hot, a cui si accede frequentemente e che vengono sovrascritti più spesso, i blocchi di dati più piccoli vengono compressi, rendendo il processo più efficiente.

L'efficienza dello storage sensibile alla temperatura (TSSE) viene introdotta in ONTAP 9.8 e attivata automaticamente sui volumi AFF appena creati con thin provisioning. È possibile abilitare l'efficienza dello storage sensibile alla temperatura sui volumi AFF esistenti e sui volumi DP non AFF con thin provisioning.

### Introduzione delle modalità "predefinite" ed "efficienti"

A partire da ONTAP 9.10.1, sono state introdotte due modalità di efficienza dello storage a livello di volume solo per i sistemi AFF, *default* e *Efficient*. Le due modalità consentono di scegliere tra la compressione file (predefinita), che è la modalità predefinita per la creazione di nuovi volumi AFF, o l'efficienza dello storage sensibile alla temperatura (efficiente), che consente l'efficienza dello storage sensibile alla temperatura. Con ONTAP 9.10.1, ["l'efficienza dello storage sensibile alla temperatura deve essere impostata in modo esplicito"](#) per attivare la compressione adattativa automatica. Tuttavia, altre funzionalità di efficienza dello storage, come la compattazione dei dati, la pianificazione della deduplica automatica, la deduplica inline, la deduplica inline tra volumi e la deduplica in background tra volumi, sono attivate per impostazione predefinita sulle piattaforme AFF sia per le modalità predefinite che per quelle efficienti.

Entrambe le modalità di efficienza dello storage (predefinite ed efficienti) sono supportate negli aggregati abilitati per FabricPool e con tutti i tipi di policy di tiering.

### Efficienza dello storage sensibile alla temperatura abilitata sulle piattaforme C-Series

L'efficienza dello storage sensibile alla temperatura è attivata per impostazione predefinita sulle piattaforme AFF C-Series e durante la migrazione dei volumi da una piattaforma non TSSE a una piattaforma C-Series abilitata a TSSE utilizzando lo spostamento del volume o SnapMirror con le seguenti release installate sulla destinazione:

- ONTAP 9.12.1P4 e versioni successive
- ONTAP 9.13.1 e versioni successive

Per ulteriori informazioni, vedere ["Comportamento in termini di efficienza dello storage con lo spostamento dei volumi e le operazioni SnapMirror"](#).

Tuttavia, per i volumi esistenti, l'efficienza dello storage sensibile alla temperatura non viene attivata automaticamente ["modificare la modalità di efficienza dello storage"](#) manualmente per passare alla modalità efficiente.



Una volta impostata la modalità di efficienza dello storage su efficiente, non sarà più possibile modificarla.

### **Efficienza dello storage migliorata grazie al confezionamento sequenziale di blocchi fisici contigui**

A partire da ONTAP 9.13.1, l'efficienza dello storage sensibile alla temperatura aggiunge un impacchettamento sequenziale di blocchi fisici contigui per migliorare ulteriormente l'efficienza dello storage. I volumi con efficienza dello storage sensibile alla temperatura attivata dispongono automaticamente del packing sequenziale attivato quando si aggiornano i sistemi a ONTAP 9.13.1. Una volta attivato il packing sequenziale, è necessario ["reimballare manualmente i dati esistenti"](#).

### **Considerazioni sull'upgrade**

Quando si esegue l'aggiornamento a ONTAP 9.10.1 e versioni successive, ai volumi esistenti viene assegnata una modalità di efficienza dello storage basata sul tipo di compressione attualmente attivata sui volumi. Durante un aggiornamento, ai volumi con compressione attivata viene assegnata la modalità predefinita e ai volumi con efficienza dello storage sensibile alla temperatura attivata viene assegnata la modalità efficiente. Se la compressione non è attivata, la modalità di efficienza dello storage rimane vuota.

## **Sicurezza**

### **Autenticazione e autorizzazione del client**

ONTAP utilizza metodi standard per proteggere l'accesso client e amministratore allo storage e per proteggerlo dai virus. Sono disponibili tecnologie avanzate per la crittografia dei dati a riposo e per lo storage WORM.

ONTAP autentica un computer client e un utente verificando la propria identità con un'origine attendibile. ONTAP autorizza un utente ad accedere a un file o a una directory confrontando le credenziali dell'utente con le autorizzazioni configurate nel file o nella directory.

### **Autenticazione**

È possibile creare account utente locali o remoti:

- Un account locale è un account in cui le informazioni dell'account risiedono nel sistema di storage.
- Un account remoto è un account in cui le informazioni sull'account vengono memorizzate in un controller di dominio Active Directory, in un server LDAP o in un server NIS.



ONTAP utilizza i servizi dei nomi locali o esterni per cercare informazioni relative a nome host, utente, gruppo, netgroup e mappatura dei nomi. ONTAP supporta i seguenti servizi per i nomi:

- Utenti locali
- DNS
- Domini NIS esterni
- Domini LDAP esterni

Una *name service switch table* specifica le fonti per la ricerca delle informazioni di rete e l'ordine in cui ricercarle (fornendo la funzionalità equivalente del file `/etc/nsswitch.conf` sui sistemi UNIX). Quando un client NAS si connette a SVM, ONTAP verifica i servizi dei nomi specificati per ottenere le informazioni richieste.

**supporto Kerberos** Kerberos è un protocollo di autenticazione di rete che fornisce “autenticazione through” crittografando le password utente nelle implementazioni client-server. ONTAP supporta l'autenticazione Kerberos 5 con controllo dell'integrità (krb5i) e l'autenticazione Kerberos 5 con controllo della privacy (krb5p).

### Autorizzazione

ONTAP valuta tre livelli di sicurezza per determinare se un'entità è autorizzata a eseguire un'azione richiesta su file e directory che risiedono su una SVM. L'accesso è determinato dalle autorizzazioni effettive dopo la valutazione dei livelli di sicurezza:

- Sicurezza di esportazione (NFS) e condivisione (SMB)

La sicurezza di esportazione e condivisione si applica all'accesso client a una data esportazione NFS o condivisione SMB. Gli utenti con privilegi amministrativi possono gestire la sicurezza a livello di esportazione e condivisione dai client SMB e NFS.

- Protezione di file e directory di Access Guard a livello di storage

La sicurezza di Access Guard a livello di storage si applica all'accesso dei client SMB e NFS ai volumi SVM. Sono supportate solo le autorizzazioni di accesso NTFS. Affinché ONTAP esegua controlli di sicurezza sugli utenti UNIX per l'accesso ai dati sui volumi per i quali è stato applicato Storage-Level Access Guard, l'utente UNIX deve eseguire il mapping a un utente Windows sulla SVM proprietaria del volume.

- Sicurezza nativa a livello di file in NTFS, UNIX e NFSv4

La protezione nativa a livello di file esiste nel file o nella directory che rappresenta l'oggetto di storage. È possibile impostare la sicurezza a livello di file da un client. Le autorizzazioni dei file sono efficaci indipendentemente dal fatto che SMB o NFS vengano utilizzati per accedere ai dati.

### Autenticazione con SAML

ONTAP supporta il linguaggio SAML (Security Assertion Markup Language) per l'autenticazione degli utenti remoti. Sono supportati diversi provider di identità (IDP). Per ulteriori informazioni sugli IDP supportati e istruzioni per l'attivazione dell'autenticazione SAML, fare riferimento a ["Configurare l'autenticazione SAML"](#).

### OAuth 2,0 con client API REST ONTAP

Il supporto per il framework Open Authorization (OAuth 2,0) è disponibile a partire da ONTAP 9,14. È possibile utilizzare OAuth 2,0 solo per prendere decisioni di autorizzazione e controllo degli accessi quando il client

utilizza l'API REST per accedere a ONTAP. Tuttavia, puoi configurare e abilitare la funzionalità con qualsiasi interfaccia amministrativa di ONTAP, inclusi CLI, System Manager e API REST.

Le funzionalità standard di OAuth 2,0 sono supportate insieme a diversi server di autorizzazione più diffusi. È possibile migliorare ulteriormente la protezione di ONTAP utilizzando token di accesso con vincoli di mittente basati su TLS comuni. Inoltre, è disponibile una vasta gamma di opzioni di autorizzazione, tra cui ambiti indipendenti, oltre all'integrazione con i ruoli REST di ONTAP e le definizioni degli utenti locali. Vedere ["Panoramica dell'implementazione di ONTAP OAuth 2,0"](#) per ulteriori informazioni.

## Autenticazione amministratore e RBAC

Gli amministratori utilizzano account di accesso locali o remoti per autenticarsi al cluster e alla SVM. RBAC (Role-Based Access Control) determina i comandi a cui un amministratore ha accesso.

### Autenticazione

È possibile creare account di amministratore SVM e cluster locali o remoti:

- Un account locale è un account in cui le informazioni sull'account, la chiave pubblica o il certificato di protezione risiedono nel sistema di storage.
- Un account remoto è un account in cui le informazioni sull'account vengono memorizzate in un controller di dominio Active Directory, in un server LDAP o in un server NIS.

Ad eccezione del DNS, ONTAP utilizza gli stessi servizi di nome per autenticare gli account amministratore utilizzati per autenticare i client.

### RBAC

Il *ruolo* assegnato a un amministratore determina i comandi a cui l'amministratore ha accesso. Il ruolo viene assegnato quando si crea l'account per l'amministratore. È possibile assegnare un ruolo diverso o definire ruoli personalizzati in base alle esigenze.

### Scansione virus

È possibile utilizzare la funzionalità antivirus integrata nel sistema di storage per proteggere i dati da virus o altri codici dannosi. La scansione antivirus di ONTAP, denominata *Vscan*, combina il software antivirus di terze parti più all'avanguardia con le funzionalità di ONTAP che offrono la flessibilità necessaria per controllare quali file vengono sottoposti a scansione e quando.

I sistemi storage trasferiscono le operazioni di scansione a server esterni che ospitano software antivirus di terze parti. Il *connettore antivirus ONTAP*, fornito da NetApp e installato sul server esterno, gestisce le comunicazioni tra il sistema di storage e il software antivirus.

- È possibile utilizzare *on-access scanning* per verificare la presenza di virus quando i client aprono, leggono, rinominano o chiudono i file su SMB. L'operazione sul file viene sospesa fino a quando il server esterno non riporta lo stato di scansione del file. Se il file è già stato sottoposto a scansione, ONTAP consente l'operazione. In caso contrario, richiede una scansione dal server.

La scansione on-access non è supportata per NFS.

- È possibile utilizzare la *scansione on-demand* per controllare i file alla ricerca di virus immediatamente o in

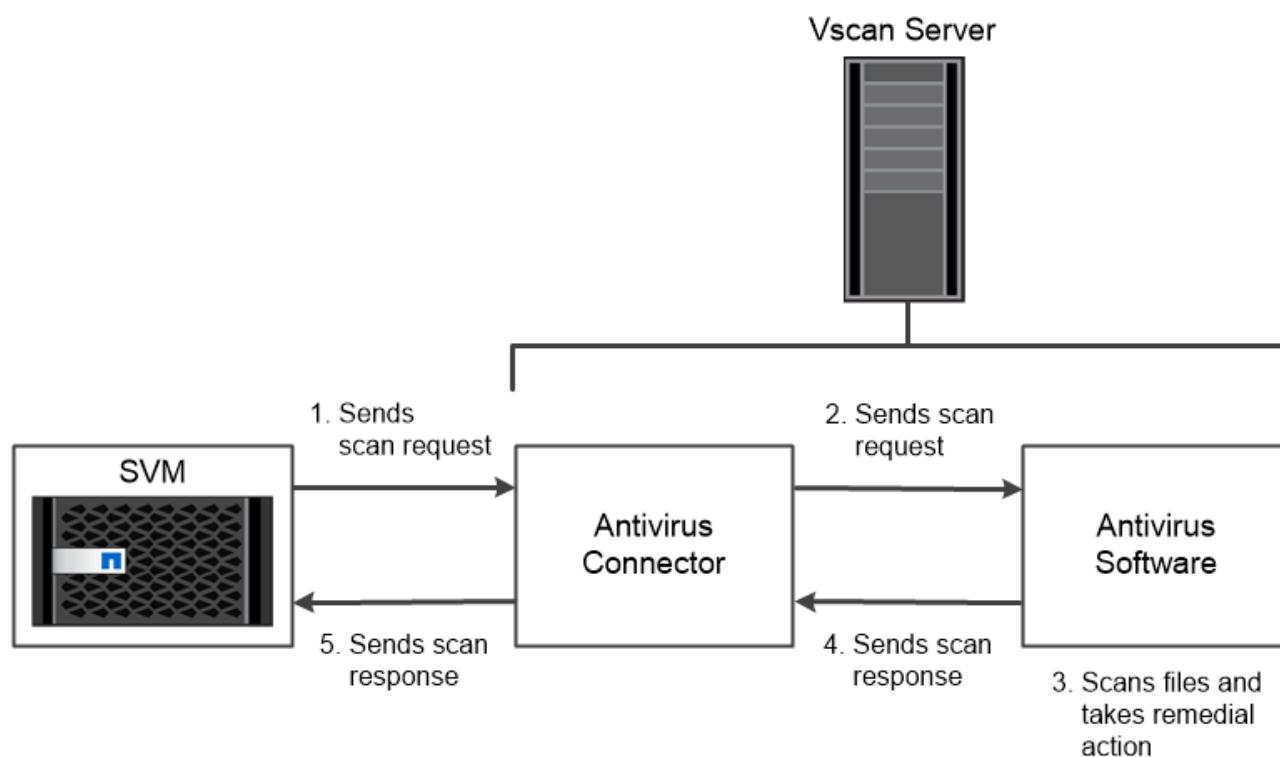
base a una pianificazione. Ad esempio, è possibile eseguire scansioni solo in ore non di punta. Il server esterno aggiorna lo stato di scansione dei file selezionati, in modo che la latenza di accesso ai file (presupponendo che non siano stati modificati) sia in genere ridotta al successivo accesso tramite SMB.

È possibile utilizzare la scansione on-demand per qualsiasi percorso nello spazio dei nomi SVM, anche per i volumi esportati solo tramite NFS.

In genere, si abilitano entrambe le modalità di scansione su una SVM. In entrambe le modalità, il software antivirus esegue un'azione correttiva sui file infetti in base alle impostazioni del software.

#### ***scansione virus in disaster recovery e configurazioni MetroCluster***

Per le configurazioni di disaster recovery e MetroCluster, è necessario configurare server Vscan separati per i cluster locali e partner.



*The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.*

## **Crittografia**

ONTAP offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

ONTAP è conforme agli standard federali sull'elaborazione delle informazioni (FIPS) 140-2 per tutte le connessioni SSL. È possibile utilizzare le seguenti soluzioni di crittografia:

- Soluzioni hardware:

- NetApp Storage Encryption (NSE)

NSE è una soluzione hardware che utilizza dischi con crittografia automatica (SED).

- SED NVMe

ONTAP offre la crittografia completa del disco per i SED NVMe che non dispongono della certificazione FIPS 140-2.

- Soluzioni software:

- NetApp aggregate Encryption (NAE)

NAE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con chiavi univoche per ciascun aggregato.

- NetApp Volume Encryption (NVE)

NVE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con una chiave univoca per ciascun volume.

Utilizzare soluzioni di crittografia sia software (NAE o NVE) che hardware (NSE o NVMe SED) per ottenere una doppia crittografia a riposo. L'efficienza dello storage non è influenzata dalla crittografia NAE o NVE.

### **Crittografia dello storage NetApp**

NetApp Storage Encryption (NSE) supporta i SED che crittografano i dati durante la scrittura. I dati non possono essere letti senza una chiave di crittografia memorizzata sul disco. La chiave di crittografia, a sua volta, è accessibile solo a un nodo autenticato.

In caso di richiesta i/o, un nodo esegue l'autenticazione in un SED utilizzando una chiave di autenticazione recuperata da un server di gestione delle chiavi esterno o da Onboard Key Manager:

- Il server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi di autenticazione ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).
- Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati.

NSE supporta HDD e SSD con crittografia automatica. È possibile utilizzare NetApp Volume Encryption con NSE per la doppia crittografia dei dati sui dischi NSE.



Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSE non crittografa i dati che risiedono nel modulo Flash cache.

### **Dischi con crittografia automatica NVMe**

I dischi SED NVMe non dispongono della certificazione FIPS 140-2, tuttavia, utilizzano la crittografia trasparente dei dischi AES a 256 bit per proteggere i dati inattivi.

Le operazioni di crittografia dei dati, come la generazione di una chiave di autenticazione, vengono eseguite internamente. La chiave di autenticazione viene generata la prima volta che il sistema di storage accede al disco. In seguito, i dischi proteggono i dati inattivi richiedendo l'autenticazione del sistema di storage ogni volta che vengono richieste operazioni sui dati.

## Crittografia aggregata NetApp

NetApp aggregate Encryption (NAE) è una tecnologia software per la crittografia di tutti i dati su un aggregato. Un vantaggio di NAE è che i volumi sono inclusi nella deduplica a livello di aggregato, mentre i volumi NVE sono esclusi.

Con NAE attivato, i volumi all'interno dell'aggregato possono essere crittografati con chiavi aggregate.

A partire da ONTAP 9,7, gli aggregati e i volumi appena creati sono crittografati per impostazione predefinita, quando si dispone di "[Licenza NVE](#)" e gestione della chiave integrata o esterna.

## Crittografia dei volumi NetApp

NetApp Volume Encryption (NVE) è una tecnologia software per la crittografia dei dati inattivi di un volume alla volta. Una chiave di crittografia accessibile solo al sistema di storage garantisce che i dati del volume non possano essere letti se il dispositivo sottostante è separato dal sistema.

Entrambi i dati, incluse le copie Snapshot, e i metadati sono crittografati. L'accesso ai dati viene fornito da una chiave XTS-AES-256 univoca, una per volume. Un Onboard Key Manager integrato protegge le chiavi dello stesso sistema con i dati.

È possibile utilizzare NVE su qualsiasi tipo di aggregato (HDD, SSD, ibrido, LUN array), con qualsiasi tipo di RAID e in qualsiasi implementazione ONTAP supportata, incluso ONTAP Select. È inoltre possibile utilizzare NVE con NetApp Storage Encryption (NSE) per eseguire la doppia crittografia dei dati sui dischi NSE.

**quando utilizzare i server KMIP** sebbene sia meno costoso e generalmente più conveniente utilizzare Onboard Key Manager, è necessario configurare i server KMIP se si verifica una delle seguenti condizioni:

- La soluzione di gestione delle chiavi di crittografia deve essere conforme agli standard FIPS (Federal Information Processing Standards) 140-2 o ALLO standard OASIS KMIP.
- Hai bisogno di una soluzione multi-cluster. I server KMIP supportano più cluster con gestione centralizzata delle chiavi di crittografia.

I server KMIP supportano più cluster con gestione centralizzata delle chiavi di crittografia.

- La tua azienda richiede una maggiore sicurezza nell'archiviazione delle chiavi di autenticazione su un sistema o in una posizione diversa dai dati.

I server KMIP memorizzano le chiavi di autenticazione separatamente dai dati.

## Informazioni correlate

["FAQ - NetApp Volume Encryption e NetApp aggregate Encryption"](#)

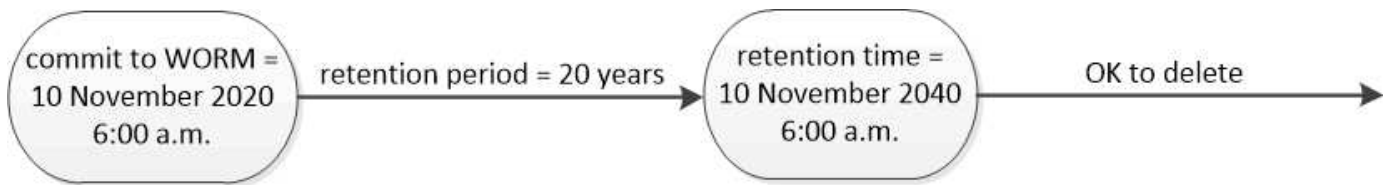
## Storage WORM

**SnapLock** è una soluzione per la compliance dalle performance elevate per le organizzazioni che utilizzano lo storage *write once, Read Many (WORM)* per conservare i file critici in forma non modificata per scopi normativi e di governance.

Una singola licenza consente di utilizzare SnapLock in una *modalità di conformità* rigorosa, per soddisfare mandati esterni come la norma SEC 17a-4, e una *modalità aziendale* più allentata, per soddisfare le normative interne per la protezione delle risorse digitali. SnapLock utilizza un *ComplianceClock* a prova di manomissione

per determinare quando è trascorso il periodo di conservazione di un file WORM.

È possibile utilizzare *SnapLock for SnapVault* per proteggere WORM le copie Snapshot sullo storage secondario. È possibile utilizzare SnapMirror per replicare i file WORM in un'altra posizione geografica per il disaster recovery e altri scopi.



*SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.*

## Gestione dei dati consapevole dell'applicazione

La gestione dei dati consapevole delle applicazioni consente di descrivere l'applicazione che si desidera implementare su ONTAP in termini di applicazione, piuttosto che in termini di storage. L'applicazione può essere configurata e pronta per la distribuzione rapida dei dati con input minimi utilizzando System Manager e le API REST.

La funzione di gestione dei dati basata sulle applicazioni consente di configurare, gestire e monitorare lo storage a livello di singole applicazioni. Questa funzionalità incorpora le Best practice ONTAP pertinenti per il provisioning ottimale delle applicazioni, con posizionamento bilanciato degli oggetti storage in base ai livelli di servizio delle performance desiderati e alle risorse di sistema disponibili.

La funzionalità di gestione dei dati consapevole dell'applicazione include un set di modelli di applicazione, con ciascun modello costituito da un set di parametri che descrivono collettivamente la configurazione di un'applicazione. Questi parametri, spesso preimpostati con valori predefiniti, definiscono le caratteristiche che un amministratore dell'applicazione può specificare per il provisioning dello storage su un sistema ONTAP, come dimensioni del database, livelli di servizio, elementi di accesso al protocollo come LIF, criteri di protezione locale e criteri di protezione remota. In base ai parametri specificati, ONTAP configura entità di storage come LUN e volumi con dimensioni e livelli di servizio appropriati per l'applicazione.

È possibile eseguire le seguenti attività per le applicazioni:

- Creare applicazioni utilizzando i modelli di applicazione
- Gestire lo storage associato alle applicazioni
- Modificare o eliminare le applicazioni
- Visualizzare le applicazioni
- Gestire le copie Snapshot delle applicazioni
- Creare [gruppi di coerenza](#) Fornire funzionalità di protezione dei dati selezionando più LUN nello stesso volume o in volumi diversi

## FabricPool

Molti clienti NetApp dispongono di quantità significative di dati memorizzati a cui si accede raramente. Chiamiamo i dati *cold*. I clienti hanno anche dati ai quali si accede

frequentemente, che chiamiamo *hot data*. Idealmente, si desidera conservare i dati più caldi sullo storage più veloce per ottenere le migliori performance. I dati cold possono passare a uno storage più lento, purché sia immediatamente disponibile, se necessario. Ma come fai a sapere quali parti dei tuoi dati sono calde e quali sono fredde?

FabricPool è una funzionalità di ONTAP che sposta automaticamente i dati tra un Tier locale ad alte performance (aggregato) e un Tier cloud in base ai modelli di accesso. Il tiering libera lo storage locale costoso per i dati hot mantenendo i dati cold prontamente disponibili dallo storage a oggetti a basso costo nel cloud. FabricPool monitora costantemente l'accesso ai dati e sposta i dati tra i Tier per ottenere le migliori performance e il massimo risparmio.

L'utilizzo di FabricPool per il Tier dei dati cold nel cloud è uno dei modi più semplici per ottenere l'efficienza del cloud e creare una configurazione del cloud ibrido. FabricPool funziona a livello di blocchi di storage, quindi funziona sia con i dati di file che con i dati LUN.

Ma FabricPool non è solo per il tiering dei dati on-premise nel cloud. Molti clienti utilizzano FabricPool in Cloud Volumes ONTAP per eseguire il tiering dei dati cold da uno storage cloud più costoso a uno storage a oggetti a basso costo all'interno del cloud provider. A partire da ONTAP 9.8, puoi acquisire analytics su volumi abilitati FabricPool con ["Analisi del file system"](#) oppure ["efficienza dello storage sensibile alla temperatura"](#).

Le applicazioni che utilizzano i dati non sono consapevoli del fatto che i dati sono a livelli, pertanto non sono necessarie modifiche alle applicazioni. Il tiering è completamente automatico, quindi non è necessaria alcuna amministrazione in corso.

È possibile memorizzare i dati cold nello storage a oggetti di uno dei principali provider di cloud. Oppure scegli NetApp StorageGRID per conservare i tuoi dati nel tuo cloud privato, per ottenere le massime performance e il controllo completo sui tuoi dati.

#### **Informazioni correlate**

["Documento Gestore di sistema di FabricPool"](#)

["Tiering BlueXP"](#)

["Elenco di riproduzione FabricPool su NetApp TechComm TV"](#)



# Configurazione, aggiornamento e ripristino del software e del firmware ONTAP

## Configurare ONTAP

### Inizia subito a configurare il cluster di ONTAP

Puoi utilizzare System Manager o l'interfaccia a riga di comando (CLI) di ONTAP per configurare nuovi cluster ONTAP. Prima di iniziare, è necessario raccogliere le informazioni necessarie per completare la configurazione del cluster, ad esempio la porta dell'interfaccia di gestione del cluster e l'indirizzo IP.

NetApp consiglia di farlo ["Utilizza System Manager per configurare nuovi cluster"](#). System Manager offre un workflow semplice e facile per la configurazione e la configurazione del cluster, che include l'assegnazione di un indirizzo IP di gestione dei nodi, l'inizializzazione del cluster, la creazione di un Tier locale, la configurazione dei protocolli e il provisioning dello storage iniziale.

È solo necessario a. ["USA l'interfaccia a riga di comando di ONTAP per configurare il cluster"](#) Se si utilizza ONTAP 9,7 o versione precedente su una configurazione MetroCluster. A partire da ONTAP 9.13.1, sulle piattaforme AFF A800 e FAS8700, puoi anche utilizzare l'interfaccia a riga di comando di ONTAP per creare e configurare nuovi cluster in ambienti di rete solo IPv6. Se devi utilizzare IPv6 in ONTAP 9.13.0 e versioni precedenti o su altre piattaforme in ONTAP 9.13.1 e versioni successive, puoi utilizzare System Manager per creare nuovi cluster utilizzando e versioni successive di IPv4 ["Converti in IPv6"](#).

### Tutto ciò che serve per la configurazione dei cluster

La configurazione del cluster comporta la raccolta delle informazioni necessarie per configurare l'impostazione di ciascun nodo, la creazione del cluster sul primo nodo e l'Unione di eventuali nodi rimanenti al cluster.

Inizia raccogliendo tutte le informazioni pertinenti nei fogli di lavoro per la configurazione del cluster.

Il foglio di lavoro per l'installazione del cluster consente di registrare i valori necessari durante il processo di installazione del cluster. Se viene fornito un valore predefinito, è possibile utilizzare tale valore oppure immettere il proprio.

### Impostazioni predefinite del sistema

I valori predefiniti del sistema sono i valori predefiniti per la rete cluster privata. Si consiglia di utilizzare questi valori predefiniti. Tuttavia, se non soddisfano i requisiti, è possibile utilizzare la tabella per registrare i propri valori.



Per i cluster configurati per l'utilizzo di switch di rete, ogni switch del cluster deve utilizzare la dimensione MTU 9000.

Tipi di informazioni	I tuoi valori
Porte di rete del cluster privato	
Netmask di rete del cluster	

Tipi di informazioni	I tuoi valori
Indirizzi IP dell'interfaccia del cluster (per ciascuna porta di rete del cluster su ciascun nodo) gli indirizzi IP di ciascun nodo devono trovarsi sulla stessa subnet.	

#### Informazioni sul cluster


Tipi di informazioni	I tuoi valori
Nome del cluster il nome deve iniziare con una lettera e deve contenere meno di 44 caratteri. Il nome può includere i seguenti caratteri speciali: · - _	

#### Chiavi di licenza delle funzioni

È possibile trovare le chiavi di licenza per gli ordini software iniziali o aggiuntivi nel sito di supporto NetApp in **My Support > Software Licenses**.

Tipi di informazioni	I tuoi valori
Chiavi di licenza delle funzioni	

#### SVM (Admin Storage Virtual Machine)

Tipi di informazioni	I tuoi valori
<p>Password dell'amministratore del cluster</p> <p>La password per l'account admin richiesta dal cluster prima di concedere l'accesso dell'amministratore del cluster alla console o tramite un protocollo sicuro.</p> <div>  <p>Per motivi di sicurezza, si sconsiglia di registrare le password in questo foglio di lavoro.</p> </div> <p>Le regole predefinite per le password sono le seguenti:</p> <ul style="list-style-type: none"> <li>• La password deve contenere almeno otto caratteri.</li> <li>• Una password deve contenere almeno una lettera e un numero.</li> </ul>	
<p>Porta dell'interfaccia di gestione del cluster</p> <p>La porta fisica connessa alla rete dati e che consente all'amministratore del cluster di gestire il cluster.</p>	

Tipi di informazioni	I tuoi valori
<p>Indirizzo IP dell'interfaccia di gestione del cluster</p> <p>Un indirizzo IPv4 o IPv6 univoco per l'interfaccia di gestione del cluster. L'amministratore del cluster utilizza questo indirizzo per accedere alla SVM amministrativa e gestire il cluster. In genere, questo indirizzo deve trovarsi sulla rete dati.</p> <p>È possibile ottenere questo indirizzo IP dall'amministratore responsabile dell'assegnazione degli indirizzi IP all'interno dell'organizzazione.</p> <p>Esempio: 192.0.2.66</p>	
<p>Netmask dell'interfaccia di gestione del cluster (IPv4)</p> <p>Subnet mask che definisce l'intervallo di indirizzi IPv4 validi sulla rete di gestione del cluster.</p> <p>Esempio: 255.255.255.0</p>	
<p>Interfaccia di gestione del cluster lunghezza netmask (IPv6)</p> <p>Se l'interfaccia di gestione del cluster utilizza un indirizzo IPv6, questo valore rappresenta la lunghezza del prefisso che definisce l'intervallo di indirizzi IPv6 validi sulla rete di gestione del cluster.</p> <p>Esempio: 64</p>	
<p>Gateway predefinito dell'interfaccia di gestione del cluster</p> <p>L'indirizzo IP del router sulla rete di gestione del cluster.</p>	
<p>Nome di dominio DNS</p> <p>Il nome del dominio DNS della rete.</p> <p>Il nome di dominio deve essere composto da caratteri alfanumerici. Per inserire più nomi di dominio DNS, separare ciascun nome con una virgola o uno spazio.</p>	
<p>Indirizzi IP del server dei nomi</p> <p>Gli indirizzi IP dei server dei nomi DNS. Separare ciascun indirizzo con una virgola o uno spazio.</p>	

**Informazioni sui nodi (per ciascun nodo del cluster)**

<b>Tipi di informazioni</b>	<b>I tuoi valori</b>
<p>Posizione fisica del controller (opzionale)</p> <p>Una descrizione della posizione fisica del controller. Utilizzare una descrizione che identifichi dove trovare questo nodo nel cluster (ad esempio, "Lab 5, Row 7, rack B").</p>	
<p>Porta di interfaccia per la gestione dei nodi</p> <p>La porta fisica connessa alla rete di gestione dei nodi e che consente all'amministratore del cluster di gestire il nodo.</p>	
<p>Indirizzo IP dell'interfaccia di gestione dei nodi</p> <p>Indirizzo IPv4 o IPv6 univoco per l'interfaccia di gestione dei nodi sulla rete di gestione. Se la porta dell'interfaccia di gestione dei nodi è stata definita una porta dati, l'indirizzo IP deve essere un indirizzo IP univoco sulla rete dati.</p> <p>È possibile ottenere questo indirizzo IP dall'amministratore responsabile dell'assegnazione degli indirizzi IP all'interno dell'organizzazione.</p> <p>Esempio: 192.0.2.66</p>	
<p>Netmask dell'interfaccia di gestione dei nodi (IPv4)</p> <p>Subnet mask che definisce l'intervallo di indirizzi IP validi sulla rete di gestione dei nodi.</p> <p>Se la porta dell'interfaccia di gestione dei nodi è stata definita una porta dati, la netmask deve essere la subnet mask della rete dati.</p> <p>Esempio: 255.255.255.0</p>	
<p>Interfaccia di gestione dei nodi lunghezza netmask (IPv6)</p> <p>Se l'interfaccia di gestione dei nodi utilizza un indirizzo IPv6, questo valore rappresenta la lunghezza del prefisso che definisce l'intervallo di indirizzi IPv6 validi sulla rete di gestione dei nodi.</p> <p>Esempio: 64</p>	

Tipi di informazioni	I tuoi valori
Gateway predefinito dell'interfaccia di gestione dei nodi  L'indirizzo IP del router sulla rete di gestione dei nodi.	

#### Informazioni sul server NTP

Tipi di informazioni	I tuoi valori
Indirizzi del server NTP  Gli indirizzi IP dei server NTP (Network Time Protocol) del sito. Questi server vengono utilizzati per sincronizzare l'ora nel cluster.	

## Configurare ONTAP su un nuovo cluster con Gestione di sistema

System Manager offre un workflow semplice e semplice per la configurazione di un nuovo cluster e dello storage.

In alcuni casi, ad esempio in alcune implementazioni MetroCluster o in alcuni cluster che richiedono l'indirizzamento di rete IPv6, potrebbe essere necessario utilizzare l'interfaccia utente di ONTAP per configurare un nuovo cluster. Fare clic su ["qui"](#) Per ulteriori informazioni su questi requisiti, nonché per la procedura di configurazione del cluster con l'interfaccia utente di ONTAP.

#### Prima di iniziare

- È necessario installare, cablare e accendere il nuovo sistema di storage seguendo le istruzioni di installazione e configurazione del modello di piattaforma in uso. Vedere ["Documentazione AFF e FAS"](#).
- Le interfacce di rete del cluster devono essere configurate su ciascun nodo del cluster per la comunicazione all'interno del cluster.
- È necessario conoscere i seguenti requisiti di supporto per System Manager:
  - Quando si imposta manualmente la gestione dei nodi utilizzando la CLI, System Manager supporta solo IPv4 e non IPv6. Tuttavia, se si avvia System Manager dopo aver completato la configurazione dell'hardware utilizzando DHCP con un indirizzo IP assegnato automaticamente e con il rilevamento di Windows, System Manager può configurare un indirizzo di gestione IPv6.

In ONTAP 9.6 e versioni precedenti, System Manager non supporta le implementazioni che richiedono una rete IPv6.

- Il supporto per la configurazione MetroCluster è per le configurazioni IP MetroCluster con due nodi in ogni sito.

In ONTAP 9.7 e versioni precedenti, System Manager non supporta la nuova configurazione del cluster per le configurazioni MetroCluster.



## Assegnare un indirizzo IP di gestione dei nodi

### Sistema Windows

Collegare il computer Windows alla stessa subnet dei controller. In questo modo, viene assegnato automaticamente un indirizzo IP di gestione dei nodi al sistema.

### Fase

1. Dal sistema Windows, aprire l'unità **Network** per rilevare i nodi.
2. Fare doppio clic sul nodo per avviare l'installazione guidata del cluster.

### Altri sistemi

È necessario configurare l'indirizzo IP di gestione dei nodi per uno dei nodi nel cluster. È possibile utilizzare questo indirizzo IP di gestione dei nodi per avviare la configurazione guidata del cluster.

Vedere "[Creazione del cluster sul primo nodo](#)" Per informazioni sull'assegnazione di un indirizzo IP di gestione dei nodi.

## Inizializzare il cluster

Per inizializzare il cluster, impostare una password amministrativa per il cluster e le reti di gestione dei nodi e del cluster. È inoltre possibile configurare servizi come un server DNS per risolvere i nomi host e un server NTP per sincronizzare l'ora.

### Fasi

1. In un browser Web, immettere l'indirizzo IP di gestione dei nodi configurato: "<a href='\"https://node-management-IP\"' class='\"bare\"'>https://node-management-IP</a>

System Manager rileva automaticamente i nodi rimanenti nel cluster.

2. Inizializzare il sistema storage configurando gli indirizzi IP di gestione della rete di gestione del cluster e dei nodi per tutti i nodi.

## Crea il tuo Tier locale

Crea Tier locali dai dischi o dagli SSD disponibili nei tuoi nodi. System Manager calcola automaticamente la configurazione del miglior livello in base all'hardware.

### Fasi

1. Fare clic su **Dashboard**, quindi su **Prepare Storage** (prepara storage).

Accetta le raccomandazioni relative allo storage per il tuo Tier locale.

## Configurare i protocolli

A seconda delle licenze attivate sul cluster, è possibile attivare i protocolli desiderati sul cluster. Si creano

quindi interfacce di rete che consentono di accedere allo storage.

### Fasi

1. Fare clic su **Dashboard**, quindi su **Configure Protocols** (Configura protocolli).
  - Abilitare iSCSI o FC per l'accesso SAN.
  - Abilitare NFS o SMB per l'accesso NAS.
  - Abilitare NVMe per l'accesso FC-NVMe.

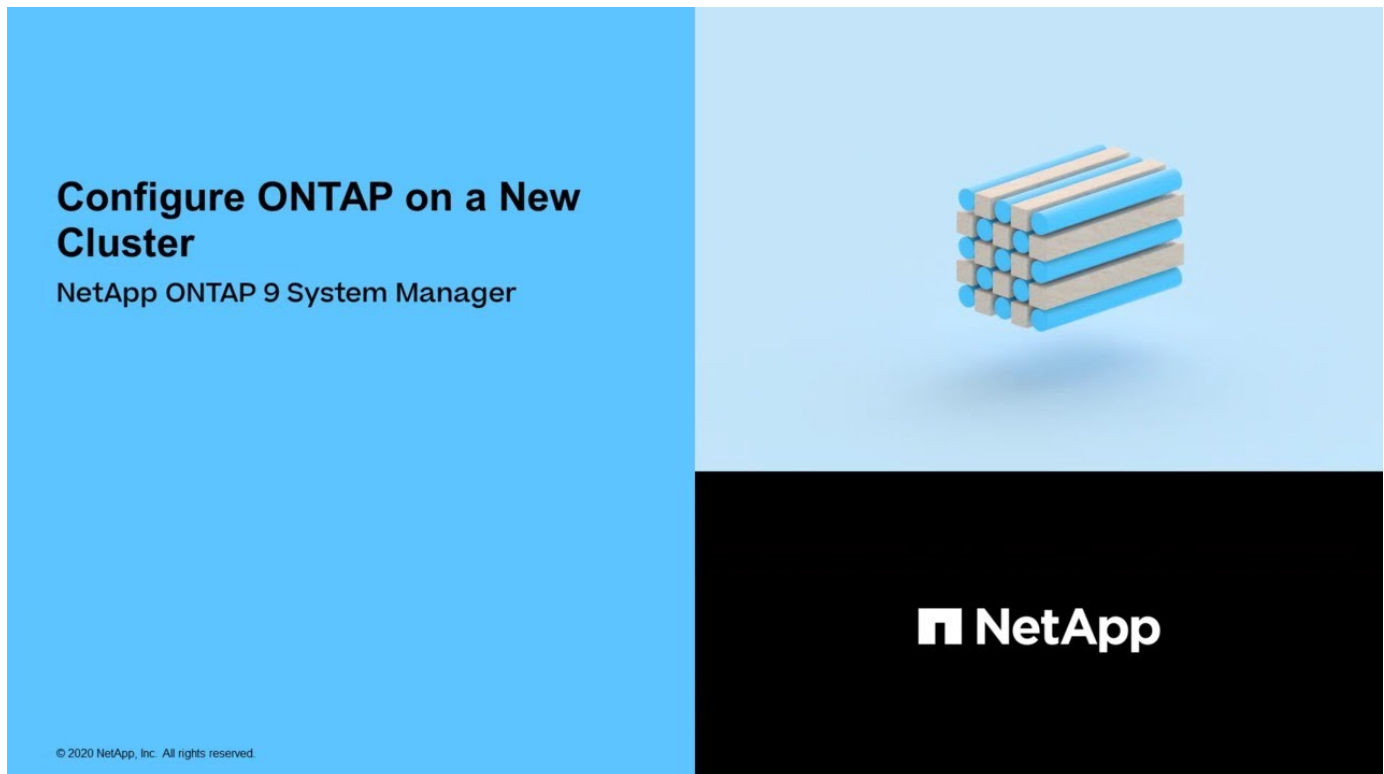
### Provisioning dello storage

Dopo aver configurato i protocolli, è possibile eseguire il provisioning dello storage. Le opzioni visualizzate dipendono dalle licenze installate.

### Fasi

1. Fare clic su **Dashboard**, quindi su **Provision Storage**.
  - A. "[Provisioning dell'accesso SAN](#)", Fare clic su **Aggiungi LUN**.
  - A. "[Provisioning dell'accesso NAS](#)", Fare clic su **Add Volumes** (Aggiungi volumi).
  - A. "[Esegui il provisioning dello storage NVMe](#)", Fare clic su **Aggiungi spazi dei nomi**.

### Configurare ONTAP su un nuovo video del cluster



### Configurare un cluster con la CLI

#### Creare il cluster sul primo nodo

La procedura guidata Cluster Setup consente di creare il cluster sul primo nodo. La procedura guidata consente di configurare la rete del cluster che connette i nodi, creare



la SVM (Cluster Admin Storage Virtual Machine), aggiungere chiavi di licenza delle funzionalità e creare l'interfaccia di gestione dei nodi per il primo nodo.

### Prima di iniziare

- È necessario installare, cablare e accendere il nuovo sistema di storage seguendo le istruzioni di installazione e configurazione del modello di piattaforma in uso. Vedere "[Documentazione AFF e FAS](#)".
- Le interfacce di rete del cluster devono essere configurate su ciascun nodo del cluster per la comunicazione all'interno del cluster.
- Se si configura IPv6 nel cluster, IPv6 deve essere configurato nel BMC (base Management Controller) in modo da poter accedere al sistema utilizzando SSH.

### Fasi

1. Accendere tutti i nodi che si stanno aggiungendo al cluster. Questo è necessario per abilitare il rilevamento per la configurazione del cluster.
2. Connettersi alla console del primo nodo.

Il nodo viene avviato, quindi viene avviata la procedura guidata di installazione del cluster sulla console.

```
Welcome to the cluster setup wizard....
```

3. Riconoscere l'istruzione AutoSupport.

```
Type yes to confirm and continue {yes}: yes
```



AutoSupport è attivato per impostazione predefinita.

4. Seguire le istruzioni visualizzate sullo schermo per assegnare un indirizzo IP al nodo.

A partire da ONTAP 9.13.1, è possibile assegnare indirizzi IPv6 per le LIF di gestione sulle piattaforme A800 e FAS8700. Per le versioni di ONTAP precedenti alla 9.13.1 o per la versione 9.13.1 e successive su altre piattaforme, è necessario assegnare indirizzi IPv4 per le LIF di gestione, quindi convertire in IPv6 dopo aver completato la configurazione del cluster.

5. Premere **Invio** per continuare.

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:
```

6. Creare un nuovo cluster: `create`
7. Accettare le impostazioni predefinite del sistema o inserire i propri valori.
8. Una volta completata l'installazione, accedere al cluster e verificare che il cluster sia attivo e che il primo nodo funzioni correttamente immettendo il comando ONTAP CLI: `cluster show`

L'esempio seguente mostra un cluster in cui il primo nodo (cluster1-01) è integro e idoneo a partecipare:

```
cluster1::> cluster show
Node                      Health  Eligibility
-----
cluster1-01              true    true
```

È possibile accedere alla procedura guidata di configurazione del cluster per modificare i valori immessi per la SVM amministrativa o il nodo SVM utilizzando `cluster setup` comando.

### Al termine

Se necessario, ["Converti da IPv4 a IPv6"](#).

### Unire i nodi rimanenti al cluster

Dopo aver creato un nuovo cluster, utilizzare la procedura guidata di installazione del cluster per unire ciascun nodo rimanente al cluster, uno alla volta. La procedura guidata consente di configurare l'interfaccia di gestione dei nodi di ciascun nodo.

Quando si uniscono due nodi in un cluster, si crea una coppia ad alta disponibilità (ha). Se si uniscono 4 nodi, si creano due coppie ha. Per ulteriori informazioni su ha, vedere ["Scopri di più su ha"](#).

È possibile unire un solo nodo al cluster alla volta. Quando si inizia a unire un nodo al cluster, è necessario completare l'operazione di Unione per quel nodo e il nodo deve far parte del cluster prima di poter iniziare a unirsi al nodo successivo.

**Best practice:** se si dispone di un sistema FAS2720 con 24 o meno dischi NL-SAS, verificare che la configurazione dello storage predefinita sia impostata su Active/Passive (attivo/passivo) per ottimizzare le prestazioni. Per ulteriori informazioni, vedere ["Impostazione di una configurazione Active-passive sui nodi utilizzando la partizione dei dati root"](#)

1. Accedere al nodo a cui si intende accedere nel cluster.

L'installazione guidata del cluster viene avviata dalla console.

```
Welcome to the cluster setup wizard....
```

2. Riconoscere l'istruzione AutoSupport.



AutoSupport è attivato per impostazione predefinita.

```
Type yes to confirm and continue {yes}: yes
```

3. Seguire le istruzioni visualizzate sullo schermo per assegnare un indirizzo IP al nodo.

A partire da ONTAP 9.13.1, è possibile assegnare indirizzi IPv6 per le LIF di gestione sulle piattaforme A800 e FAS8700. Per le versioni di ONTAP precedenti alla 9.13.1 o per la versione 9.13.1 e successive su altre piattaforme, è necessario assegnare indirizzi IPv4 per le LIF di gestione, quindi convertire in IPv6 dopo aver completato la configurazione del cluster.

4. Premere **Invio** per continuare.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

5. Unire il nodo al cluster: `join`

6. Seguire le istruzioni sullo schermo per configurare il nodo e unirsi al cluster.

7. Una volta completata l'installazione, verificare che il nodo sia integro e idoneo a partecipare al cluster:  
`cluster show`

L'esempio seguente mostra un cluster dopo che il secondo nodo (cluster1-02) è stato Unito al cluster:

```
cluster1::> cluster show
Node                               Health  Eligibility
-----
cluster1-01                       true    true
cluster1-02                       true    true
```

È possibile accedere alla procedura guidata di configurazione del cluster per modificare i valori immessi per la SVM amministrativa o il nodo SVM utilizzando il comando di configurazione del cluster.

8. Ripetere questa operazione per ogni nodo rimanente.

### Al termine

Se necessario, ["Converti da IPv4 a IPv6"](#).

### Converti i LIF di gestione da IPv4 a IPv6

A partire da ONTAP 9.13.1, è possibile assegnare gli indirizzi IPv6 alle LIF di gestione sulle piattaforme A800 e FAS8700 durante la configurazione iniziale del cluster. Per le versioni di ONTAP precedenti alla 9.13.1 o per la versione 9.13.1 e successive su altre piattaforme, è necessario assegnare gli indirizzi IPv4 alle LIF di gestione, quindi convertire in indirizzi IPv6 dopo aver completato la configurazione del cluster.

### Fasi

1. Abilitare IPv6 per il cluster:

```
network options ipv6 modify -enable true
```

2. Impostare il privilegio su Advanced (avanzato):

```
set priv advanced
```

3. Visualizzare l'elenco dei prefissi RA appresi sulle varie interfacce:

```
network ndp prefix show
```

#### 4. Creare una LIF di gestione IPv6:

Utilizzare il formato `prefix::id` Nel parametro `address` per costruire manualmente l'indirizzo IPv6.

```
network interface create -vserver <svm_name> -lif <LIF> -home-node  
<home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask  
-length <netmask_length> -failover-policy <policy> -service-policy  
<service_policy> -auto-revert true
```

#### 5. Verificare che la LIF sia stata creata:

```
network interface show
```

#### 6. Verificare che l'indirizzo IP configurato sia raggiungibile:

```
network ping6
```

#### 7. Contrassegna LIF IPv4 come amministrativamente inattivo:

```
network interface modify -vserver <svm_name> -lif <lif_name> -status  
-admin down
```

#### 8. Eliminare la LIF di gestione IPv4:

```
network interface delete -vserver <svm_name> -lif <lif_name>
```

#### 9. Verificare che la LIF di gestione IPv4 sia stata eliminata:

```
network interface show
```

### Controllare il cluster con Active IQ Config Advisor

Dopo aver Unito tutti i nodi al nuovo cluster, eseguire Active IQ Config Advisor per convalidare la configurazione e verificare la presenza di errori di configurazione comuni.

Config Advisor è un'applicazione basata sul web che viene installata su laptop, macchina virtuale o server e funziona su piattaforme Windows, Linux e Mac.

Config Advisor esegue una serie di comandi per convalidare l'installazione e controllare lo stato generale della configurazione, inclusi gli switch del cluster e dello storage.

1. Scaricare e installare Active IQ Config Advisor.

["Active IQ Config Advisor"](#)

2. Avviare Active IQ e impostare una passphrase quando richiesto.
3. Rivedere le impostazioni e fare clic su **Save** (Salva).
4. Nella pagina **obiettivi**, fare clic su **convalida post-implementazione ONTAP**.
5. Scegliere la modalità guidata o Expert.

Se si sceglie la modalità guidata, gli switch collegati vengono rilevati automaticamente.

6. Inserire le credenziali del cluster.
7. (Facoltativo) fare clic su **Form Validate** (convalida modulo).
8. Per iniziare a raccogliere i dati, fare clic su **Save & Evaluate** (Salva e valuta).
9. Una volta completata la raccolta dei dati, in **Job Monitor > Actions** (monitoraggio del processo), visualizzare i dati raccolti facendo clic sull'icona **Data View** (visualizzazione dati) e visualizzare i risultati facendo clic sull'icona **Results** (risultati).
10. Risolvere i problemi identificati da Config Advisor.

## Sincronizzare l'ora di sistema nel cluster

La sincronizzazione dell'ora garantisce che ogni nodo del cluster abbia lo stesso tempo e previene gli errori CIFS e Kerberos.

È necessario configurare un server NTP (Network Time Protocol) presso la propria sede. A partire da ONTAP 9.5, è possibile configurare il server NTP con autenticazione simmetrica. Per ulteriori informazioni, vedere ["Gestione del tempo del cluster \(solo amministratori del cluster\)"](#).

È possibile sincronizzare l'ora nel cluster associando il cluster a uno o più server NTP.

1. Verificare che l'ora e il fuso orario del sistema siano impostati correttamente per ciascun nodo.

Tutti i nodi del cluster devono essere impostati sullo stesso fuso orario.

- a. Utilizzare il comando `cluster date show` per visualizzare la data, l'ora e il fuso orario correnti per ciascun nodo.

```
cluster1::> cluster date show
Node          Date          Time zone
-----
cluster1-01   01/06/2015 09:35:15 America/New_York
cluster1-02   01/06/2015 09:35:15 America/New_York
cluster1-03   01/06/2015 09:35:15 America/New_York
cluster1-04   01/06/2015 09:35:15 America/New_York
4 entries were displayed.
```

- b. Utilizzare il comando `cluster date modify` per modificare la data o il fuso orario di tutti i nodi.

In questo esempio, il fuso orario del cluster viene modificato in GMT:

```
cluster1::> cluster date modify -timezone GMT
```

2. Utilizzare il comando `cluster time-service ntp server create` per associare il cluster al server NTP.

- Per configurare il server NTP senza autenticazione simmetrica, immettere il seguente comando:  
`cluster time-service ntp server create -server server_name`
- Per configurare il server NTP con autenticazione simmetrica, immettere il seguente comando:  
`cluster time-service ntp server create -server server_ip_address -key-id key_id`



L'autenticazione simmetrica è disponibile a partire da ONTAP 9.5. Non è disponibile in ONTAP 9.4 o versioni precedenti.

Questo esempio presuppone che il DNS sia stato configurato per il cluster. Se il DNS non è stato configurato, specificare l'indirizzo IP del server NTP:

```
cluster1::> cluster time-service ntp server create -server  
ntp1.example.com
```

3. Verificare che il cluster sia associato a un server NTP: `cluster time-service ntp server show`

```
cluster1::> cluster time-service ntp server show  
Server                Version  
-----  
ntp1.example.com      auto
```

## Informazioni correlate

["Amministrazione del sistema"](#)

## Comandi per la gestione dell'autenticazione simmetrica sui server NTP

A partire da ONTAP 9.5, è supportato il protocollo NTP (Network Time Protocol) versione 3. NTPv3 include l'autenticazione simmetrica utilizzando chiavi SHA-1 che aumenta la sicurezza della rete.

A tal fine...	Utilizzare questo comando...
Configurare un server NTP senza autenticazione simmetrica	<code>cluster time-service ntp server create -server server_name</code>

A tal fine...	Utilizzare questo comando...
Configurare un server NTP con autenticazione simmetrica	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
<p>Abilitare l'autenticazione simmetrica per un server NTP esistente</p> <p>È possibile modificare un server NTP esistente per abilitare l'autenticazione aggiungendo l'ID chiave richiesto.</p>	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
Configurare una chiave NTP condivisa	<code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code> <p><b>Nota:</b> le chiavi condivise sono indicate da un ID. L'ID, il tipo e il valore devono essere identici sia sul nodo che sul server NTP</p>
Configurare un server NTP con un ID chiave sconosciuto	<code>cluster time-service ntp server create -server server_name -key-id key_id</code>
Configurare un server con un ID chiave non configurato sul server NTP.	<code>cluster time-service ntp server create -server server_name -key-id key_id</code> <p><b>Nota:</b> l'ID, il tipo e il valore della chiave devono essere identici all'ID, al tipo e al valore della chiave configurati sul server NTP.</p>
Disattiva autenticazione simmetrica	<code>cluster time-service ntp server modify -server server_name -authentication disabled</code>

### Attività aggiuntive di configurazione del sistema da completare

Dopo aver configurato un cluster, è possibile utilizzare Gestore di sistema o l'interfaccia della riga di comando (CLI) di ONTAP per continuare la configurazione del cluster.

Attività di configurazione del sistema	Risorsa
<p>Configurare la rete:</p> <ul style="list-style-type: none"> <li>• Creare domini di broadcast</li> <li>• Creare sottoreti</li> <li>• Creare spazi IP</li> </ul>	<a href="#">"Configurazione della rete"</a>



Attività di configurazione del sistema	Risorsa
Configurare il Service Processor	<a href="#">"Amministrazione del sistema"</a>
Disporre gli aggregati	<a href="#">"Gestione di dischi e aggregati"</a>
Creazione e configurazione di macchine virtuali per lo storage dei dati (SVM)	<a href="#">"Configurazione NFS"</a> <a href="#">"Configurazione SMB"</a> <a href="#">"Amministrazione SAN"</a>
Configurare le notifiche degli eventi	<a href="#">"Configurazione EMS"</a>

## Configurare il software di array SAN all-flash

### Panoramica della configurazione del software degli array SAN all-flash

Gli array SAN all-flash NetApp (ASA) sono disponibili a partire da ONTAP 9,7. Gli ASA sono soluzioni solo SAN all-flash basate su piattaforme NetApp AFF comprovate.

Le piattaforme ASA utilizzano Active-Active simmetrico per il multipathing. Tutti i percorsi sono attivi/ottimizzati, quindi in caso di failover dello storage, l'host non deve attendere che la transizione ALUA dei percorsi di failover riprenda l'i/O. In questo modo si riduce il tempo di failover.

#### Configurare un ASA

Gli All-Flash SAN Array (ASA) seguono la stessa procedura di configurazione dei sistemi non ASA.

System Manager guida l'utente attraverso le procedure necessarie per inizializzare il cluster, creare un Tier locale, configurare i protocolli e eseguire il provisioning dello storage per ASA.

[Inizia subito a configurare il cluster di ONTAP.](#)

#### Impostazioni e utility dell'host ASA

Le impostazioni dell'host per la configurazione degli array SAN all-flash (ASA) sono identiche a quelle di tutti gli altri host SAN.

È possibile scaricare ["Software NetApp host Utilities"](#) per gli host specifici dal sito di supporto.

#### Metodi per identificare un sistema ASA

È possibile identificare un sistema ASA utilizzando Gestione di sistema o l'interfaccia a riga di comando (CLI) di ONTAP.

- **Dalla dashboard di System Manager:** Fare clic su **Cluster > Overview** e selezionare il nodo di sistema.

La **PERSONALITÀ** viene visualizzata come **All-Flash SAN Array**.

- **Dalla CLI:** Immettere il `san config show` comando.

Il valore dell'array SAN all-flash restituisce il valore vero per i sistemi ASA.

#### Informazioni correlate

- ["Report tecnico 4968: Integrità e disponibilità dei dati degli array NetApp All-SAN"](#)
- ["Report tecnico NetApp 4080: Best practice per le SAN moderne"](#)

#### Limiti di configurazione e supporto degli array SAN all-flash

I limiti di configurazione e il supporto degli array SAN all-flash (ASA) variano in base alla versione di ONTAP.

I dettagli più aggiornati sui limiti di configurazione supportati sono disponibili in ["NetApp Hardware Universe"](#).

#### Protocolli SAN e nodi per cluster

Il supporto ASA per i protocolli SAN e i nodi per cluster è il seguente:

Inizio con ONTAP...	Supporto del protocollo	Numero massimo di nodi per cluster
9.12.1	<ul style="list-style-type: none"><li>• NVMe (supportato nelle configurazioni MetroCluster IP a 4 nodi e nelle configurazioni IP non MetroCluster)</li><li>• FC</li><li>• ISCSI</li></ul>	12
9.9.1	<ul style="list-style-type: none"><li>• NVMe (supportato nelle configurazioni IP non MetroCluster)</li><li>• FC</li><li>• ISCSI</li></ul>	<ul style="list-style-type: none"><li>• 12 nodi (per configurazioni IP non MetroCluster)</li><li>• 8 nodi (per le configurazioni IP MetroCluster)</li></ul>
9.7	<ul style="list-style-type: none"><li>• FC</li><li>• ISCSI</li></ul>	4

#### Supporto per porte persistenti

A partire da ONTAP 9,8, le porte persistenti sono abilitate per impostazione predefinita sugli array All-Flash SAN (ASA) configurati per utilizzare il protocollo FC. Le porte persistenti sono disponibili solo per FC e richiedono l'appartenenza alla zona identificata dal World Wide Port Name (WWPN).

Le porte persistenti riducono l'impatto dei takeover creando una LIF shadow sulla porta fisica corrispondente del partner ha. Quando un nodo viene sostituito, la LIF shadow sul nodo partner assume l'identità della LIF originale, inclusa la WWPN. Prima che lo stato del percorso verso il nodo preso in consegna venga modificato in difettoso, la LIF shadow viene visualizzata come percorso attivo/ottimizzato verso lo stack MPIO host e l'i/o viene spostato. In questo modo si riducono le interruzioni di i/o perché l'host rileva sempre lo stesso numero di percorsi verso la destinazione, anche durante le operazioni di failover dello storage.

Per le porte persistenti, le seguenti caratteristiche della porta FCP devono essere identiche all'interno della coppia ha:

- Numero di porte FCP
- Nomi delle porte FCP
- Velocità delle porte FCP
- Zoning basato su WWPN FCP LIF

Se una di queste caratteristiche non è identica all'interno della coppia ha, viene generato il seguente messaggio EMS:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Per ulteriori informazioni sulle porte persistenti, vedere ["Report tecnico NetApp 4080: Best practice per le SAN moderne"](#).

## Aggiornare ONTAP

### Panoramica sull'aggiornamento di ONTAP

Quando aggiorni il software ONTAP, puoi sfruttare le nuove e migliorate funzionalità di ONTAP che possono aiutarti a ridurre i costi, accelerare i carichi di lavoro critici, migliorare la sicurezza ed espandere l'ambito di protezione dei dati disponibile per la tua organizzazione.

Un aggiornamento ONTAP principale consiste nel passare da una versione con numero inferiore a una versione con numero ONTAP superiore. Ad esempio, un upgrade del cluster da ONTAP 9.8 a ONTAP 9.12.1.

Un aggiornamento minore (o patch) consiste nel passare da una versione ONTAP inferiore a una versione ONTAP superiore all'interno della stessa versione numerata. Un esempio potrebbe essere l'aggiornamento del cluster da ONTAP 9.12.1P1 a 9.12.1P4.

Per iniziare, è necessario ["preparazione per l'aggiornamento"](#). Se si dispone di un contratto SupportEdge attivo per Active IQ Digital Advisor, è necessario ["Pianificate l'aggiornamento con Upgrade Advisor"](#). Upgrade Advisor fornisce informazioni che consentono di ridurre al minimo le incertezze e i rischi valutando il cluster e creando un piano di upgrade specifico per la configurazione in uso.

Dopo la preparazione per l'aggiornamento, si consiglia di eseguire gli aggiornamenti utilizzando ["Upgrade automatizzato senza interruzioni \(ANDU\) da System Manager"](#). ANDU sfrutta la tecnologia di failover ad alta disponibilità (ha) di ONTAP per garantire che i cluster continuino a servire i dati senza interruzioni durante l'upgrade.



A partire da ONTAP 9.12.1, System Manager è completamente integrato con BlueXP. Se BlueXP è configurato sul tuo sistema, puoi eseguire l'aggiornamento tramite l'ambiente di lavoro BlueXP.

Se desideri assistenza per l'aggiornamento del software ONTAP, i servizi di assistenza professionale NetApp offrono una ["Servizio di upgrade gestito"](#). Se siete interessati a utilizzare questo servizio, contattate il vostro rappresentante commerciale NetApp o ["Inviare il modulo per la richiesta di informazioni sulle vendite NetApp"](#). Il Servizio di aggiornamento gestito e altri tipi di supporto per l'aggiornamento sono disponibili per i clienti con ["Servizi SupportEdge Expert"](#) senza costi aggiuntivi.

## Quando è necessario aggiornare ONTAP?

È necessario aggiornare regolarmente il software ONTAP. L'aggiornamento di ONTAP consente di sfruttare funzioni e funzionalità nuove e migliorate e di implementare le correzioni correnti per i problemi noti.

### Principali aggiornamenti di ONTAP

Un importante aggiornamento ONTAP o una release di funzionalità generalmente include:

- Nuove funzioni di ONTAP
- Modifiche chiave all'infrastruttura, come modifiche fondamentali al funzionamento di NetApp WAFL o al funzionamento di RAID
- Supporto dei nuovi sistemi hardware sviluppati da NetApp
- Supporto per componenti hardware sostitutivi, come schede di interfaccia di rete più recenti o adattatori bus host

Le nuove release ONTAP hanno diritto al supporto completo per 3 anni. NetApp consiglia di eseguire la release più recente per 1 anno dopo la disponibilità generale (GA), quindi utilizzare il tempo rimanente nella finestra di supporto completa per pianificare la transizione a una release ONTAP più recente.

### Aggiornamenti patch ONTAP

Gli aggiornamenti delle patch forniscono correzioni tempestive per bug critici che non possono attendere la prossima importante release delle funzionalità di ONTAP. Gli aggiornamenti delle patch non critiche devono essere applicati ogni 3-6 mesi. Gli aggiornamenti critici delle patch devono essere applicati il più presto possibile.

Scopri di più ["livelli minimi consigliati di patch"](#) Per le versioni ONTAP.

### Date di pubblicazione di ONTAP

A partire dalla release ONTAP 9,8, NetApp rilascia le release di ONTAP due volte all'anno. Anche se i piani sono soggetti a modifiche, l'intento è quello di rilasciare nuove release ONTAP nel secondo e quarto trimestre di ogni anno solare. Utilizzate queste informazioni per pianificare il periodo di tempo necessario per l'aggiornamento e usufruire della versione più recente di ONTAP.

Versione	Data di rilascio
9.14.1	Gennaio 2024
9.13.1	Giugno 2023
9.12.1	Febbraio 2023
9.11.1	Luglio 2022
9.10.1	Gennaio 2022
9.9.1	Giugno 2021

## Livelli di supporto ONTAP

Il livello di supporto disponibile per una specifica versione di ONTAP varia a seconda della data di rilascio del software.

Livello di supporto	Supporto completo			Supporto limitato		Supporto self-service		
Anno	1	2	3	4	5	6	7	8
Accesso alla documentazione online	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
Supporto tecnico	Sì	Sì	Sì	Sì	Sì			
Analisi delle cause alla radice	Sì	Sì	Sì	Sì	Sì			
Download di software	Sì	Sì	Sì	Sì	Sì			
Aggiornamenti di servizio (release di patch [release P])	Sì	Sì	Sì					
Avvisi sulle vulnerabilità	Sì	Sì	Sì					

### Informazioni correlate

- Scopri ["Novità delle release ONTAP attualmente supportate"](#).
- Scopri di più ["Release ONTAP minime consigliate"](#).
- Scopri di più ["Supporto delle versioni del software ONTAP"](#).
- Scopri di più su ["Modello di release ONTAP"](#).

## Eseguire controlli pre-aggiornamento automatici ONTAP prima di un upgrade pianificato

Non è necessario aggiornare il software ONTAP per eseguire i controlli preliminari dell'aggiornamento automatico ONTAP. L'esecuzione dei controlli di pre-aggiornamento indipendentemente dal processo di aggiornamento automatico di ONTAP consente di vedere quali controlli vengono eseguiti sul cluster e fornisce un elenco di eventuali errori o avvisi da correggere prima di iniziare l'aggiornamento effettivo. Ad esempio, si supponga di voler aggiornare il software ONTAP durante una finestra di manutenzione programmata entro due settimane. In attesa della data pianificata, è possibile eseguire i controlli preliminari dell'aggiornamento automatico e intraprendere tutte le azioni correttive necessarie prima della finestra di manutenzione. In questo modo si riducono i rischi di errori di configurazione imprevisti dopo l'avvio dell'aggiornamento.

Per iniziare l'aggiornamento del software ONTAP, non è necessario eseguire questa procedura. È necessario seguire la "[processo di aggiornamento automatizzato](#)", che include l'esecuzione dei controlli preliminari di aggiornamento automatici.



Per le configurazioni MetroCluster, eseguire prima questi passaggi sul cluster A, quindi eseguire gli stessi passaggi sul cluster B.

### **Prima di iniziare**

Dovresti "[Scaricare l'immagine del software ONTAP di destinazione](#)".

Per eseguire i controlli preliminari dell'upgrade automatico per un "[upgrade diretto multi-hop](#)", È sufficiente scaricare il pacchetto software per la versione ONTAP di destinazione. Non sarà necessario caricare la versione ONTAP intermedia finché non si inizia l'aggiornamento effettivo. Ad esempio, se si eseguono controlli automatici di pre-aggiornamento per un aggiornamento da 9,8 a 9.13.1, è necessario scaricare il pacchetto software per ONTAP 9.13.1. Non è necessario scaricare il pacchetto software per ONTAP 9.12.1.

## Esempio 1. Fasi

### System Manager

#### 1. Convalida dell'immagine di destinazione ONTAP:



Se si sta aggiornando una configurazione MetroCluster, è necessario convalidare il cluster A e ripetere la procedura di convalida sul cluster B.

#### a. A seconda della versione di ONTAP in esecuzione, eseguire una delle seguenti operazioni:

Se si esegue...	Eseguire questa operazione...
ONTAP 9.8 o versione successiva	Fare clic su <b>Cluster &gt; Overview</b> (Cluster > Panoramica).
ONTAP 9.5, 9.6 e 9.7	Fare clic su <b>Configuration &gt; Cluster &gt; Update</b> .
ONTAP 9.4 o versioni precedenti	Fare clic su <b>Configuration &gt; Cluster Update</b> .

#### b. Nell'angolo destro del riquadro **Panoramica**, fare clic su .

#### c. Fare clic su **aggiornamento ONTAP**.

#### d. Nella scheda **Cluster Update**, aggiungere una nuova immagine o selezionare un'immagine disponibile.

Se si desidera...	Quindi...
Aggiungere una nuova immagine software da una cartella locale  Dovresti già averlo fatto "immagine scaricata" al client locale.	<ul style="list-style-type: none"><li>i. In <b>immagini software disponibili</b>, fare clic su <b>Aggiungi da locale</b>.</li><li>ii. Individuare la posizione in cui è stata salvata l'immagine software, selezionare l'immagine, quindi fare clic su <b>Apri</b>.</li></ul>
Aggiungere una nuova immagine software da un server HTTP o FTP	<ul style="list-style-type: none"><li>i. Fare clic su <b>Aggiungi dal server</b>.</li><li>ii. Nella finestra di dialogo <b>Aggiungi nuova immagine software</b>, immettere l'URL del server HTTP o FTP sul quale è stata scaricata l'immagine del software ONTAP dal sito di supporto NetApp.  Per l'FTP anonimo, è necessario specificare l'URL in <a href="#">ftp://anonymous@ftpserver</a> formato.</li><li>iii. Fare clic su <b>Aggiungi</b>.</li></ul>
Selezionare un'immagine disponibile	Scegliere una delle immagini elencate.



e. Fare clic su **convalida** per eseguire i controlli di convalida pre-aggiornamento.

Se durante la convalida vengono rilevati errori o avvisi, questi vengono visualizzati insieme a un elenco di azioni correttive. È necessario risolvere tutti gli errori prima di procedere con l'aggiornamento. È buona norma risolvere anche gli avvisi.

## CLI

1. Caricare l'immagine software ONTAP di destinazione nell'archivio dei pacchetti cluster:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url  
http://www.example.com/software/9.13.1/image.tgz
```

```
Package download completed.  
Package processing completed.
```

2. Verificare che il pacchetto software sia disponibile nel repository dei pacchetti del cluster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository  
Package Version  Package Build Time  
-----  
9.13.1           MM/DD/YYYY 10:32:15
```

3. Eseguire i controlli automatici pre-aggiornamento:

```
cluster image validate -version package_version_number -show  
-validation-details true
```



Se si sta eseguendo un "upgrade diretto multi-hop", Utilizzare il pacchetto ONTAP di destinazione per la verifica. Non è necessario convalidare separatamente l'immagine di aggiornamento intermedia. Ad esempio, se si esegue l'aggiornamento da 9.8 a 9.13.1, è necessario utilizzare il pacchetto 9.13.1 per la verifica. Non è necessario convalidare il pacchetto 9.12.1 separatamente.

```
cluster1::> cluster image validate -version 9.14.1 -show-validation  
-details true
```

It can take several minutes to complete validation...  
Validation checks started successfully. Run the "cluster image  
show-update-progress" command to check validation status.

#### 4. Controllare lo stato di convalida:

```
cluster image show-update-progress
```



Se lo **Stato** è "in corso", attendere ed eseguire nuovamente il comando fino al completamento.

```
cluster1::*> cluster image show-update-progress
```

Update Phase	Status	Duration
Pre-update checks	completed	00:10:00

Details:

Pre-update Check	Status	Error-Action
AMPQ Router and Broker Config Cleanup	OK	N/A
Aggregate online status and parity check	OK	N/A
Aggregate plex resync status check	OK	N/A
Application Provisioning Cleanup	OK	N/A
Autoboot Bootargs Status	OK	N/A
Backend	OK	N/A
...		
Volume Conversion In Progress Check	OK	N/A
Volume move progress status check	OK	N/A
Volume online status check	OK	N/A
iSCSI target portal groups status check	OK	N/A
Overall Status	Warning	Warning

75 entries were displayed.

Viene visualizzato un elenco di controlli preliminari completi dell'aggiornamento automatico insieme a eventuali errori o avvisi che devono essere risolti prima di iniziare il processo di aggiornamento.



## Esempio di output completo dei controlli preliminari di aggiornamento

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
```

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed successfully.

Refer to the Upgrade Advisor Plan or the "What should I verify before I upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP" documentation for the remaining manual validation checks that need to be performed before update.

Upgrade ONTAP documentation available at: <https://docs.netapp.com/us-en/ontap/upgrade/index.html>

The list of checks are available at: [https://docs.netapp.com/us-en/ontap/upgrade/task\\_what\\_to\\_check\\_before\\_upgrade.html](https://docs.netapp.com/us-en/ontap/upgrade/task_what_to_check_before_upgrade.html)

Failing to do so can result in an update failure or an I/O disruption. Please use Interoperability Matrix Tool (IMT <http://mysupport.netapp.com/matrix>) to verify host system supportability configuration information.

Validation checks started successfully. Run the "cluster image show-update-progress" command to check validation status.

```
fas2820-2n-wic-1::*> cluster image show-update-progress
```

Update Phase	Status	Estimated Duration	Elapsed Duration
Pre-update checks	in-progress	00:10:00	00:00:42

Details:

Pre-update Check	Status	Error-Action
-----	-----	-----
-----	-----	-----

```
fas2820-2n-wic-1::*> cluster image show-update-progress
```

Update Phase	Status	Estimated Duration	Elapsed Duration
Pre-update checks	completed	00:10:00	00:01:03

# Details:

Pre-update Check	Status	Error-Action
-----	-----	-----
AMPQ Router and Broker Config Cleanup	OK	N/A
Aggregate online status and parity check	OK	N/A
Aggregate plex resync status check	OK	N/A
Application Provisioning Cleanup	OK	N/A
Autoboot Bootargs Status	OK	N/A
Backend Configuration Status	OK	N/A
Boot Menu Status	Warning	Warning: bootarg.init.bootmenu is  enabled on nodes: fas2820-wic- 1a,  fas2820-wic-1b. The boot process of  the nodes will be delayed. Action: Set the  bootarg.init.bootmenu  bootarg to false before  proceeding  with the upgrade.
Broadcast Domain availability and uniqueness for HA pair status	OK	N/A
CIFS compatibility status check	OK	N/A
CLAM quorum online status check	OK	N/A
CPU Utilization Status	OK	N/A
Capacity licenses install status check	OK	N/A
Check For SP/BMC Connectivity To Nodes	OK	N/A

Check LDAP fastbind users using unsecure connection.	OK	N/A
Check for unsecure kex algorithm configurations.	OK	N/A
Check for unsecure mac configurations.	OK	N/A
Cloud keymanager connectivity check	OK	N/A
Cluster health and eligibility status	OK	N/A
Cluster quorum status check	OK	N/A
Cluster/management switch check	OK	N/A
Compatible New Image Check	OK	N/A
Current system version check if it is susceptible to possible outage during NDU	OK	N/A
Data ONTAP Version and Previous Upgrade Status	OK	N/A
Data aggregates HA policy check	OK	N/A
Disk status check for failed, broken or non-compatibility	OK	N/A
Duplicate Initiator Check	OK	N/A
Encryption key migration status check	OK	N/A
External key-manager with legacy KMIP client check	OK	N/A
External keymanager key server status check	OK	N/A
Fabricpool Object Store Availability	OK	N/A
High Availability	OK	N/A



configuration		
status check		
Infinite Volume	OK	N/A
availability check		
LIF failover	OK	N/A
capability status		
check		
LIF health check	OK	N/A
LIF load balancing	OK	N/A
status check		
LIFs is on home	OK	N/A
node status		
Logically over	OK	N/A
allocated DP		
volumes check		
MetroCluster	OK	N/A
configuration		
status check for		
compatibility		
Minimum number of	OK	N/A
aggregate disks		
check		
NAE Aggregate and	OK	N/A
NVE Volume		
Encryption Check		
NDMP sessions check	OK	N/A
NFS mounts status	Warning	Warning: This cluster is serving
NFS		
check		clients. If NFS soft mounts are
used,		
		there is a possibility of
frequent		
		NFS timeouts and race conditions
that		
		can lead to data corruption
during		
		the upgrade.
		Action: Use NFS hard mounts, if
		possible. To list Vservers
running		
		NFS, run the following command:
		vserver nfs show
Name Service	OK	N/A
Configuration DNS		
Check		
Name Service	OK	N/A

## Configuration LDAP

### Check

Node to SP/BMC connectivity check	OK	N/A
OKM/KMIP enabled systems - Missing keys check	OK	N/A
ONTAP API to REST transition warning data last 30 days approaching automation REST	Warning	Warning: NetApp ONTAP API has been used on this cluster for ONTAP storage management within the last 30 days. NetApp ONTAP API is approaching end of availability. Action: Transition your tools from ONTAP API to ONTAP API. For more details, refer to CPC-00410 - End of availability: ONTAPI
		<a href="https://mysupport.netapp.com/info/communications/ECMLP2880232.html">https://mysupport.netapp.com/info/communications/ECMLP2880232.html</a>
ONTAP Image Capability Status	OK	N/A
OpenSSL 3.0.x upgrade validation check	OK	N/A
Openssh 7.2 upgrade validation check	OK	N/A
Platform Health Monitor check	OK	N/A
Pre-Update Configuration Verification	OK	N/A
RDB Replica Health Check	OK	N/A
Replicated database schema consistency check	OK	N/A
Running Jobs Status	OK	N/A
SAN LIF association status check	OK	N/A

SAN compatibility for manual configurability check	OK	N/A
SAN kernel agent status check	OK	N/A
Secure Purge operation Check	OK	N/A
Shelves and Sensors check	OK	N/A
SnapLock Version Check	OK	N/A
SnapMirror Synchronous relationship status check	OK	N/A
SnapMirror compatibility status check	OK	N/A
Supported platform check	OK	N/A
Target ONTAP release support for FiberBridge 6500N check	OK	N/A
Upgrade Version Compatibility Status	OK	N/A
Verify all bgp peer-groups are in the up state	OK	N/A
Verify if a cluster management LIF exists	OK	N/A
Verify that e0M is home to no LIFs with high speed services.	OK	N/A
Volume Conversion In Progress Check	OK	N/A
Volume move progress status check	OK	N/A
Volume online status check	OK	N/A
iSCSI target portal groups status check	OK	N/A

Overall Status      Warning      Warning  
75 entries were displayed.

## Prepararsi per un aggiornamento di ONTAP

### Prepararsi per un aggiornamento del software ONTAP

La preparazione corretta per un aggiornamento software ONTAP consente di identificare e ridurre i potenziali rischi o blocchi di aggiornamento prima di iniziare il processo di aggiornamento. Durante la preparazione dell'aggiornamento, è inoltre possibile identificare eventuali considerazioni speciali che potrebbero essere necessarie prima di eseguire l'aggiornamento. Ad esempio, se la modalità SSL FIPS è attivata sul cluster e gli account amministratore utilizzano chiavi pubbliche SSH per l'autenticazione, è necessario verificare che l'algoritmo della chiave host sia supportato nella versione ONTAP di destinazione.

Per preparare l'aggiornamento, effettuare le seguenti operazioni:

1. ["Creare un piano di aggiornamento"](#).

Se si dispone di un contratto SupportEdge attivo per ["Consulente digitale Active IQ"](#), Pianificare l'aggiornamento con Upgrade Advisor. Se non si dispone dell'accesso a Active IQ Digital Advisor, creare un piano di aggiornamento personalizzato.

2. ["Scegli la tua versione ONTAP di destinazione"](#).

3. Esaminare ["Note di rilascio di ONTAP"](#) per la release di destinazione.

La sezione "attenzione all'aggiornamento" descrive i potenziali problemi da tenere presenti prima di eseguire l'aggiornamento alla nuova release. Le sezioni "Novità" e "problemi e limitazioni noti" descrivono il nuovo comportamento del sistema dopo l'aggiornamento alla nuova versione.

4. ["Verificare il supporto ONTAP per la configurazione hardware"](#).

La piattaforma hardware, gli switch per la gestione del cluster e gli switch IP MetroCluster devono supportare la release di destinazione. Se il cluster è configurato per SAN, la configurazione SAN deve essere completamente supportata.

5. ["Utilizzare Active IQ Config Advisor per verificare che non siano presenti errori di configurazione comuni."](#)

6. Esaminare il ONTAP supportato ["percorsi di aggiornamento"](#) per determinare se è possibile eseguire un aggiornamento diretto o se è necessario completare l'aggiornamento in fasi.

7. ["Verifica della configurazione di failover della LIF"](#).

Prima di eseguire un aggiornamento, è necessario verificare che i criteri di failover del cluster e i gruppi di failover siano configurati correttamente.

8. ["Verificare la configurazione del routing SVM"](#).

9. ["Verificare le considerazioni speciali"](#) per il tuo cluster.

Se nel cluster esistono determinate configurazioni, è necessario intraprendere azioni specifiche prima di

iniziare un aggiornamento software di ONTAP.

10. ["Riavviare SP o BMC"](#).

## Creare un piano di aggiornamento ONTAP

È consigliabile creare un piano di aggiornamento. Se si dispone di un'opzione attiva ["Servizi SupportEdge"](#) contratto per ["Consulente digitale Active IQ"](#), È possibile utilizzare Upgrade Advisor per generare un piano di aggiornamento. In caso contrario, è necessario creare un piano personalizzato.

### Pianifica l'upgrade con Upgrade Advisor

Il servizio Upgrade Advisor di Active IQ Digital Advisor fornisce informazioni utili per pianificare l'upgrade e ridurre al minimo incertezza e rischi.

Active IQ identifica i problemi dell'ambiente che possono essere risolti eseguendo l'aggiornamento a una versione più recente di ONTAP. Il servizio preparazione aggiornamento ti aiuta a pianificare un aggiornamento corretto e fornisce un report dei problemi che potresti dover essere a conoscenza della versione di ONTAP a cui stai eseguendo l'aggiornamento.

### Fasi

1. ["Avviare Active IQ"](#)
2. A Active IQ ["visualizza tutti i rischi associati al cluster ed esegui manualmente azioni correttive"](#).

I rischi inclusi nelle categorie **Modifica configurazione SW**, **Modifica configurazione HW** e **Sostituzione HW** devono essere risolti prima di eseguire un aggiornamento ONTAP.

3. Esaminare il percorso di aggiornamento consigliato e. ["genera il tuo piano di upgrade"](#).

### Quanto tempo richiede un aggiornamento di ONTAP?

Dovresti pianificare per almeno 30 minuti di completamento dei passaggi preparatori per un upgrade di ONTAP, 60 minuti per eseguire l'upgrade di ciascuna coppia ha e almeno 30 minuti per completare i passaggi successivi all'upgrade.



Se si utilizza NetApp Encryption con un server di gestione delle chiavi esterno e il protocollo KMIP (Key Management Interoperability Protocol), l'aggiornamento di ciascuna coppia ha dovrebbe essere superiore a un'ora.

Queste linee guida sulla durata dell'aggiornamento si basano su configurazioni e carichi di lavoro tipici. È possibile utilizzare queste linee guida per stimare il tempo necessario per eseguire un aggiornamento senza interruzioni nel proprio ambiente. La durata effettiva del processo di upgrade dipende dal singolo ambiente e dal numero di nodi.

### Scegliere la versione ONTAP di destinazione per un aggiornamento

Utilizzando Upgrade Advisor per generare un piano di upgrade per il cluster, è prevista una release ONTAP di destinazione consigliata per l'aggiornamento. Il consiglio fornito da Upgrade Advisor si basa sulla configurazione corrente e sulla versione ONTAP corrente.

Se non si utilizza Upgrade Advisor per pianificare l'aggiornamento, è necessario scegliere la versione ONTAP

di destinazione per l'aggiornamento in base ai consigli NetApp o la versione minima necessaria per soddisfare le esigenze di prestazioni del .

- Aggiornamento all'ultima versione disponibile (consigliato)

NetApp consiglia di aggiornare il software ONTAP all'ultima versione della patch dell'ultima versione numerata di ONTAP. Se ciò non è possibile perché l'ultima release numerata non è supportata dai sistemi storage nel cluster, è necessario eseguire l'aggiornamento all'ultima release numerata supportata.

- Versione minima consigliata

Per limitare l'upgrade alla release minima consigliata per il cluster, consulta la sezione ["Release ONTAP minime consigliate"](#) Per determinare la versione di ONTAP a cui eseguire l'aggiornamento.

## Verificare il supporto ONTAP per la configurazione hardware

Prima di aggiornare ONTAP, è necessario verificare che la configurazione hardware sia in grado di supportare la versione ONTAP di destinazione.

### Tutte le configurazioni

Utilizzare ["NetApp Hardware Universe"](#) Per confermare che la piattaforma hardware e gli switch per cluster e gestione sono supportati nella versione ONTAP di destinazione. Il cluster e gli switch di gestione includono switch di rete cluster (NX-OS), switch di rete di gestione (IOS) e file di configurazione di riferimento (RCF). Se il cluster e gli switch di gestione sono supportati, ma non eseguono le versioni minime del software richieste per la release ONTAP di destinazione, aggiorna gli switch alle versioni software supportate.

- ["Download NetApp: Switch cluster Broadcom"](#)
- ["Download NetApp: Switch Ethernet Cisco"](#)
- ["Download NetApp: Switch cluster NetApp"](#)



Se è necessario aggiornare gli switch, NetApp consiglia di completare prima l'aggiornamento del software ONTAP, quindi eseguire l'aggiornamento del software per gli switch.

### Configurazioni MetroCluster

Prima di aggiornare ONTAP, se si dispone di una configurazione MetroCluster, utilizzare ["Tool di matrice di interoperabilità NetApp"](#) Per verificare che gli switch IP MetroCluster in uso siano supportati nella versione ONTAP di destinazione.

### Configurazioni SAN

Prima di aggiornare ONTAP, se il cluster è configurato per SAN, utilizzare l' ["Tool di matrice di interoperabilità NetApp"](#) Per verificare che la configurazione SAN sia completamente supportata.

Tutti i componenti SAN, inclusi la versione del software ONTAP di destinazione, il sistema operativo host e le patch, il software delle utility host richiesto, il software di multipathing, i driver e il firmware dell'adattatore, devono essere supportati.

## Identificare gli errori di configurazione con Active IQ Config Advisor

Prima di aggiornare ONTAP, è possibile utilizzare lo strumento Active IQ Config Advisor

per verificare la presenza di errori di configurazione comuni.

Active IQ Config Advisor è un tool di convalida della configurazione per i sistemi NetApp. Può essere implementato su siti protetti e siti non protetti per raccolta di dati e analisi del sistema.



Il supporto per Active IQ Config Advisor è limitato ed è disponibile solo online.

## Fasi

1. Accedere a ["Sito di supporto NetApp"](#), Quindi fare clic su **STRUMENTI > Strumenti**.
2. In **Active IQ Config Advisor**, fare clic su ["Scarica l'app"](#).
3. Scaricare, installare ed eseguire Active IQ Config Advisor.
4. Dopo aver eseguito Active IQ Config Advisor, rivedere l'output dello strumento e seguire i consigli forniti per risolvere eventuali problemi rilevati dallo strumento.

## Percorsi di aggiornamento ONTAP supportati

La versione di ONTAP aggiornabile dipende dalla piattaforma hardware e dalla versione di ONTAP attualmente in esecuzione sui nodi del cluster.

Per verificare che la piattaforma hardware in uso sia supportata per la versione di aggiornamento di destinazione, vedere ["NetApp Hardware Universe"](#). Utilizzare ["Tool di matrice di interoperabilità NetApp"](#) a ["verificare il supporto per la configurazione"](#).

### Per determinare la versione corrente di ONTAP:

- In System Manager, fare clic su **Cluster > Panoramica**.
- Dall'interfaccia della riga di comando (CLI), utilizzare `cluster image show` comando.  
È inoltre possibile utilizzare `system node image show` al livello di privilegi avanzati per visualizzare i dettagli.

## Tipi di percorsi di upgrade

Quando possibile, si consigliano aggiornamenti automatici senza interruzioni (ANU). A seconda delle release attuali e di destinazione, il percorso di aggiornamento sarà **diretto**, **diretto multi-hop** o **multi-stage**.

### • Diretto

È sempre possibile eseguire l'aggiornamento direttamente alla famiglia di versioni ONTAP adiacenti utilizzando un'unica immagine software. Per la maggior parte delle release, è anche possibile installare un'immagine software che consente di eseguire l'aggiornamento direttamente alle release che sono due release superiori a quella in esecuzione.

Ad esempio, è possibile utilizzare il percorso di aggiornamento diretto da 9.8 a 9.9 o da 9.8 a 9.10.1.

**Nota:** a partire da ONTAP 9.11.1, le immagini software supportano l'aggiornamento diretto a release che sono tre o più release superiori rispetto alla release in esecuzione. Ad esempio, è possibile utilizzare il percorso di aggiornamento diretto da 9,8 a 9.12.1.

Tutti i percorsi di aggiornamento *diretto* sono supportati per ["cluster di versioni miste"](#).

### • Direct multi-hop

Per alcuni upgrade automatici e senza interruzioni (ANDU) a release non adiacenti, è necessario installare l'immagine software per una release intermedia oltre alla release di destinazione. Il processo di



aggiornamento automatico utilizza l'immagine intermedia in background per completare l'aggiornamento alla release di destinazione.

Ad esempio, se il cluster esegue 9.3 e si desidera eseguire l'aggiornamento alla versione 9.7, caricare i pacchetti di installazione di ONTAP per 9.5 e 9.7, quindi avviare ANDU alla versione 9.7. ONTAP esegue automaticamente l'upgrade del cluster prima a 9,5, quindi a 9,7. Durante il processo, è necessario prevedere più operazioni di Takeover/giveback e relativi riavvii.

- **Multistadio**

Se non è disponibile un percorso multi-hop diretto o diretto per la release di destinazione non adiacente, è necessario prima eseguire l'aggiornamento a una release intermedia supportata, quindi eseguire l'aggiornamento alla release di destinazione.

Ad esempio, se si utilizza 9.6 e si desidera eseguire l'aggiornamento alla versione 9.11.1, è necessario completare un aggiornamento multi-fase: Prima da 9.6 a 9.8, quindi da 9.8 a 9.11.1. Gli aggiornamenti delle release precedenti potrebbero richiedere tre o più fasi, con diversi aggiornamenti intermedi.

**Nota:** prima di iniziare gli aggiornamenti multi-fase, assicurarsi che la release di destinazione sia supportata sulla piattaforma hardware.

Prima di iniziare un importante aggiornamento, si consiglia di eseguire l'aggiornamento alla versione più recente della patch di ONTAP in esecuzione nel cluster. In questo modo, tutti i problemi della versione corrente di ONTAP verranno risolti prima dell'aggiornamento.

Ad esempio, se nel sistema è in esecuzione ONTAP 9.3P9 e si prevede di eseguire l'aggiornamento alla versione 9.11.1, è necessario prima eseguire l'aggiornamento alla versione più recente della patch 9.3, quindi seguire il percorso di aggiornamento da 9.3 a 9.11.1.

Scopri di più ["Numero minimo di release ONTAP consigliate sul sito del supporto NetApp"](#).

#### Percorsi di upgrade supportati

I seguenti percorsi di aggiornamento sono supportati per gli aggiornamenti automatici e manuali del software ONTAP. Questi percorsi di upgrade si applicano a ONTAP e ONTAP Select on-premise. Ci sono diversi ["Percorsi di aggiornamento supportati per Cloud Volumes ONTAP"](#).



**Per i cluster ONTAP in versione mista:** Tutti i percorsi di aggiornamento *direct* e *direct multi-hop* includono le versioni ONTAP compatibili con i cluster in versione mista. Le versioni di ONTAP incluse negli aggiornamenti *multi-stage* non sono compatibili con i cluster di versioni miste. Ad esempio, un aggiornamento da 9,8 a 9.12.1 è un aggiornamento *diretto*. Un cluster con nodi che eseguono 9,8 e 9.12.1 è una versione mista supportata. Un aggiornamento da 9,8 a 9.13.1 è un aggiornamento *multi-stage*. Un cluster con nodi che eseguono 9,8 e 9.13.1 non è un cluster in versione mista supportata.

#### Da ONTAP 9.10.1 e successivi

Gli aggiornamenti automatici e manuali da ONTAP 9.10.1 e versioni successive seguono gli stessi percorsi di aggiornamento.

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico o manuale è...
9.13.1	9.14.1	diretto

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico o manuale è...
9.12.1	9.14.1	diretto
	9.13.1	diretto
9.11.1	9.14.1	diretto
	9.13.1	diretto
	9.12.1	diretto
9.10.1	9.14.1	diretto
	9.13.1	diretto
	9.12.1	diretto
	9.11.1	diretto

### Da ONTAP 9.9.1

Gli aggiornamenti automatici e manuali da ONTAP 9.9.1 seguono gli stessi percorsi di aggiornamento.

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico o manuale è...
9.9.1	9.14.1	multi-stage -9.9.1→9.13.1 -9.13.1→9.14.1
	9.13.1	diretto
	9.12.1	diretto
	9.11.1	diretto
	9.10.1	diretto

### Da ONTAP 9,8

Gli aggiornamenti automatici e manuali da ONTAP 9,8 seguono gli stessi percorsi di aggiornamento.



Se si sta aggiornando una configurazione IP di MetroCluster dalla versione 9,8 alla 9.10.1 o successiva su una delle seguenti piattaforme, è necessario eseguire l'aggiornamento alla versione 9.9.1 prima di eseguire l'aggiornamento alla versione 9.10.1 o successiva.

- FAS2750
- FAS500f
- AFF A220
- AFF A250

I cluster delle configurazioni MetroCluster IP su queste piattaforme non possono essere aggiornati direttamente dalla versione 9,8 alla 9.10.1 o successiva. I percorsi di aggiornamento diretto elencati possono essere utilizzati per tutte le altre piattaforme.

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico o manuale è...
9.8	9.14.1	multi-stage -9.8 → 9.12.1 -9.12.1 → 9.14.1
9.13.1	multi-stage -9.8 → 9.12.1 -9.12.1 → 9.13.1	9.12.1
diretto	9.11.1	diretto
9.10.1	diretto	9.9.1

### Da ONTAP 9,7

I percorsi di aggiornamento da ONTAP 9,7 possono variare a seconda che si stia eseguendo un aggiornamento automatico o manuale.

### Percorsi automatizzati

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
9.7	9.14.1	multi-stage -9.7 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-stage -9.7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multi-stage -9.7 → 9.8 -9.8 → 9.12.1
	9.11.1	multi-hop diretto (richiede immagini per 9,8 e 9.11.1)
	9.10.1	Multi-hop diretto (richiede immagini per 9,8 e 9.10.1P1 o versione successiva P)
	9.9.1	diretto
	9.8	diretto

### Percorsi manuali

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento manuale è...
9.7	9.14.1	multi-stage -9.7 → 9.8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-stage -9.7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multi-stage - 9.7 → 9.8 - 9.8 → 9.12.1
	9.11.1	multi-stage - 9.7 → 9.8 - 9.8 → 9.11.1
	9.10.1	multi-stage - 9.7 → 9.8 - 9.8 → 9.10.1
	9.9.1	diretto
	9.8	diretto

## Da ONTAP 9,6

I percorsi di aggiornamento da ONTAP 9,6 possono variare a seconda che si stia eseguendo un aggiornamento automatico o manuale.

### Percorsi automatizzati

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
9.6	9.14.1	multi-stage -9,6 → 9,8 -9.8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multi-stage -9,6 → 9,8 -9.8 → 9.12.1 -9.12.1 → 9.13.1
	9.12.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.12.1
	9.11.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.11.1
	9.10.1	Multi-hop diretto (richiede immagini per 9,8 e 9.10.1P1 o versione successiva P)
	9.9.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.9.1
	9.8	diretto
	9.7	diretto

### Percorsi manuali

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento manuale è...
9.6	9.14.1	multi-stage - 9,6 → 9,8 - 9.8 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.12.1
	9.11.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.11.1
	9.10.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.10.1
	9.9.1	multi-stage - 9.6 → 9.8 - 9.8 → 9.9.1
	9.8	diretto
	9.7	diretto

## **Da ONTAP 9,5**

I percorsi di aggiornamento da ONTAP 9,5 possono variare a seconda che si stia eseguendo un aggiornamento automatico o manuale.

## Percorsi automatizzati

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
9.5	9.14.1	multi-stage - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.10.1
	9.9.1	multi-hop diretto (richiede immagini per 9,7 e 9,9.1)
	9.8	multi-stage - 9.5 → 9.7 - 9.7 → 9.8
	9.7	diretto
	9.6	diretto

## Percorsi di aggiornamento manuale

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento manuale è...
9.5	9.14.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.5 → 9.7 - 9.7 → 9.8
	9.7	diretto
	9.6	diretto

### Da ONTAP 9,4-9,0

I percorsi di aggiornamento da ONTAP 9,4, 9,3, 9,2, 9,1 e 9,0 possono variare a seconda che si stia eseguendo un aggiornamento automatico o manuale.



Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
9.4	9.14.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1) - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop diretto, richiede immagini per 9,7 e 9,9.1)
	9.8	multi-stage - 9,4 → 9,5 - 9,5 → 9,8 (multi-hop diretto, richiede immagini per 9,7 e 9,8)
	9.7	multi-stage - 9.4 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.4 → 9.5 - 9.5 → 9.6
	9.5	diretto

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
9.3	9.14.1	multi-stage - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7) - 9.7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multi-stage - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7) - 9.7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multi-stage - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7) - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7) - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7) - 9,7 → 9.10.1 (multi-hop diretto, richiede immagini per 9,8 e 9.10.1)
	9.9.1	multi-stage - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7) - 9.7 → 9.9.1
	9.8	multi-stage - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7) - 9.7 → 9.8
	9.7	multi-hop diretto (richiede immagini per 9,5 e 9,7)
	9.6	multi-stage - 9.3 → 9.5 - 9.5 → 9.6
	9.5	diretto
	9.4	non disponibile

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
9.2		

	9.7	multi-stage - 9,2 → 9,3 - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7)
Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
		multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.3 → 9.5 - 9.5 → 9.6
	9.4	non disponibile
	9.3	diretto

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
9.1		

	9.7	multi-stage - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7)
Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è
	9.6	multi-stage - 9,1 → 9,3 - 9,3 → 9,6 (multi-hop diretto, richiede immagini per 9,5 e 9,6)
	9.5	multi-stage - 9.1 → 9.3 - 9.3 → 9.5
	9.4	non disponibile
	9.3	diretto
	9.2	non disponibile

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
9.0		

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il percorso di aggiornamento automatico è...
		- 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7) - 9,7 → 9.9.1
	9.8	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7) - 9.7 → 9.8
	9.7	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop diretto, richiede immagini per 9,5 e 9,7)
	9.6	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5
	9.4	non disponibile
	9.3	multi-stage - 9.0 → 9.1 - 9.1 → 9.3
	9.2	non disponibile
	9.1	diretto



## Percorsi di aggiornamento manuale

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il tuo percorso DI aggiornamento ANDU è...
9.4	9.14.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.4 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.4 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.4 → 9.5 - 9.5 → 9.6
	9.5	diretto

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il tuo percorso DI aggiornamento ANDU è...
9.3	9.14.1	multi-stage - 9,3 → 9,5 - 9,5 → 9,7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.3 → 9.5 - 9.5 → 9.6
	9.5	diretto
	9.4	non disponibile

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il tuo percorso DI aggiornamento ANDU è...
9.2	9.14.1	multi-stage - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.2 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.2 → 9.3 - 9.3 → 9.5
	9.4	non disponibile
	9.3	diretto

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il tuo percorso DI aggiornamento ANDU è...
9.1	9.14.1	multi-stage - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.1 → 9.3 - 9.3 → 9.5
	9.4	non disponibile
	9.3	diretto
	9.2	non disponibile

Se la versione corrente di ONTAP è...	E la tua release ONTAP di destinazione è...	Il tuo percorso DI aggiornamento ANDU è...
9.0	9.14.1	multi-stage - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.9.1
	9.8	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7 - 9.7 → 9.8
	9.7	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.7
	9.6	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5 - 9.5 → 9.6
	9.5	multi-stage - 9.0 → 9.1 - 9.1 → 9.3 - 9.3 → 9.5
	9.4	non disponibile
	9.3	multi-stage - 9.0 → 9.1 - 9.1 → 9.3
	9.2	non disponibile
	9.1	diretto

## Data ONTAP 8

Verificare che la piattaforma sia in grado di eseguire la release ONTAP di destinazione utilizzando ["NetApp Hardware Universe"](#).

**Nota:** la Guida all'aggiornamento di Data ONTAP 8.3 afferma erroneamente che in un cluster a quattro nodi, è necessario pianificare l'aggiornamento del nodo che contiene epsilon per ultimo. Questo non è più un requisito per gli aggiornamenti a partire da Data ONTAP 8.2.3. Per ulteriori informazioni, vedere ["ID bug online NetApp Bugs 805277"](#).

## Da Data ONTAP 8.3.x

Puoi eseguire l'aggiornamento direttamente a ONTAP 9.1, quindi eseguire l'aggiornamento alle versioni successive.

## Dalle release di Data ONTAP precedenti alla 8.3.x, inclusa la versione 8.2.x.

È necessario prima eseguire l'aggiornamento a Data ONTAP 8.3.x, quindi eseguire l'aggiornamento a ONTAP 9.1, quindi eseguire l'aggiornamento alle versioni successive.

## Verifica della configurazione di failover della LIF

Prima di aggiornare ONTAP, è necessario verificare che i criteri di failover del cluster e i gruppi di failover siano configurati correttamente.

Durante il processo di aggiornamento, i LIF vengono migrati in base al metodo di aggiornamento. A seconda del metodo di aggiornamento, il criterio di failover LIF potrebbe non essere utilizzato.

Se nel cluster sono presenti 8 o più nodi, l'aggiornamento automatico viene eseguito utilizzando il metodo batch. Il metodo di aggiornamento in batch prevede la suddivisione del cluster in batch di upgrade multipli, l'aggiornamento del set di nodi nel primo batch, l'aggiornamento dei partner ad alta disponibilità (ha) e la ripetizione del processo per i batch rimanenti. In ONTAP 9.7 e versioni precedenti, se viene utilizzato il metodo batch, i file LIF vengono migrati al partner ha del nodo da aggiornare. In ONTAP 9.8 e versioni successive, se viene utilizzato il metodo batch, i file LIF vengono migrati nell'altro gruppo batch.

Se nel cluster sono presenti meno di 8 nodi, l'aggiornamento automatico viene eseguito utilizzando il metodo a rotazione. Il metodo di Rolling upgrade implica l'avvio di un'operazione di failover su ciascun nodo di una coppia ha, l'aggiornamento del nodo da cui è stato eseguito il failover, l'avvio del giveback e la ripetizione del processo per ogni coppia ha del cluster. Se viene utilizzato il metodo rolling, i LIF vengono migrati nel nodo di destinazione del failover come definito dal criterio di failover LIF.

## Fasi

1. Visualizzare la policy di failover per ciascun LIF di dati:

Se la versione di ONTAP è...	Utilizzare questo comando
9.6 o versione successiva	<code>network interface show -service-policy *data* -failover</code>
9.5 o versioni precedenti	<code>network interface show -role data -failover</code>

Questo esempio mostra la configurazione di failover predefinita per un cluster a due nodi con due LIF di dati:

```
cluster1::> network interface show -role data -failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
vs0	lif0	node0:e0b	nextavail	system-
defined		Failover Targets: node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f, node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f		
vs1	lif1	node1:e0b	nextavail	system-
defined		Failover Targets: node1:e0b, node1:e0c, node1:e0d, node1:e0e, node1:e0f, node0:e0b, node0:e0c, node0:e0d, node0:e0e, node0:e0f		

Il campo **failover targets** (destinazioni di failover) mostra un elenco con priorità di destinazioni di failover per ciascun LIF. Ad esempio, se 'lif0' esegue il failover dalla porta principale (e0b su node0), tenta prima di eseguire il failover sulla porta e0c su node0. Se lif0 non riesce a eseguire il failover su e0c, tenta di eseguire il failover sulla porta e0d su node0 e così via.

2. Se il criterio di failover è impostato su **disabilitato** per qualsiasi LIF, diversa da quella SAN, utilizza `network interface modify` comando per abilitare il failover.
3. Per ogni LIF, verificare che il campo **failover targets** includa le porte dati di un nodo diverso che rimarranno in funzione durante l'aggiornamento del nodo principale LIF.

È possibile utilizzare `network interface failover-groups modify` comando per aggiungere una destinazione di failover al gruppo di failover.

### Esempio

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

### Informazioni correlate

["Gestione di rete e LIF"](#)

### Verificare la configurazione del routing SVM

Per evitare interruzioni, prima di aggiornare il software ONTAP, devi assicurarti che il

percorso SVM predefinito sia in grado di raggiungere qualsiasi indirizzo di rete non raggiungibile da un percorso più specifico. Si consiglia di configurare un percorso predefinito per una SVM. Per ulteriori informazioni, vedere ["SU134: L'accesso alla rete potrebbe essere interrotto da una configurazione di routing non corretta in ONTAP"](#).

La tabella di routing per una SVM determina il percorso di rete utilizzato dalla SVM per comunicare con una destinazione. È importante comprendere il funzionamento delle tabelle di routing in modo da prevenire i problemi di rete prima che si verifichino.

Le regole di routing sono le seguenti:

- ONTAP instrada il traffico sul percorso più specifico disponibile.
- ONTAP instrada il traffico su un percorso di gateway predefinito (con 0 bit di netmask) come ultima risorsa, quando non sono disponibili percorsi più specifici.

Nel caso di percorsi con la stessa destinazione, netmask e metrica, non vi è alcuna garanzia che il sistema utilizzi lo stesso percorso dopo un riavvio o un aggiornamento. Questo può essere un problema soprattutto se sono stati configurati più percorsi predefiniti.

## Considerazioni particolari

### Considerazioni speciali prima di un aggiornamento di ONTAP

Alcune configurazioni cluster richiedono azioni specifiche prima di iniziare un aggiornamento software ONTAP. Ad esempio, se si dispone di una configurazione SAN, verificare che ogni host sia configurato con il numero corretto di percorsi diretti e indiretti prima di iniziare l'aggiornamento.

Consultare la tabella seguente per determinare quali ulteriori passaggi è necessario eseguire.

Prima di aggiornare ONTAP, chiediti...	Se la risposta è sì, eseguire questa operazione...
Il mio cluster è attualmente in uno stato di versione mista?	<a href="#">Verificare i requisiti di versione mista</a>
Si dispone di una configurazione MetroCluster?	<a href="#">Verifica dei requisiti di aggiornamento specifici per le configurazioni MetroCluster</a>
Si dispone di una configurazione SAN?	<a href="#">Verificare la configurazione dell'host SAN</a>
Il mio cluster dispone di relazioni SnapMirror definite?	<a href="#">"Verifica la compatibilità delle versioni di ONTAP per le relazioni di SnapMirror"</a>
Ho definito relazioni di SnapMirror di tipo DP e sto eseguendo l'aggiornamento a ONTAP 9.12.1 o versione successiva?	<a href="#">"Converti le relazioni di tipo DP esistenti in XDP"</a>
Utilizzo NetApp Storage Encryption con server di gestione delle chiavi esterni?	<a href="#">Eliminare le connessioni esistenti al server di gestione delle chiavi</a>
I netgroup sono caricati nelle SVM?	<a href="#">Verificare che il file netgroup sia presente su ogni nodo</a>
I client LDAP utilizzano SSLv3?	<a href="#">Configurare i client LDAP per l'utilizzo di TLS</a>



Prima di aggiornare ONTAP, chiediti...	Se la risposta è sì, eseguire questa operazione...
Si utilizzano protocolli orientati alla sessione?	<a href="#">Esaminare le considerazioni relative ai protocolli orientati alla sessione</a>
La modalità SSL FIPS è abilitata su un cluster in cui gli account amministratore autenticano con una chiave pubblica SSH?	<a href="#">Verificare il supporto dell'algoritmo della chiave host SSH</a>

### Cluster ONTAP a versione mista

Un cluster ONTAP a versione mista è costituito da nodi che eseguono due diverse release principali di ONTAP per un periodo di tempo limitato. Ad esempio, se un cluster è attualmente costituito da nodi che eseguono ONTAP 9.8 e 9.12.1, il cluster è in versione mista. Analogamente, un cluster in cui i nodi eseguono ONTAP 9.9.1 e 9.13.1 sarebbe un cluster a versione mista. NetApp supporta cluster ONTAP a versione mista per periodi di tempo limitati e in scenari specifici.

Di seguito sono riportati gli scenari più comuni in cui un cluster ONTAP si trova in uno stato di versione mista:

- Aggiornamenti del software ONTAP in cluster di grandi dimensioni
- Gli aggiornamenti del software ONTAP sono necessari quando si prevede di aggiungere nuovi nodi a un cluster

Le informazioni si applicano alle versioni di ONTAP che supportano i sistemi con piattaforme NetApp, come AFF A-Series e C-Series, ASA, FAS e C-Series. Le informazioni non sono valide per le versioni cloud di ONTAP (9.x.0), ad esempio 9.12.0.

### Requisiti per i cluster ONTAP a versione mista

Se il cluster deve entrare in uno stato di versione ONTAP misto, è necessario essere a conoscenza di requisiti e restrizioni importanti.

- In un cluster non possono essere presenti più di due versioni principali di ONTAP diverse per volta. Ad esempio, ONTAP 9.9.1 e 9.13.1 sono supportati, ma ONTAP 9.9.1, 9.12.1 e 9.13.1 non lo sono. I cluster con nodi in esecuzione con diversi livelli di patch P o D della stessa release di ONTAP, come ONTAP 9.9.1P1 e 9.9.1P5, non sono considerati cluster ONTAP con versione mista.
- Mentre il cluster si trova in uno stato di versione mista, non inserire alcun comando che alteri l'operazione o la configurazione del cluster, ad eccezione di quelli richiesti per il processo di aggiornamento o di migrazione dei dati. Ad esempio, attività come la migrazione LIF (ma non solo), operazioni pianificate di failover dello storage o la creazione o l'eliminazione di oggetti su larga scala non devono essere eseguite fino al completamento dell'upgrade e della migrazione dei dati.
- Per un funzionamento ottimale del cluster, il tempo in cui il cluster si trova in uno stato di versione mista deve essere il più breve possibile. La durata massima di permanenza di un cluster in uno stato di versione mista dipende dalla versione ONTAP più bassa del cluster.

Se la versione più bassa di ONTAP in esecuzione nel cluster di versioni miste è:	Quindi, è possibile rimanere in uno stato di versione misto per un massimo di
ONTAP 9.8 o superiore	90 giorni
ONTAP 9.7 o versione precedente	7 giorni

- A partire da ONTAP 9,8, la differenza di versione tra i nodi originali e i nuovi nodi non può essere superiore a quattro. Ad esempio, un cluster ONTAP con versione mista potrebbe avere nodi che eseguono ONTAP 9.8 e 9.12.1 o nodi che eseguono ONTAP 9.9.1 e 9.13.1. Tuttavia, un cluster ONTAP con versione mista con nodi che eseguono ONTAP 9,8 e 9.13.1 non sarebbe supportato.

Per un elenco completo dei cluster di versioni miste supportati, vedere ["percorsi di aggiornamento supportati"](#). Tutti i percorsi di aggiornamento *diretto* sono supportati per i cluster di versioni miste.

## Aggiornamento della versione ONTAP di un cluster di grandi dimensioni

Uno scenario per l'accesso a uno stato di cluster con versione mista prevede l'aggiornamento della versione ONTAP di un cluster con più nodi per sfruttare le funzionalità disponibili nelle versioni successive di ONTAP 9. Quando è necessario aggiornare la versione ONTAP di un cluster più grande, si inserisce uno stato del cluster a versione mista per un periodo di tempo durante l'aggiornamento di ciascun nodo del cluster.

## Aggiunta di nuovi nodi a un cluster ONTAP

Un altro scenario per l'inserimento di uno stato di cluster con versione mista prevede l'aggiunta di nuovi nodi al cluster. È possibile aggiungere nuovi nodi al cluster per espanderne la capacità oppure aggiungere nuovi nodi durante il processo di sostituzione completa dei controller. In entrambi i casi, è necessario abilitare la migrazione dei dati dai controller esistenti ai nuovi nodi nel nuovo sistema.

Se si prevede di aggiungere nuovi nodi al cluster e tali nodi richiedono una versione minima di ONTAP successiva alla versione attualmente in esecuzione nel cluster, è necessario eseguire eventuali aggiornamenti software supportati sui nodi esistenti nel cluster prima di aggiungere i nuovi nodi.

Idealmente, si dovrebbe aggiornare tutti i nodi esistenti alla versione minima di ONTAP richiesta dai nodi che si intende aggiungere al cluster. Tuttavia, se questo non è possibile perché alcuni dei nodi esistenti non supportano la versione successiva di ONTAP, sarà necessario immettere uno stato di versione mista per un periodo di tempo limitato come parte del processo di aggiornamento. Se si dispone di nodi che non supportano la versione minima di ONTAP richiesta dai nuovi controller, attenersi alla seguente procedura:

1. ["Eseguire l'upgrade"](#) I nodi che non supportano la versione minima di ONTAP richiesta dai nuovi controller fino alla versione massima di ONTAP supportata.

Ad esempio, se si dispone di un sistema FAS8080 con ONTAP 9,5 e si sta aggiungendo una nuova piattaforma C-Series con ONTAP 9.12.1, è necessario aggiornare il sistema FAS8080 a ONTAP 9,8 (ovvero la versione ONTAP massima supportata).

2. ["Aggiungere i nuovi nodi al cluster"](#).
3. ["Migrare i dati"](#) dai nodi rimossi dal cluster ai nuovi nodi aggiunti.
4. ["Rimuovere i nodi non supportati dal cluster"](#).
5. ["Eseguire l'upgrade"](#) gli altri nodi del cluster, con la stessa versione dei nuovi nodi.

In alternativa, è possibile eseguire l'upgrade dell'intero cluster (compresi i nuovi nodi) al ["ultima versione di patch consigliata"](#) Della versione di ONTAP in esecuzione sui nuovi nodi.

Per ulteriori informazioni sulla migrazione dei dati, consulta:

- ["Creare un aggregato e spostare i volumi nei nuovi nodi"](#)
- ["Impostazione di nuove connessioni iSCSI per gli spostamenti dei volumi SAN"](#)

- "Spostamento di volumi con crittografia"

## Requisiti di aggiornamento di ONTAP per le configurazioni MetroCluster

Prima di aggiornare il software ONTAP su una configurazione MetroCluster, i cluster devono soddisfare determinati requisiti.

- Entrambi i cluster devono eseguire la stessa versione di ONTAP.

È possibile verificare la versione di ONTAP utilizzando il comando `version`.

- Se si sta eseguendo un aggiornamento ONTAP importante, la configurazione MetroCluster deve essere in modalità normale.
- Se si sta eseguendo un aggiornamento di patch ONTAP, la configurazione MetroCluster può essere in modalità normale o di switchover.
- Per tutte le configurazioni, ad eccezione dei cluster a due nodi, è possibile aggiornare entrambi i cluster senza interruzioni allo stesso tempo.

Per un upgrade senza interruzioni in cluster a due nodi, i cluster devono essere aggiornati un nodo alla volta.

- Gli aggregati in entrambi i cluster non devono trovarsi nello stato RAID di resyncing.

Durante la riparazione MetroCluster, gli aggregati mirrorati vengono risincronizzati. È possibile verificare se la configurazione MetroCluster si trova in questo stato utilizzando `storage aggregate plex show -in-progress true` comando. Se vengono sincronizzati degli aggregati, non eseguire un aggiornamento fino al completamento della risincronizzazione.

- Le operazioni di switchover negoziate non avranno esito positivo durante l'aggiornamento.

Per evitare problemi con le operazioni di upgrade o revert, non tentare uno switchover non pianificato durante un'operazione di upgrade o revert, a meno che tutti i nodi su entrambi i cluster non eseguano la stessa versione di ONTAP.

## Requisiti di configurazione per il normale funzionamento dell'MetroCluster

- I LIF SVM di origine devono essere attivi e posizionati sui nodi domestici.

Non è necessario che le LIF dei dati per le SVM di destinazione siano attive o che si trovino sui propri nodi domestici.

- Tutti gli aggregati del sito locale devono essere online.
- Tutti i volumi root e di dati di proprietà delle SVM del cluster locale devono essere online.

## Requisiti di configurazione per lo switchover di MetroCluster

- Tutti i LIF devono essere attivi e posizionati sui propri nodi domestici.
- Tutti gli aggregati devono essere online, ad eccezione degli aggregati root del sito DR.

Gli aggregati root del sito DR sono offline durante alcune fasi di switchover.

- Tutti i volumi devono essere online.

**Informazioni correlate**

["Verifica dello stato di rete e storage per le configurazioni MetroCluster"](#)

**Verificare la configurazione dell’host SAN prima di un aggiornamento ONTAP**

L’aggiornamento di ONTAP in un ambiente SAN modifica i percorsi diretti. Prima di eseguire l’upgrade di un cluster SAN, occorre verificare che ogni host sia configurato con il numero corretto di percorsi diretti e indiretti e che ogni host sia connesso alle LIF corrette.

**Fasi**

- 1. Su ciascun host, verificare che sia configurato un numero sufficiente di percorsi diretti e indiretti e che ciascun percorso sia attivo.

Ciascun host deve disporre di un percorso per ciascun nodo del cluster.

- 2. Verificare che ciascun host sia connesso a una LIF su ciascun nodo.

È necessario registrare l'elenco degli iniziatori per il confronto dopo l'aggiornamento.

Per...	Inserisci...
ISCSI	<pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre>
FC	<pre>fcp initiator show -fields igroup,wwpn,lif</pre>

**SnapMirror**

**Versioni ONTAP compatibili per le relazioni SnapMirror**

Prima di creare una relazione di data Protection SnapMirror, i volumi di origine e destinazione devono eseguire versioni di ONTAP compatibili. Prima di eseguire l’aggiornamento di ONTAP, devi verificare che la tua versione attuale di ONTAP sia compatibile con la tua versione di ONTAP di destinazione per le relazioni SnapMirror.

**Relazioni di replica unificate**

Per le relazioni SnapMirror di tipo “XDP”, utilizzando release on-premise o Cloud Volumes ONTAP:

A partire da ONTAP 9.9.0:



- Le release ONTAP 9.x,0 sono release solo per cloud e supportano i sistemi Cloud Volumes ONTAP. L'asterisco (\*) dopo la versione della release indica una release solo cloud.
- Le release ONTAP 9.x,1 sono release generali e supportano sistemi Cloud Volumes ONTAP e on-premise.



L'interoperabilità è bidirezionale.

### Interoperabilità per ONTAP versione 9.3 e successive

Versione di ONTAP ...	Interagisce con queste versioni precedenti di ONTAP...																	
	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9.8	9.7	9.6	9.5	9.4	9.3
9.14.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No	No
9.14.0*	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì	No	Sì	No	Sì	No	No	No	No	No
9.13.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No	No
9.13.0*	Sì	No	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì	No	Sì	No	No	No	No	No
9.12.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No
9.12.0*	Sì	No	Sì	No	Sì	Sì	Sì	No	Sì	No	Sì	No	Sì	Sì	No	No	No	No
9.11.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No
9.11.0*	Sì	No	Sì	No	Sì	No	Sì	Sì	Sì	No	Sì	No	Sì	Sì	Sì	No	No	No
9.10.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No
9.10.0*	Sì	No	Sì	No	Sì	No	Sì	No	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	No	No
9.9.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No
9.9.0*	Sì	No	Sì	No	Sì	No	Sì	No	Sì	No	Sì	Sì	Sì	Sì	Sì	Sì	No	No
9.8	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì

9.7	No	No	No	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì
9.6	No	No	No	No	No	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	Sì
9.5	No	No	No	No	No	No	No	No	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì
9.4	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	Sì	Sì	Sì
9.3	No	No	No	No	No	No	No	No	No	No	No	No	Sì	Sì	Sì	Sì	Sì	Sì

## Relazioni sincroni di SnapMirror



SnapMirror Synchronous non è supportato per le istanze cloud di ONTAP.

Versione di ONTAP ...	Interagisce con queste versioni precedenti di ONTAP...									
	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5
9.14.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No
9.13.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No
9.12.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No
9.11.1	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No	No
9.10.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No	No
9.9.1	Sì	Sì	Sì	Sì	Sì	Sì	Sì	Sì	No	No
9.8	Sì	Sì	Sì	No	Sì	Sì	Sì	Sì	Sì	No
9.7	No	Sì	Sì	No	No	Sì	Sì	Sì	Sì	Sì
9.6	No	No	No	No	No	No	Sì	Sì	Sì	Sì
9.5	No	No	No	No	No	No	No	Sì	Sì	Sì

## Relazioni di disaster recovery di SnapMirror SVM

- Per i dati di disaster recovery SVM e la protezione SVM:

Il disaster recovery delle SVM è supportato solo tra cluster che eseguono la stessa versione di ONTAP.

**L'indipendenza dalla versione non è supportata per la replica SVM.**

- Per il disaster recovery SVM per la migrazione SVM:
  - La replica è supportata in una singola direzione da una versione precedente di ONTAP sull'origine alla stessa o versione successiva di ONTAP sulla destinazione.
- La versione di ONTAP nel cluster di destinazione non deve essere più recente di due versioni principali on-premise o due versioni principali di cloud più recenti, come mostrato nella tabella seguente.
  - La replica non è supportata per i casi di utilizzo a lungo termine della protezione dei dati.

L'asterisco (\*) dopo la versione della release indica una release solo cloud.

Per determinare il supporto, individuare la versione di origine nella colonna della tabella a sinistra, quindi

individuare la versione di destinazione nella riga superiore (DR/migrazione per le versioni simili e migrazione solo per le versioni più recenti).

Origine	Destinazione																	
	9.3	9.4	9.5	9.6	9.7	9.8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1
9.3	Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione													
9.4		Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione												
9.5			Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione											
9.6				Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione										
9.7					Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione									
9.8						Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione								
9.9.0*							Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione							
9.9.1								Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione						
9.10.0*									Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione					
9.10.1										Dr/migrazione	Migrazione	Migrazione	Migrazione	Migrazione				

9.11 .0*										Dr/ migr azio ne	Migr azio ne	Migr azio ne	Migr azio ne	Migr azio ne			
9.11 .1										Dr/ migr azio ne	Migr azio ne	Migr azio ne	Migr azio ne	Migr azio ne			
9.12 .0*											Dr/ migr azio ne	Migr azio ne	Migr azio ne	Migr azio ne	Migr azio ne		
9.12 .1												Dr/ migr azio ne	Migr azio ne	Migr azio ne	Migr azio ne	Migr azio ne	
9.13 .0*													Dr/ migr azio ne	Migr azio ne	Migr azio ne	Migr azio ne	
9.13 .1														Dr/ migr azio ne	Migr azio ne	Migr azio ne	
9.14 .0*															Dr/ migr azio ne	Migr azio ne	
9.14 .1																Dr/ migr azio ne	

## Relazioni di disaster recovery di SnapMirror

Per le relazioni SnapMirror di tipo “DP” e di tipo di policy “async-mirror”:



I mirror di tipo DP non possono essere inizializzati a partire da ONTAP 9.11.1 e sono completamente deprecati in ONTAP 9.12.1. Per ulteriori informazioni, vedere ["Deprecazione delle relazioni SnapMirror per la protezione dei dati"](#).



Nella tabella seguente, la colonna a sinistra indica la versione di ONTAP sul volume di origine, mentre la riga superiore indica le versioni di ONTAP disponibili sul volume di destinazione.

Origine	Destinazione											
	9.11.1	9.10.1	9.9.1	9.8	9.7	9.6	9.5	9.4	9.3	9.2	9.1	9
9.11.1	Sì	No	No	No	No	No	No	No	No	No	No	No



9.10.1	Sì	Sì	No	No	No	No	No	No	No	No	No	No
9.9.1	Sì	Sì	Sì	No	No	No	No	No	No	No	No	No
9.8	No	Sì	Sì	Sì	No	No	No	No	No	No	No	No
9.7	No	No	Sì	Sì	Sì	No	No	No	No	No	No	No
9.6	No	No	No	Sì	Sì	Sì	No	No	No	No	No	No
9.5	No	No	No	No	Sì	Sì	Sì	No	No	No	No	No
9.4	No	No	No	No	No	Sì	Sì	Sì	No	No	No	No
9.3	No	No	No	No	No	No	Sì	Sì	Sì	No	No	No
9.2	No	No	No	No	No	No	No	Sì	Sì	Sì	No	No
9.1	No	No	No	No	No	No	No	No	Sì	Sì	Sì	No
9	No	No	No	No	No	No	No	No	No	Sì	Sì	Sì



L'interoperabilità non è bidirezionale.

### Convertire una relazione di tipo DP esistente in XDP

Se si esegue l'aggiornamento a ONTAP 9.12.1 o versioni successive, è necessario convertire le relazioni di tipo DP in XDP prima di eseguire l'aggiornamento. ONTAP 9.12.1 e versioni successive non supportano le relazioni di tipo DP. È possibile convertire facilmente una relazione di tipo DP esistente in XDP per sfruttare SnapMirror flessibile in versione.

#### A proposito di questa attività

- SnapMirror non converte automaticamente le relazioni di tipo DP esistenti in XDP. Per convertire la relazione, è necessario interrompere ed eliminare la relazione esistente, creare una nuova relazione XDP e risincronizzare la relazione. Per informazioni generali, vedere ["XDP sostituisce DP come impostazione predefinita di SnapMirror"](#).
- Durante la pianificazione della conversione, è necessario tenere presente che la preparazione in background e la fase di data warehousing di una relazione SnapMirror XDP possono richiedere molto tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.



Dopo aver convertito un tipo di relazione SnapMirror da DP a XDP, le impostazioni relative allo spazio, come la dimensione automatica e la garanzia dello spazio, non vengono più replicate nella destinazione.

#### Fasi

1. Dal cluster di destinazione, assicurarsi che la relazione SnapMirror sia di tipo DP, che lo stato del mirror sia SnapMirrored, che lo stato della relazione sia inattivo e che la relazione sia integra:

```
snapmirror show -destination-path <SVM:volume>
```

L'esempio seguente mostra l'output di `snapmirror show` comando:

```
cluster_dst:>snapmirror show -destination-path svm_backup:volA_dst
```

```
Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```



Potrebbe essere utile conservare una copia di `snapmirror show` output dei comandi per tenere traccia delle impostazioni delle relazioni esistenti.

2. Dai volumi di origine e di destinazione, assicurarsi che entrambi i volumi dispongano di una copia Snapshot comune:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Nell'esempio riportato di seguito viene illustrato il `volume snapshot show` output per i volumi di origine e di destinazione:

```
cluster_src:> volume snapshot show -vserver svml -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svml volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.
```

```
cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
-----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Per garantire che gli aggiornamenti pianificati non vengano eseguiti durante la conversione, interrompere la relazione DP-type esistente:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path  
<SVM:volume>
```

Per la sintassi completa dei comandi, vedere ["pagina man"](#).



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio seguente viene meno la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

#### 4. Interrompere la relazione di tipo DP esistente:

```
snapmirror break -destination-path <SVM:volume>
```

Per la sintassi completa dei comandi, vedere ["pagina man"](#).



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio seguente viene spezzata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

#### 5. Se l'eliminazione automatica delle copie Snapshot è attivata sul volume di destinazione, disattivarla:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_  
-enabled false
```

Nell'esempio seguente viene disattivata l'eliminazione automatica della copia Snapshot sul volume di destinazione `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup  
-volume volA_dst -enabled false
```

#### 6. Eliminare la relazione DP-type esistente:

```
snapmirror delete -destination-path <SVM:volume>
```

Per la sintassi completa dei comandi, vedere ["pagina man"](#).



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio riportato di seguito viene eliminata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

#### 7. Rilasciare la relazione di disaster recovery della SVM di origine sull'origine:

```
snapmirror release -destination-path <SVM:volume> -relationship-info  
-only true
```

L'esempio seguente rilascia la relazione di disaster recovery della SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst  
-relationship-info-only true
```

#### 8. È possibile utilizzare l'output conservato da `snapmirror show` Comando per creare la nuova relazione XDP-type:

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type XDP -schedule <schedule> -policy <policy>
```

La nuova relazione deve utilizzare lo stesso volume di origine e di destinazione. Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

L'esempio seguente crea una relazione di disaster recovery SnapMirror tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup` utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst  
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

## 9. Risincronizzare i volumi di origine e di destinazione:

```
snapmirror resync -source-path <SVM:volume> -destination-path  
<SVM:volume>
```

Per migliorare il tempo di risincronizzazione, è possibile utilizzare `-quick-resync` tuttavia, è importante tenere presente che i risparmi in termini di efficienza dello storage possono andare persi. Per la sintassi completa dei comandi, vedere la pagina man: "[Comando di risync di SnapMirror](#)".



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

## 10. Se l'eliminazione automatica delle copie Snapshot è stata disattivata, riattivarla:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>  
-enabled true
```

### Al termine

1. Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror.
2. Quando il volume di destinazione SnapMirror XDP inizia ad aggiornare le copie Snapshot come definito dalla policy SnapMirror, utilizzare l'output di `snapmirror list-destinations` Dal cluster di origine per visualizzare la nuova relazione SnapMirror XDP.

### Eliminare le connessioni al server di gestione chiavi esterno esistenti prima di aggiornare ONTAP

Prima di eseguire l'upgrade di ONTAP, se si esegue ONTAP 9,2 o versione precedente con crittografia dello storage NetApp (NSE) ed eseguire l'aggiornamento a ONTAP 9,3 o versione successiva, è necessario utilizzare l'interfaccia a riga di comando (CLI) per eliminare qualsiasi connessione server di gestione delle chiavi esterna (KMIP) esistente.

### Fasi

1. Verificare che le unità NSE siano sbloccate, aperte e impostate sull'ID protetto predefinito 0x0:

```
storage encryption disk show -disk *
```

2. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

3. Utilizzare l'ID protetto predefinito 0x0 per assegnare la chiave FIPS ai dischi con crittografia automatica (SED):

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

4. Verificare che l'assegnazione della chiave FIPS a tutti i dischi sia completata:

```
storage encryption disk show-status
```

5. Verificare che la **modalità** per tutti i dischi sia impostata su dati

```
storage encryption disk show
```

6. Visualizzare i server KMIP configurati:

```
security key-manager show
```

7. Eliminare i server KMIP configurati:

```
security key-manager delete -address kmip_ip_address
```

8. Eliminare la configurazione del gestore delle chiavi esterno:

```
security key-manager delete-kmip-config
```



Questa fase non rimuove i certificati NSE.

### Cosa succederà

Una volta completato l'aggiornamento, è necessario [Riconfigurare le connessioni del server KMIP](#).

**Verificare che il file netgroup sia presente su tutti i nodi prima di un aggiornamento di ONTAP**

Prima di eseguire l'upgrade di ONTAP, se sono stati caricati netgroup nelle Storage Virtual Machine (SVM), è necessario verificare la presenza del file netgroup in ciascun nodo. Un file netgroup mancante su un nodo può causare un errore di aggiornamento.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Visualizzare lo stato del netgroup per ogni SVM:

```
vserver services netgroup status
```

3. Verificare che per ogni SVM, ciascun nodo mostri lo stesso valore hash del file netgroup:

```
vserver services name-service netgroup status
```

In questo caso, è possibile saltare il passaggio successivo e procedere con l'aggiornamento o il ripristino. In caso contrario, passare alla fase successiva.

4. Su un nodo qualsiasi del cluster, caricare manualmente il file netgroup:

```
vserver services netgroup load -vserver vserver_name -source uri
```

Questo comando scarica il file netgroup su tutti i nodi. Se un file netgroup esiste già su un nodo, viene sovrascritto.

## Informazioni correlate

["Lavorare con i netgroup"](#)

### Configurare i client LDAP in modo che utilizzino TLS per la massima sicurezza

Prima di aggiornare ONTAP, è necessario configurare i client LDAP utilizzando SSLv3 per comunicazioni protette con i server LDAP per utilizzare TLS. SSL non sarà disponibile dopo l'aggiornamento.

Per impostazione predefinita, le comunicazioni LDAP tra applicazioni client e server non sono crittografate. È necessario non consentire l'utilizzo di SSL e imporre l'utilizzo di TLS.

## Fasi

1. Verificare che i server LDAP nel proprio ambiente supportino TLS.

In caso contrario, non procedere. È necessario aggiornare i server LDAP a una versione che supporti TLS.

2. Controllare quali configurazioni del client LDAP ONTAP hanno abilitato LDAP su SSL/TLS:

```
vserver services name-service ldap client show
```

In caso contrario, è possibile saltare i passaggi rimanenti. Tuttavia, è consigliabile utilizzare LDAP su TLS per una maggiore sicurezza.



3. Per ogni configurazione del client LDAP, non consentire a SSL di imporre l'utilizzo di TLS:

```
vserver services name-service ldap client modify -vserver vserver_name  
-client-config ldap_client_config_name -allow-ssl false
```

4. Verificare che l'utilizzo di SSL non sia più consentito per i client LDAP:

```
vserver services name-service ldap client show
```

## Informazioni correlate

["Gestione NFS"](#)

### Considerazioni per i protocolli orientati alla sessione

I cluster e i protocolli orientati alle sessioni possono causare effetti negativi su client e applicazioni in determinate aree, come il servizio i/o durante gli aggiornamenti.

Se si utilizzano protocolli orientati alla sessione, considerare quanto segue:

- PMI

Se si utilizzano condivisioni CA (Continuously Available) con SMBv3, è possibile utilizzare il metodo di aggiornamento automatico senza interruzioni (con System Manager o CLI) e il client non subiva alcuna interruzione.

Se si forniscono condivisioni con SMBv1 o SMBv2 o condivisioni non CA con SMBv3, le sessioni client vengono interrotte durante le operazioni di takeover e reboot dell'upgrade. Gli utenti devono terminare le sessioni prima di eseguire l'aggiornamento.

Hyper-V e SQL Server su SMB supportano operazioni senza interruzioni (NDOS). Se è stata configurata una soluzione Hyper-V o SQL Server su SMB, i server delle applicazioni e le macchine virtuali o i database contenuti rimangono online e garantiscono una disponibilità continua durante l'aggiornamento di ONTAP.

- NFSv4.x

I client NFSv4.x ripristineranno automaticamente le perdite di connessione riscontrate durante l'aggiornamento utilizzando le normali procedure di ripristino NFSv4.x. Durante questo processo, le applicazioni potrebbero riscontrare un ritardo i/O.

- NDMP

Lo stato viene perso e l'utente client deve riprovare l'operazione.

- Backup e ripristini

Lo stato viene perso e l'utente client deve riprovare l'operazione.



Non avviare un backup o un ripristino durante o immediatamente prima di un aggiornamento. Ciò potrebbe causare la perdita di dati.

- Applicazioni (ad esempio, Oracle o Exchange)

Gli effetti dipendono dalle applicazioni. Per le applicazioni basate sul timeout, potrebbe essere possibile modificare l'impostazione del timeout su un tempo superiore al tempo di riavvio di ONTAP per ridurre al minimo gli effetti negativi.

#### Verificare il supporto dell'algoritmo della chiave host SSH prima dell'aggiornamento di ONTAP

Prima di aggiornare ONTAP, se la modalità SSL FIPS è attivata su un cluster in cui gli account amministratore si autenticano con una chiave pubblica SSH, è necessario assicurarsi che l'algoritmo della chiave host sia supportato nella versione ONTAP di destinazione.

La seguente tabella indica gli algoritmi del tipo di chiave host supportati per le connessioni SSH ONTAP. Questi tipi di chiave non si applicano alla configurazione dell'autenticazione pubblica SSH.

Release di ONTAP	Tipi di chiave supportati in modalità FIPS	Tipi di chiave supportati in modalità non FIPS
9.11.1 e versioni successive	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 e versioni precedenti	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa



Il supporto per l'algoritmo della chiave host ssh-ed25519 viene rimosso a partire da ONTAP 9.11.1.

Per ulteriori informazioni, vedere ["Configurare la sicurezza di rete utilizzando FIPS"](#).

Gli account a chiave pubblica SSH esistenti senza gli algoritmi a chiave supportati devono essere riconfigurati con un tipo di chiave supportato prima di eseguire l'aggiornamento, altrimenti l'autenticazione dell'amministratore avrà esito negativo.

["Scopri di più sull'abilitazione degli account a chiave pubblica SSH."](#)

#### Riavviare SP o BMC per preparare l'aggiornamento del firmware durante un aggiornamento ONTAP

Non è necessario aggiornare manualmente il firmware prima di un aggiornamento ONTAP. Il firmware del cluster viene incluso nel pacchetto di aggiornamento ONTAP e viene copiato nel dispositivo di boot di ciascun nodo. Il nuovo firmware viene quindi installato come parte del processo di aggiornamento.

Il firmware per i seguenti componenti viene aggiornato automaticamente se la versione del cluster è precedente a quella del firmware fornito con il pacchetto di aggiornamento ONTAP:

- BIOS/CARICATORE
- Service Processor (SP) o Baseboard Management Controller (BMC)
- Shelf di storage

- Disco
- Flash cache

Per prepararsi a un aggiornamento senza problemi, è necessario riavviare il SP o il BMC prima dell'inizio dell'aggiornamento.

## Fase

1. Riavviare il SP o BMC prima dell'aggiornamento:

```
system service-processor reboot-sp -node node_name
```

Riavviare un solo SP o BMC alla volta. Prima di riavviare il successivo, attendere che il SP o il BMC siano completamente riciclati.

Puoi anche farlo ["aggiornare il firmware manualmente"](#) Tra un aggiornamento e l'altro di ONTAP. Se si dispone di Active IQ, è possibile ["Consente di visualizzare l'elenco delle versioni firmware attualmente incluse nell'immagine ONTAP"](#).

Le versioni aggiornate del firmware sono disponibili come segue:

- ["Firmware di sistema \(BIOS, BMC, SP\)"](#)
- ["Firmware dello shelf"](#)
- ["Disco e firmware Flash cache"](#)

## Scaricare l'immagine del software ONTAP

Prima di aggiornare ONTAP, è necessario scaricare l'immagine del software ONTAP di destinazione dal sito di supporto NetApp. A seconda della versione di ONTAP, è possibile scaricare il software ONTAP su un server HTTPS, HTTP o FTP sulla rete o in una cartella locale.

Se si esegue...	È possibile scaricare l'immagine in questa posizione...
ONTAP 9.6 e versioni successive	<ul style="list-style-type: none"> <li>• Sul sistema locale deve essere installato un server HTTPS e il certificato CA del server.</li> <li>• Una cartella locale</li> <li>• Un server HTTP o FTP</li> </ul>
ONTAP 9.4 e versioni successive	<ul style="list-style-type: none"> <li>• Una cartella locale</li> <li>• Un server HTTP o FTP</li> </ul>
ONTAP 9.0 e versioni successive	Un server HTTP o FTP

### A proposito di questa attività

- Se stai eseguendo un upgrade automatizzato e non disgregativo (ANDU) utilizzando un ["percorso di upgrade diretto multi-hop"](#), è necessario ["scarica"](#) Il pacchetto software sia per la versione ONTAP

intermedia che per la versione ONTAP di destinazione necessari per l'aggiornamento. Ad esempio, se si esegue l'aggiornamento da ONTAP 9,8 a ONTAP 9.13.1, è necessario scaricare i pacchetti software sia per ONTAP 9.12.1 che per ONTAP 9.13.1. Vedere ["percorsi di aggiornamento supportati"](#) per determinare se il percorso di aggiornamento richiede il download di un pacchetto software intermedio.

- Se si esegue l'aggiornamento di un sistema con crittografia dei volumi NetApp a ONTAP 9.5 o versione successiva, è necessario scaricare l'immagine del software ONTAP per i paesi senza restrizioni, che include crittografia dei volumi NetApp.

Se si utilizza l'immagine del software ONTAP per i paesi con restrizioni per aggiornare un sistema con crittografia dei volumi NetApp, il sistema esegue una panoramica e si perde l'accesso ai volumi.

- Non è necessario scaricare un pacchetto software separato per il firmware. L'aggiornamento del firmware per il cluster è incluso nel pacchetto di aggiornamento software ONTAP e viene copiato nel dispositivo di boot di ogni nodo. Il nuovo firmware viene quindi installato come parte del processo di aggiornamento.

## Fasi

1. Individuare il software ONTAP di destinazione in ["Download di software"](#) Area del NetApp Support Site.

Per un aggiornamento ONTAP Select, selezionare **aggiornamento nodo ONTAP Select**.

2. Copiare l'immagine software (ad esempio, 97\_q\_image.tgz) nella posizione appropriata.

A seconda della versione di ONTAP, la posizione sarà una directory di un server HTTP, HTTPS o FTP da cui l'immagine verrà servita al sistema locale o a una cartella locale del sistema di storage.

## Metodi di aggiornamento di ONTAP

### Metodi di aggiornamento del software ONTAP

Puoi eseguire un aggiornamento automatico del software ONTAP utilizzando Gestione sistema. In alternativa, è possibile eseguire un aggiornamento automatico o manuale utilizzando l'interfaccia a riga di comando (CLI) di ONTAP. Il metodo utilizzato per aggiornare ONTAP dipende dalla configurazione, dalla versione corrente di ONTAP e dal numero di nodi nel cluster. NetApp consiglia di utilizzare System Manager per eseguire aggiornamenti automatici, a meno che la configurazione non richieda un approccio diverso. Ad esempio, se disponi di una configurazione MetroCluster con 4 nodi in cui è in esecuzione ONTAP 9,3 o versione successiva, dovresti utilizzare System Manager per eseguire un upgrade automatico (talvolta indicato come upgrade automatico senza interruzioni o ANDU). Se disponi di una configurazione MetroCluster con 8 nodi in esecuzione su ONTAP 9,2 o versione precedente, devi utilizzare la CLI per eseguire un aggiornamento manuale.

È possibile eseguire un aggiornamento utilizzando il processo di aggiornamento in sequenza o il processo di aggiornamento in batch. Entrambi sono senza interruzioni.

Per gli upgrade automatici, ONTAP installa automaticamente l'immagine ONTAP di destinazione su ciascun nodo, convalida i componenti del cluster per garantire l'upgrade senza interruzioni del cluster, quindi esegue un batch o un Rolling upgrade in background in base al numero di nodi. Per gli aggiornamenti manuali, l'amministratore conferma manualmente che ogni nodo del cluster è pronto per l'aggiornamento, quindi esegue i passaggi necessari per eseguire un Rolling upgrade.

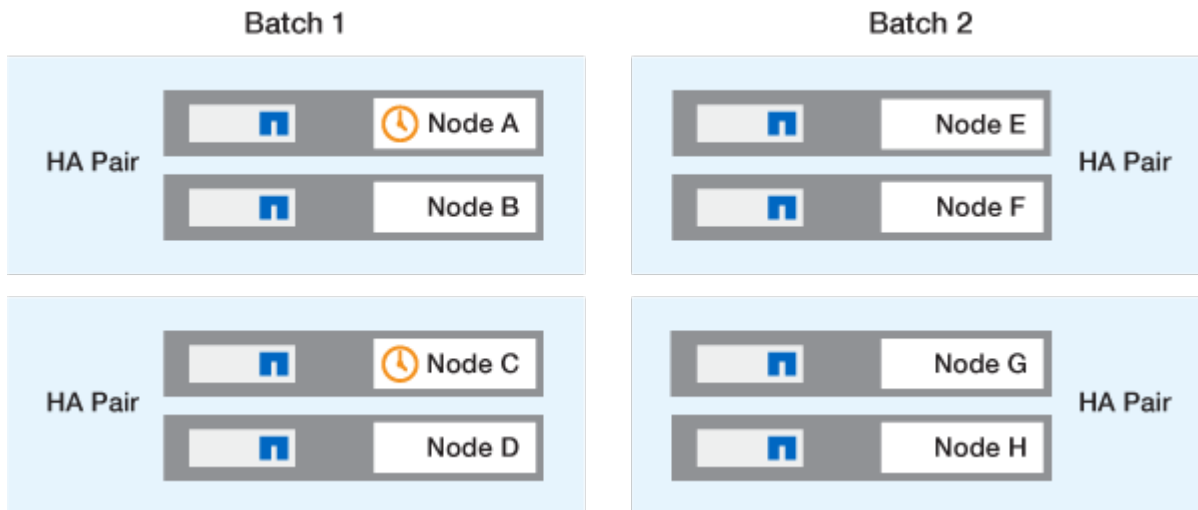
## Rolling upgrade di ONTAP

L'Rolling upgrade è l'impostazione predefinita per i cluster con meno di 8 nodi. Durante il processo di aggiornamento continuo, un nodo viene portato offline e aggiornato mentre il partner assume il controllo dello storage. Quando l'aggiornamento del nodo è completo, il nodo partner restituisce il controllo al nodo proprietario originale e il processo viene ripetuto sul nodo partner. Ogni coppia ha aggiuntiva viene aggiornata in sequenza fino a quando tutte le coppie ha non eseguono la release di destinazione.

### Aggiornamenti batch ONTAP

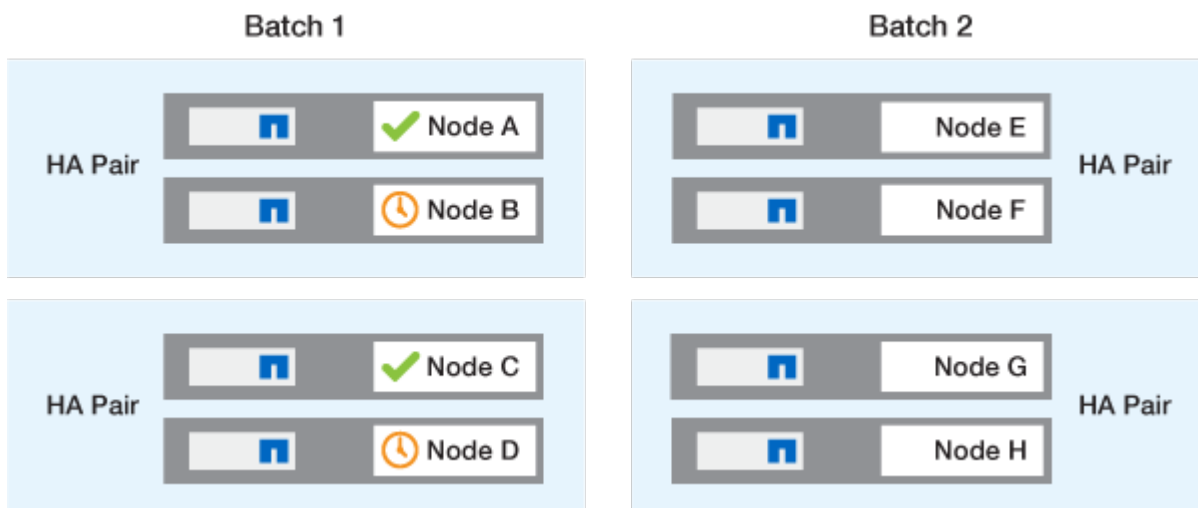
Il processo di aggiornamento in batch è l'impostazione predefinita per i cluster di 8 o più nodi. Nel processo di aggiornamento batch, il cluster è diviso in due batch. Ogni batch contiene più coppie ha. Nel primo batch, il primo nodo di ciascuna coppia ha viene aggiornato simultaneamente al primo nodo di tutte le altre coppie ha del batch.

Nel seguente esempio, esistono due coppie ha in ogni batch. Quando inizia l'aggiornamento batch, il nodo A e il nodo C vengono aggiornati contemporaneamente.



Al termine dell'upgrade dei primi nodi di ciascuna coppia ha, vengono aggiornati contemporaneamente i nodi partner del batch 1.

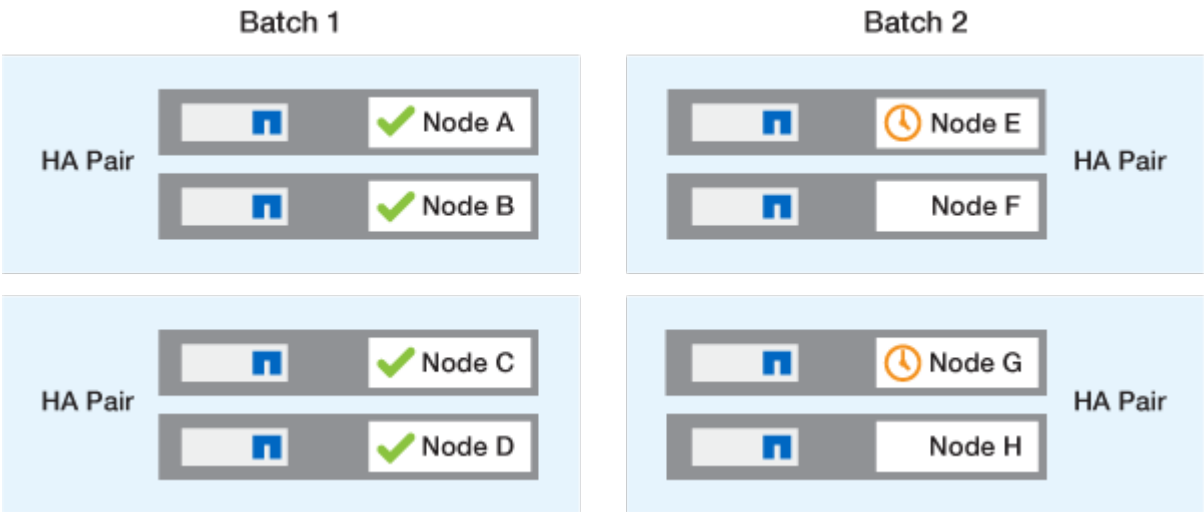
Nell'esempio seguente, dopo l'aggiornamento del nodo A e del nodo C, il nodo B e il nodo D vengono aggiornati contemporaneamente.



Il processo viene quindi ripetuto per i nodi nel batch 2; il primo nodo di ogni coppia ha viene aggiornato

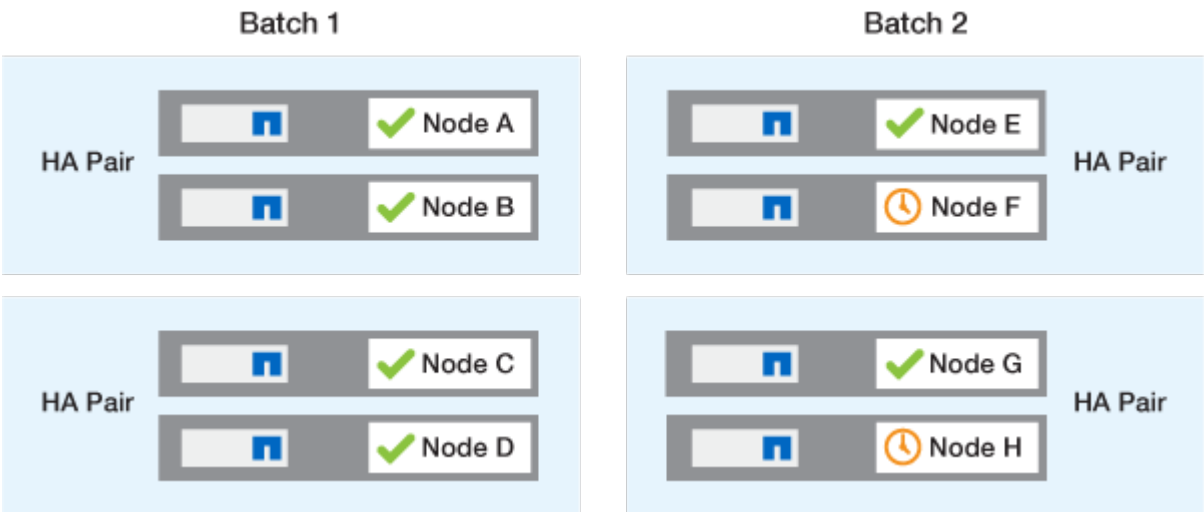
simultaneamente al primo nodo di tutte le altre coppie ha nel batch.

Nell'esempio seguente, il nodo e e il nodo G vengono aggiornati simultaneamente.



Al termine dell'upgrade dei primi nodi di ciascuna coppia ha, vengono aggiornati contemporaneamente i nodi partner del batch 2.

Nell'esempio seguente, il nodo F e il nodo H vengono aggiornati simultaneamente per completare il processo di aggiornamento in batch.



**Metodi di aggiornamento ONTAP consigliati in base alla configurazione**

I metodi di aggiornamento supportati dalla configurazione in uso sono elencati in ordine di utilizzo consigliato.

Configurazione	Versione di ONTAP	Numero di nodi	Metodo di aggiornamento consigliato
Standard	9.0 o versione successiva	2 o più	<ul style="list-style-type: none"> <li>• Automazione senza interruzioni con System Manager</li> <li>• Automazione senza interruzioni con CLI</li> </ul>
Standard	9.0 o versione successiva	Singola	"Interruzione automatizzata"
MetroCluster	9.3 o versione successiva	8	<ul style="list-style-type: none"> <li>• Automazione senza interruzioni con CLI</li> <li>• Manuale senza interruzioni per MetroCluster a 4 o 8 nodi utilizzando la CLI</li> </ul>
MetroCluster	9.3 o versione successiva	2,4	<ul style="list-style-type: none"> <li>• Automazione senza interruzioni con System Manager</li> <li>• Automazione senza interruzioni con CLI</li> </ul>
MetroCluster	9.2 o versioni precedenti	4, 8	Manuale senza interruzioni per MetroCluster a 4 o 8 nodi utilizzando la CLI
MetroCluster	9.2 o versioni precedenti	2	Manuale senza interruzioni per MetroCluster a 2 nodi utilizzando la CLI

L'utilizzo di System Manager è il metodo di aggiornamento consigliato per tutti gli aggiornamenti delle patch, indipendentemente dalla configurazione.



R [aggiornamento manuale con interruzioni delle attività](#) può essere eseguita su qualsiasi configurazione. Tuttavia, non si consiglia di eseguire un aggiornamento senza interruzioni, a meno che non sia possibile disattivare il cluster per tutta la durata dell'aggiornamento. Se si opera in un ambiente SAN, è necessario essere pronti a chiudere o sospendere tutti i client SAN prima di eseguire un aggiornamento disgregativo. Gli aggiornamenti disruptive vengono eseguiti utilizzando l'interfaccia utente di ONTAP.

### Upgrade ONTAP senza interruzioni e automatizzati

Quando esegui un upgrade automatico, ONTAP installa automaticamente l'immagine ONTAP di destinazione su ogni nodo, convalida la possibilità di aggiornare il cluster ed esegue quindi un [batch o rolling upgrade](#) in background in base al numero di nodi nel

cluster.

Se è supportato dalla configurazione, è necessario utilizzare System Manager per eseguire un aggiornamento automatico. Se la configurazione in uso non supporta l'upgrade automatico con System Manager, puoi utilizzare l'interfaccia a riga di comando (CLI) di ONTAP per eseguire un upgrade automatico.



Modifica dell'impostazione di `storage failover modify-auto-giveback` L'opzione di comando prima dell'avvio di un aggiornamento automatico senza interruzioni non ha alcun impatto sul processo di aggiornamento. Il processo ANDU ignora qualsiasi valore preimpostato di questa opzione durante il takeover/giveback richiesto per l'aggiornamento. Ad esempio, l'impostazione `-autogiveback To false` prima di iniziare ANDU non interrompe l'aggiornamento automatico prima del giveback.

### Prima di iniziare

- Dovresti ["prepararsi per l'aggiornamento"](#).
- Dovresti ["Scaricare l'immagine del software ONTAP"](#) Per la versione ONTAP di destinazione.

Se si sta eseguendo un ["upgrade diretto multi-hop"](#), È necessario scaricare entrambe le immagini ONTAP richieste per lo specifico ["percorso di upgrade"](#).

- Per ogni coppia ha, ogni nodo deve avere una o più porte sullo stesso dominio di trasmissione.

Se si dispone di 8 o più nodi, il metodo di aggiornamento in batch viene utilizzato nell'aggiornamento automatico senza interruzioni. In ONTAP 9.7 e versioni precedenti, se viene utilizzato il metodo batch, i file LIF vengono migrati al partner ha del nodo da aggiornare. Se i partner non hanno porte nello stesso dominio di broadcast, la migrazione LIF non riesce.

In ONTAP 9.8 e versioni successive, se viene utilizzato il metodo batch, i file LIF vengono migrati nell'altro gruppo batch.

- Se stai eseguendo l'upgrade di ONTAP in una configurazione FC di MetroCluster, il cluster dovrebbe essere abilitato per uno switchover automatico e non pianificato.
- Se non si prevede di monitorare l'avanzamento del processo di aggiornamento, è necessario ["Richiedere notifiche EMS di errori che potrebbero richiedere un intervento manuale"](#).
- Se disponi di un cluster a nodo singolo, segui la ["upgrade con interruzioni automatiche"](#) processo.

Gli upgrade dei cluster a nodo singolo comportano interruzioni.



## Esempio 2. Fasi

### System Manager

#### 1. Convalida dell'immagine di destinazione ONTAP:



Se si sta aggiornando una configurazione MetroCluster, è necessario convalidare il cluster A e ripetere la procedura di convalida sul cluster B.

#### a. A seconda della versione di ONTAP in esecuzione, eseguire una delle seguenti operazioni:

Se si esegue...	Eseguire questa operazione...
ONTAP 9.8 o versione successiva	Fare clic su <b>Cluster &gt; Overview</b> (Cluster > Panoramica).
ONTAP 9.5, 9.6 e 9.7	Fare clic su <b>Configuration &gt; Cluster &gt; Update</b> .
ONTAP 9.4 o versioni precedenti	Fare clic su <b>Configuration &gt; Cluster Update</b> .

#### b. Nell'angolo destro del riquadro **Panoramica**, fare clic su .

#### c. Fare clic su **aggiornamento ONTAP**.

#### d. Nella scheda **Cluster Update**, aggiungere una nuova immagine o selezionare un'immagine disponibile.

Se si desidera...	Quindi...
Aggiungere una nuova immagine software da una cartella locale  Dovresti già averlo fatto "immagine scaricata" al client locale.	<ul style="list-style-type: none"><li>i. In <b>immagini software disponibili</b>, fare clic su <b>Aggiungi da locale</b>.</li><li>ii. Individuare la posizione in cui è stata salvata l'immagine software, selezionare l'immagine, quindi fare clic su <b>Apri</b>.</li></ul>
Aggiungere una nuova immagine software da un server HTTP o FTP	<ul style="list-style-type: none"><li>i. Fare clic su <b>Aggiungi dal server</b>.</li><li>ii. Nella finestra di dialogo <b>Aggiungi nuova immagine software</b>, immettere l'URL del server HTTP o FTP sul quale è stata scaricata l'immagine del software ONTAP dal sito di supporto NetApp.  Per l'FTP anonimo, è necessario specificare l'URL in <a href="ftp://anonymous@ftpserver">ftp://anonymous@ftpserver</a> formato.</li><li>iii. Fare clic su <b>Aggiungi</b>.</li></ul>
Selezionare un'immagine disponibile	Scegliere una delle immagini elencate.

e. Fare clic su **convalida** per eseguire i controlli di convalida pre-aggiornamento.

Se durante la convalida vengono rilevati errori o avvisi, questi vengono visualizzati insieme a un elenco di azioni correttive. È necessario risolvere tutti gli errori prima di procedere con l'aggiornamento. È buona norma risolvere anche gli avvisi.

2. Fare clic su **Avanti**.

3. Fare clic su **Aggiorna**.

La convalida viene eseguita di nuovo. Gli eventuali errori o avvisi rimanenti vengono visualizzati insieme a un elenco di azioni correttive. Gli errori devono essere corretti prima di procedere con l'aggiornamento. Se la convalida viene completata con avvisi, è possibile correggere gli avvisi o scegliere **Aggiorna con avvisi**.



Per impostazione predefinita, ONTAP utilizza "[processo di aggiornamento in batch](#)" per aggiornare i cluster con otto o più nodi. A partire da ONTAP 9.10.1, se si preferisce, è possibile selezionare **Aggiorna una coppia ha alla volta** per sovrascrivere l'impostazione predefinita e fare in modo che il cluster aggiorni una coppia ha alla volta utilizzando il processo di rolling upgrade.

Per le configurazioni MetroCluster con più di 2 nodi, il processo di upgrade ONTAP viene avviato contemporaneamente sulle coppie ha in entrambi i siti. Per una configurazione MetroCluster a 2 nodi, l'upgrade viene avviato per primo nel sito in cui non è stato avviato. L'aggiornamento sul sito rimanente inizia dopo il completamento del primo aggiornamento.

4. Se l'aggiornamento viene sospeso a causa di un errore, fare clic sul messaggio di errore per visualizzare i dettagli, quindi correggere l'errore e. "[riprendere l'aggiornamento](#)".

#### Al termine

Una volta completato l'aggiornamento, il nodo viene riavviato e viene reindirizzato alla pagina di accesso di System Manager. Se il riavvio del nodo richiede molto tempo, è necessario aggiornare il browser.

#### CLI

1. Convalidare l'immagine del software di destinazione ONTAP



Se stai aggiornando una configurazione MetroCluster, devi prima eseguire i seguenti passaggi sul cluster A, quindi eseguire gli stessi passaggi sul cluster B.

a. Eliminare il pacchetto software ONTAP precedente:

```
cluster image package delete -version previous_ONTAP_Version
```

b. Caricare l'immagine software ONTAP di destinazione nell'archivio dei pacchetti cluster:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.13.1/image.tgz

Package download completed.
Package processing completed.
```

Se si sta eseguendo un "upgrade diretto multi-hop", È inoltre necessario caricare il pacchetto software per la versione intermedia di ONTAP richiesta per l'aggiornamento. Ad esempio, se si sta eseguendo l'aggiornamento da 9,8 a 9.13.1, è necessario caricare il pacchetto software per ONTAP 9.12.1, quindi utilizzare lo stesso comando per caricare il pacchetto software per 9.13.1.

- c. Verificare che il pacchetto software sia disponibile nel repository dei pacchetti del cluster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.13.1           MM/DD/YYYY 10:32:15
```

- d. Eseguire i controlli automatici pre-aggiornamento:

```
cluster image validate -version package_version_number
```

Se si sta eseguendo un "upgrade diretto multi-hop", È sufficiente utilizzare il pacchetto ONTAP di destinazione per la verifica. Non è necessario convalidare separatamente l'immagine di aggiornamento intermedia. Ad esempio, se si sta eseguendo l'aggiornamento da 9,8 a 9.13.1, utilizzare il pacchetto 9.13.1 per la verifica. Non è necessario convalidare il pacchetto 9.12.1 separatamente.

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed...
```

- a. Monitorare l'avanzamento della convalida:

```
cluster image show-update-progress
```

- b. Completare tutte le azioni richieste identificate dalla convalida.

- c. Se si sta aggiornando una configurazione MetroCluster, ripetere i passaggi precedenti sul cluster B.

2. Generare una stima dell'aggiornamento del software:

```
cluster image update -version package_version_number -estimate-only
```



Se si sta aggiornando una configurazione MetroCluster, è possibile eseguire questo comando sul cluster A o B. Non è necessario eseguirlo su entrambi i cluster.

La stima dell'aggiornamento software visualizza i dettagli relativi a ciascun componente da aggiornare e la durata stimata dell'aggiornamento.

3. Eseguire l'aggiornamento del software:

```
cluster image update -version package_version_number
```

- Se si sta eseguendo un **"upgrade diretto multi-hop"**, Utilizzare la versione ONTAP di destinazione per il numero\_versione\_pacchetto. Ad esempio, se si esegue l'aggiornamento da ONTAP 9.8 a 9.13.1, utilizzare 9.13.1 come numero\_versione\_pacchetto.
- Per impostazione predefinita, ONTAP utilizza **"processo di aggiornamento in batch"** per aggiornare i cluster con otto o più nodi. Se si preferisce, è possibile utilizzare `-force-rolling` parametro che consente di ignorare il processo predefinito e di aggiornare il cluster di un nodo alla volta utilizzando il processo di aggiornamento in sequenza.
- Dopo aver completato ogni takeover e giveback, l'aggiornamento attende 8 minuti per consentire alle applicazioni client di eseguire il ripristino dalla pausa in i/o che si verifica durante il takeover e il giveback. Se l'ambiente richiede più o meno tempo per la stabilizzazione del client, è possibile utilizzare `-stabilize-minutes` parametro per specificare una quantità diversa di tempo di stabilizzazione.
- Per le configurazioni MetroCluster con 4 nodi in più, l'upgrade automatizzato si avvia contemporaneamente sulle coppie ha in entrambi i siti. Per una configurazione MetroCluster a 2 nodi, l'upgrade viene avviato dal sito in cui non è stato avviato. L'aggiornamento sul sito rimanente inizia dopo il completamento del primo aggiornamento.

```

cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status      Error-Action
-----
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>

```

4. Visualizzare l'avanzamento dell'aggiornamento del cluster:

```
cluster image show-update-progress
```

Se si sta aggiornando una configurazione MetroCluster a 4 o 8 nodi, il `cluster image show-update-progress` command visualizza solo l'avanzamento del nodo su cui viene eseguito il comando. È necessario eseguire il comando su ciascun nodo per visualizzare l'avanzamento dei singoli nodi.

5. Verificare che l'aggiornamento sia stato completato correttamente su ciascun nodo.

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress
```

Elapsed Update Phase Duration	Status	Estimated Duration
-----	-----	-----
-----		
Pre-update checks 00:02:07	completed	00:10:00
Data ONTAP updates 01:39:00	completed	01:31:00
Post-update checks 00:02:00	completed	00:10:00

3 entries were displayed.

Updated nodes: node0, node1.

6. Attivare una notifica AutoSupport:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Se il cluster non è configurato per l'invio di messaggi AutoSupport, una copia della notifica viene salvata localmente.

7. Se stai eseguendo l'upgrade di una configurazione MetroCluster FC a 2 nodi, verifica che il cluster sia abilitato per lo switchover automatico e non pianificato.



Se si sta aggiornando una configurazione standard, una configurazione IP MetroCluster o una configurazione FC MetroCluster con più di 2 nodi, non è necessario eseguire questa operazione.

a. Controllare se è attivato lo switchover automatico non pianificato:

```
metrocluster show
```

Se è attivato lo switchover automatico non pianificato, nell'output del comando viene visualizzata la seguente istruzione:

```
AUSO Failure Domain      auso-on-cluster-disaster
```

a. Se l'istruzione non viene visualizzata nell'output, abilitare lo switchover automatico non pianificato:

```
metrocluster modify -auto-switchover-failure-domain auso-on-  
cluster-disaster
```

- b. Verificare che sia stato attivato lo switchover automatico non pianificato:

```
metrocluster show
```

#### **Riprendere l'aggiornamento del software ONTAP dopo un errore nel processo di aggiornamento automatico**

Se un aggiornamento automatico del software ONTAP si interrompe a causa di un errore, è necessario risolvere l'errore e continuare l'aggiornamento. Una volta risolto l'errore, è possibile scegliere di continuare il processo di aggiornamento automatico o di completare manualmente il processo di aggiornamento. Se si sceglie di continuare l'aggiornamento automatico, non eseguire manualmente alcuna procedura di aggiornamento.

### Esempio 3. Fasi

#### System Manager

1. A seconda della versione di ONTAP in esecuzione, eseguire una delle seguenti operazioni:

Se si esegue...	Quindi...
ONTAP 9.8 o versione successiva	Fare clic su <b>Cluster &gt; Overview</b>
ONTAP 9,7, 9,6 o 9,5	Fare clic su <b>Configuration &gt; Cluster &gt; Update.</b>
ONTAP 9.4 o versioni precedenti	<ul style="list-style-type: none"><li>• Fare clic su <b>Configuration &gt; Cluster Update.</b></li><li>• Nell'angolo destro del riquadro <b>Panoramica</b>, fare clic sui tre punti verticali blu e selezionare <b>aggiornamento ONTAP.</b></li></ul>

2. Continuare l'aggiornamento automatico o annullarlo e continuare manualmente.

Se si desidera...	Quindi...
Riprendere l'aggiornamento automatico	Fare clic su <b>Riprendi.</b>
Annullare l'aggiornamento automatico e continuare manualmente	Fare clic su <b>Annulla.</b>

#### CLI

1. Visualizzare l'errore di aggiornamento:

```
cluster image show-update-progress
```

2. Risolvere l'errore.
3. Riprendere l'aggiornamento:

Se si desidera...	Immettere il seguente comando...
Riprendere l'aggiornamento automatico	<pre>cluster image resume-update</pre>
Annullare l'aggiornamento automatico e continuare manualmente	<pre>cluster image cancel-update</pre>

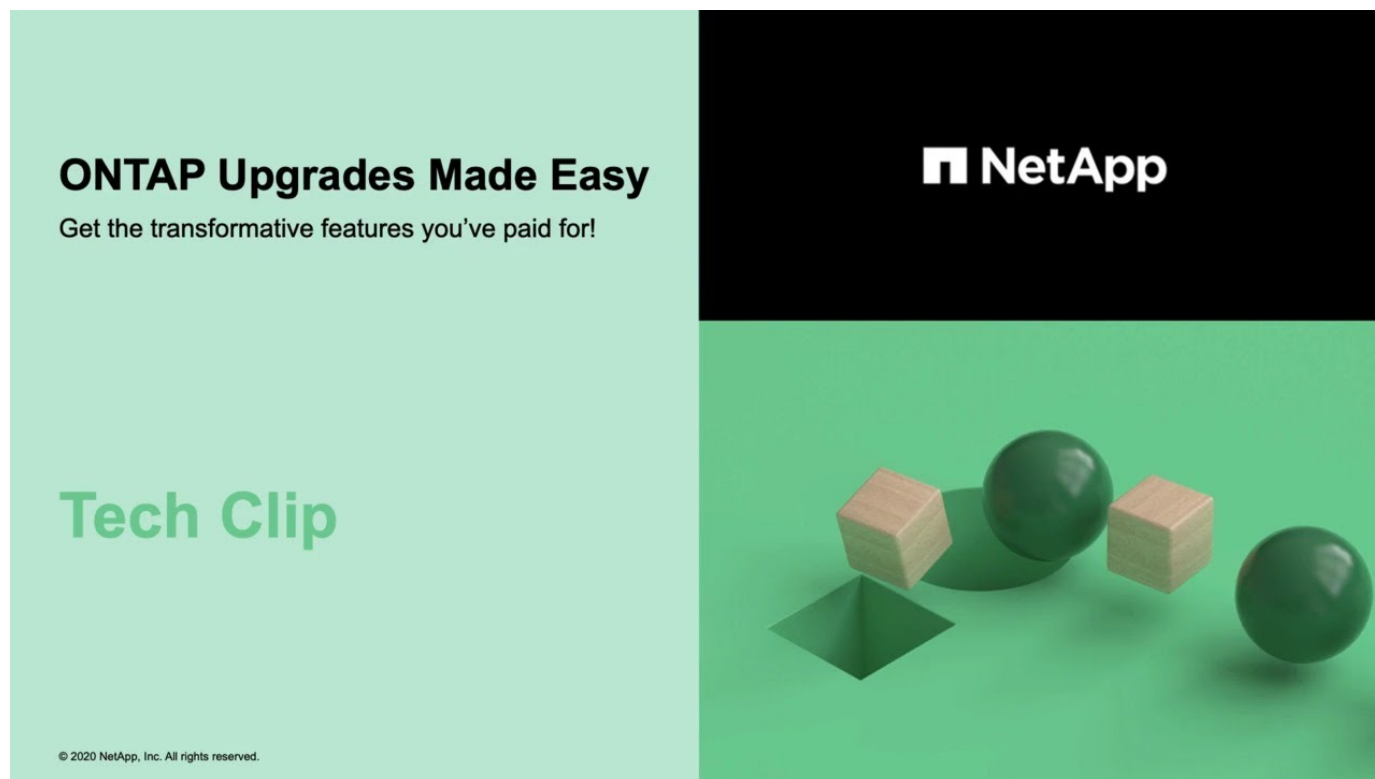
#### Al termine



["Eseguire i controlli post-aggiornamento"](#).

#### Video: Aggiornamenti semplificativi

Date un'occhiata alle funzionalità di aggiornamento ONTAP semplificate di Gestione sistemi in ONTAP 9.8.



#### Informazioni correlate

- ["Avviare Active IQ"](#)
- ["Documentazione Active IQ"](#)

#### Aggiornamenti manuali

Installare il pacchetto software ONTAP per gli aggiornamenti manuali

Dopo aver scaricato il pacchetto software ONTAP per un aggiornamento manuale, è necessario installarlo localmente prima di iniziare l'aggiornamento.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato), immettendo **y** quando viene richiesto di continuare: `set -privilege advanced`

Il prompt avanzato (\*>).

2. Installare l'immagine.

Se si possiede la seguente configurazione...	Utilizzare questo comando...
<ul style="list-style-type: none"> <li>• Non MetroCluster</li> <li>• MetroCluster a 2 nodi</li> </ul>	<pre>system node image update -node * -package _location_ -replace -package true -setdefault true -background true</pre> <p><i>Location</i> può essere un server Web o una cartella locale, a seconda della versione di ONTAP. Vedere <a href="#">system node image update pagina man</a> per i dettagli.</p> <p>Questo comando installa l'immagine software su tutti i nodi contemporaneamente. Per installare l'immagine su ciascun nodo uno alla volta, non specificare <code>-background</code> parametro.</p>
<ul style="list-style-type: none"> <li>• MetroCluster a 4 nodi</li> <li>• Configurazione MetroCluster a 8 nodi</li> </ul>	<pre>system node image update -node * -package location -replace -package true -background true -setdefault false</pre> <p>È necessario eseguire questo comando su entrambi i cluster.</p> <p>Questo comando utilizza una query estesa per modificare l'immagine software di destinazione, che viene installata come immagine alternativa su ciascun nodo.</p>

3. Invio `y` per continuare quando richiesto.

4. Verificare che l'immagine software sia installata su ciascun nodo.

```
system node image show-update-progress -node *
```

Questo comando visualizza lo stato corrente dell'installazione dell'immagine software. Continuare ad eseguire questo comando fino a quando tutti i nodi non riportano un **Run Status di Exit** e un **Exit Status di Success**.

Il comando di aggiornamento dell'immagine del nodo di sistema può non riuscire e visualizzare messaggi di errore o di avviso. Dopo aver risolto eventuali errori o avvisi, è possibile eseguire nuovamente il comando.

Questo esempio mostra un cluster a due nodi in cui l'immagine software viene installata correttamente su entrambi i nodi:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

#### Upgrade manuale e senza interruzioni della ONTAP utilizzando la CLI (configurazioni standard)

L'aggiornamento automatico tramite System Manager è il metodo di aggiornamento preferito. Se System Manager non supporta la configurazione in uso, puoi utilizzare l'interfaccia a riga di comando (CLI) di ONTAP per eseguire un aggiornamento manuale senza interruzione delle attività. Per aggiornare un cluster di due o più nodi utilizzando il metodo manuale senza interruzioni, è necessario avviare un'operazione di failover su ciascun nodo di una coppia ha, aggiornare il nodo "failed", avviare il giveback, quindi ripetere il processo per ogni coppia ha nel cluster.

#### Prima di iniziare

È necessario avere soddisfatto l'aggiornamento ["preparazione"](#) requisiti.

#### Aggiornamento del primo nodo di una coppia ha

È possibile aggiornare il primo nodo di una coppia ha avviando un Takeover da parte del partner del nodo. Il partner serve i dati del nodo mentre il primo nodo viene aggiornato.

Se si esegue un aggiornamento importante, il primo nodo da aggiornare deve essere lo stesso nodo su cui sono stati configurati i file ONTAP per la connettività esterna e installata la prima immagine LIF.

Dopo aver aggiornato il primo nodo, è necessario aggiornare il nodo partner il più rapidamente possibile. Non consentire ai due nodi di rimanere in un ["versione mista"](#) stato più lungo del necessario.

#### Fasi

1. Aggiornare il primo nodo del cluster richiamando un messaggio AutoSupport:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Questa notifica AutoSupport include un record dello stato del sistema appena prima dell'aggiornamento. Consente di salvare informazioni utili per la risoluzione dei problemi in caso di problemi con il processo di aggiornamento.

Se il cluster non è configurato per inviare messaggi AutoSupport, una copia della notifica viene salvata localmente.

2. Impostare il livello di privilegio su Advanced (avanzato), immettendo **y** quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato (\*>).

3. Impostare la nuova immagine del software ONTAP come immagine predefinita:

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

Il comando di modifica dell'immagine di sistema utilizza una query estesa per modificare la nuova immagine del software ONTAP (installata come immagine alternativa) con l'immagine predefinita per il nodo.

4. Monitorare l'avanzamento dell'aggiornamento:

```
system node upgrade-revert show
```

5. Verificare che la nuova immagine del software ONTAP sia impostata come immagine predefinita:

```
system image show
```

Nell'esempio seguente, image2 è la nuova versione di ONTAP ed è impostata come immagine predefinita su node0:

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

6. Disattiva il giveback automatico sul nodo partner se è attivato:

```
storage failover modify -node nodenameB -auto-giveback false
```

Se il cluster è un cluster a due nodi, viene visualizzato un messaggio che avvisa che la disattivazione del giveback automatico impedisce ai servizi del cluster di gestione di passare in linea in caso di guasto alternato. Invio `y` per continuare.

7. Verificare che il giveback automatico sia disattivato per il partner del nodo:

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node      auto-giveback
-----  -
node1     false
1 entry was displayed.
```

8. Eseguire due volte il comando seguente per determinare se il nodo da aggiornare sta attualmente servendo qualsiasi client

```
system node run -node nodenameA -command uptime
```

Il comando `uptime` visualizza il numero totale di operazioni eseguite dal nodo per client NFS, SMB, FC e iSCSI dall'ultimo avvio del nodo. Per ciascun protocollo, è necessario eseguire il comando due volte per determinare se i conteggi delle operazioni sono in aumento. Se sono in aumento, il nodo sta attualmente servendo i client per quel protocollo. Se non sono in aumento, il nodo non sta attualmente servendo client per quel protocollo.



È necessario prendere nota di ciascun protocollo che ha un aumento delle operazioni client in modo che, dopo l'aggiornamento del nodo, sia possibile verificare che il traffico client sia stato ripreso.

L'esempio seguente mostra un nodo con operazioni NFS, SMB, FC e iSCSI. Tuttavia, il nodo attualmente serve solo client NFS e iSCSI.

```
cluster1::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. Eseguire la migrazione di tutti i file LIF dei dati lontano dal nodo:

```
network interface migrate-all -node nodenameA
```

10. Verificare le LIF migrate:

```
network interface show
```

Per ulteriori informazioni sui parametri che è possibile utilizzare per verificare lo stato LIF, vedere la pagina man dell'interfaccia di rete.

Nell'esempio seguente viene mostrato che le LIF dei dati di node0 sono state migrate correttamente. Per ogni LIF, i campi inclusi in questo esempio consentono di verificare il nodo principale e la porta della LIF, il nodo e la porta correnti su cui è stata eseguita la migrazione e lo stato operativo e amministrativo della LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
vs0      data001 node0      e0a      node1      e0a      up      up
vs0      data002 node0      e0b      node1      e0b      up      up
vs0      data003 node0      e0b      node1      e0b      up      up
vs0      data004 node0      e0a      node1      e0a      up      up
4 entries were displayed.
```

11. Avviare un Takeover:

```
storage failover takeover -ofnode nodenameA
```

Non specificare il parametro `-option immediate`, perché è necessario un normale Takeover per il nodo che viene sostituito per avviare la nuova immagine software. Se non hai eseguito la migrazione manuale dei LIF dal nodo, questi migrano automaticamente al partner ha del nodo per garantire che non ci siano interruzioni del servizio.

Il primo nodo si avvia nello stato in attesa di giveback.



Se AutoSupport è attivato, viene inviato un messaggio AutoSupport che indica che il nodo non è al di fuori del quorum del cluster. È possibile ignorare questa notifica e procedere con l'aggiornamento.

12. Verificare che l'acquisizione sia riuscita:

```
storage failover show
```

Potrebbero essere visualizzati messaggi di errore che indicano una mancata corrispondenza della versione e problemi di formato della mailbox. Si tratta di un comportamento previsto che rappresenta uno stato temporaneo in un aggiornamento senza interruzioni e non è dannoso.

L'esempio seguente mostra che l'acquisizione è riuscita. Il nodo node0 si trova nello stato in attesa di giveback e il suo partner si trova nello stato in takeover.

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node0	node1	-	Waiting for giveback (HA mailboxes)
node1	node0	false	In takeover

2 entries were displayed.

13. Attendere almeno otto minuti per rendere effettive le seguenti condizioni:

- Il multipathing client (se implementato) è stabilizzato.
- I client vengono ripristinati dalla pausa in un'operazione di i/o che si verifica durante il takeover.

Il tempo di ripristino è specifico del client e potrebbe richiedere più di otto minuti, a seconda delle caratteristiche delle applicazioni client.

14. Restituire gli aggregati al primo nodo:

```
storage failover giveback -ofnode nodenameA
```

Il giveback restituisce prima l'aggregato root al nodo partner, quindi, una volta terminato l'avvio del nodo, restituisce gli aggregati non root e tutte le LIF impostate per il ripristino automatico. Il nodo appena avviato inizia a fornire i dati ai client da ciascun aggregato non appena l'aggregato viene restituito.

15. Verificare che tutti gli aggregati siano stati restituiti:

```
storage failover show-giveback
```

Se il campo Stato giveback indica che non ci sono aggregati da restituire, tutti gli aggregati sono stati restituiti. Se il giveback viene veto, il comando visualizza l'avanzamento del giveback e il sottosistema che ha veto il giveback.

16. Se non sono stati restituiti aggregati, attenersi alla seguente procedura:

- a. Esaminare la soluzione alternativa al veto per determinare se si desidera risolvere la condizione "veto" o ignorare il veto.

- b. Se necessario, risolvere la condizione “veto” descritta nel messaggio di errore, assicurandosi che tutte le operazioni identificate vengano terminate correttamente.
- c. Eseguire nuovamente il comando giveback di failover dello storage.

Se si decide di eseguire l'override della condizione “veto”, impostare il parametro -override-vetoes su true.

17. Attendere almeno otto minuti per rendere effettive le seguenti condizioni:

- Il multipathing client (se implementato) è stabilizzato.
- I client vengono ripristinati dalla pausa in un'operazione di i/o che si verifica durante il giveback.

Il tempo di ripristino è specifico del client e potrebbe richiedere più di otto minuti, a seconda delle caratteristiche delle applicazioni client.

18. Verificare che l'aggiornamento sia stato completato correttamente per il nodo:

a. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

b. Verificare che lo stato di aggiornamento sia completo per il nodo:

```
system node upgrade-revert show -node nodenameA
```

Lo stato deve essere indicato come completo.

Se lo stato non è completo, contattare il supporto tecnico.

a. Tornare al livello di privilegio admin:

```
set -privilege admin
```

19. Verificare che le porte del nodo siano in funzione:

```
network port show -node nodenameA
```

È necessario eseguire questo comando su un nodo aggiornato alla versione successiva di ONTAP 9.

L'esempio seguente mostra che tutte le porte del nodo sono in funzione:



```
cluster1::> network port show -node node0
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	-----
node0						
	e0M	Default	-	up	1500	auto/100
	e0a	Default	-	up	1500	auto/1000
	e0b	Default	-	up	1500	auto/1000
	e1a	Cluster	Cluster	up	9000	auto/10000
	e1b	Cluster	Cluster	up	9000	auto/10000
5 entries were displayed.						

20. Ripristinare i LIF al nodo:

```
network interface revert *
```

Questo comando restituisce i LIF migrati dal nodo.

```
cluster1::> network interface revert *  
8 entries were acted on.
```

21. Verificare che le LIF dei dati del nodo siano ripristinate correttamente al nodo e che siano in funzione:

```
network interface show
```

L'esempio seguente mostra che tutti i dati LIF ospitati dal nodo sono ritornati correttamente al nodo e che il loro stato operativo è superiore:

```
cluster1::> network interface show
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
vs0					
	data001	up/up	192.0.2.120/24	node0	e0a
true					
	data002	up/up	192.0.2.121/24	node0	e0b
true					
	data003	up/up	192.0.2.122/24	node0	e0b
true					
	data004	up/up	192.0.2.123/24	node0	e0a
true					

4 entries were displayed.

22. Se in precedenza si è stabilito che questo nodo serve i client, verificare che il nodo stia fornendo servizio per ogni protocollo che in precedenza serviva:

```
system node run -node nodenameA -command uptime
```

I conteggi delle operazioni vengono azzerati durante l'aggiornamento.

L'esempio seguente mostra che il nodo aggiornato ha ripreso a servire i propri client NFS e iSCSI:

```
cluster1::> system node run -node node0 -command uptime
3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. Riabilitare il giveback automatico sul nodo partner se era stato precedentemente disattivato:

```
storage failover modify -node nodenameB -auto-giveback true
```

È necessario procedere all'aggiornamento del partner ha del nodo il più rapidamente possibile. Se è necessario sospendere il processo di aggiornamento per qualsiasi motivo, entrambi i nodi della coppia ha devono eseguire la stessa versione di ONTAP.

### Aggiornamento del nodo partner in una coppia ha

Dopo aver aggiornato il primo nodo di una coppia ha, si aggiorna il proprio partner avviando un Takeover su di esso. Il primo nodo serve i dati del partner mentre il nodo del partner viene aggiornato.

1. Impostare il livello di privilegio su Advanced (avanzato), immettendo **y** quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato (\*>).

2. Impostare la nuova immagine del software ONTAP come immagine predefinita:

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

Il comando di modifica dell'immagine di sistema utilizza una query estesa per modificare la nuova immagine del software ONTAP (installata come immagine alternativa) come immagine predefinita per il nodo.

3. Monitorare l'avanzamento dell'aggiornamento:

```
system node upgrade-revert show
```

4. Verificare che la nuova immagine del software ONTAP sia impostata come immagine predefinita:

```
system image show
```

Nell'esempio seguente, image2 È la nuova versione di ONTAP ed è impostata come immagine predefinita sul nodo:

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node1	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

5. Disattiva il giveback automatico sul nodo partner se è attivato:

```
storage failover modify -node nodenameA -auto-giveback false
```

Se il cluster è un cluster a due nodi, viene visualizzato un messaggio che avvisa che la disattivazione del giveback automatico impedisce ai servizi del cluster di gestione di passare in linea in caso di guasto alternato. Invio `y` per continuare.

6. Verificare che il giveback automatico sia disattivato per il nodo partner:

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node      auto-giveback
-----
node0     false
1 entry was displayed.
```

7. Eseguire due volte il seguente comando per determinare se il nodo da aggiornare sta attualmente servendo qualsiasi client:

```
system node run -node nodenameB -command uptime
```

Il comando `uptime` visualizza il numero totale di operazioni eseguite dal nodo per client NFS, SMB, FC e iSCSI dall'ultimo avvio del nodo. Per ciascun protocollo, è necessario eseguire il comando due volte per determinare se i conteggi delle operazioni sono in aumento. Se sono in aumento, il nodo sta attualmente servendo i client per quel protocollo. Se non sono in aumento, il nodo non sta attualmente servendo client per quel protocollo.

**NOTA:** Prendere nota di ogni protocollo che presenta operazioni client in aumento in modo che, dopo l'aggiornamento del nodo, sia possibile verificare che il traffico client sia ripreso.

L'esempio seguente mostra un nodo con operazioni NFS, SMB, FC e iSCSI. Tuttavia, il nodo attualmente serve solo client NFS e iSCSI.

```
cluster1::> system node run -node node1 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Eseguire la migrazione di tutti i file LIF dei dati lontano dal nodo:

```
network interface migrate-all -node nodenameB
```

9. Verificare lo stato dei file LIF migrati:

```
network interface show
```

Per ulteriori informazioni sui parametri che è possibile utilizzare per verificare lo stato LIF, vedere la pagina man dell'interfaccia di rete.

Nell'esempio seguente viene mostrato che le LIF dei dati di node1 sono state migrate correttamente. Per ogni LIF, i campi inclusi in questo esempio consentono di verificare il nodo principale e la porta della LIF, il nodo e la porta correnti su cui è stata eseguita la migrazione e lo stato operativo e amministrativo della LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
vs0      data001 node1      e0a      node0      e0a      up      up
vs0      data002 node1      e0b      node0      e0b      up      up
vs0      data003 node1      e0b      node0      e0b      up      up
vs0      data004 node1      e0a      node0      e0a      up      up
4 entries were displayed.
```

#### 10. Avviare un Takeover:

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

Non specificare il parametro `-option immediate`, perché è necessario un normale Takeover per il nodo che viene sostituito per avviare la nuova immagine software. Se non hai eseguito la migrazione manuale dei LIF dal nodo, questi migrano automaticamente al partner ha del nodo, in modo da evitare interruzioni del servizio.

Viene visualizzato un avviso. È necessario immettere `y` per continuare.

Il nodo preso in consegna si avvia fino allo stato in attesa di giveback.



Se AutoSupport è attivato, viene inviato un messaggio AutoSupport che indica che il nodo non è al di fuori del quorum del cluster. È possibile ignorare questa notifica e procedere con l'aggiornamento.

#### 11. Verificare che l'acquisizione sia stata eseguita correttamente:

```
storage failover show
```

L'esempio seguente mostra che l'acquisizione è riuscita. Il nodo node1 si trova nello stato in attesa di

giveback e il suo partner si trova nello stato in takeover.

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node0	node1	-	In takeover
node1	node0	false	Waiting for giveback (HA mailboxes)

2 entries were displayed.

12. Attendere almeno otto minuti per rendere effettive le seguenti condizioni:

+

**Il multipathing client (se implementato) è stabilizzato.**

I client vengono ripristinati dalla pausa in i/o che si verifica durante il takeover.

+

Il tempo di ripristino è specifico del client e potrebbe richiedere più di otto minuti, a seconda delle caratteristiche delle applicazioni client.

13. Restituire gli aggregati al nodo partner:

```
storage failover giveback -ofnode nodenameB
```

L'operazione di giveback restituisce prima l'aggregato root al nodo partner, quindi, una volta terminato l'avvio del nodo, restituisce gli aggregati non root e tutte le LIF impostate per il ripristino automatico. Il nodo appena avviato inizia a fornire i dati ai client da ciascun aggregato non appena l'aggregato viene restituito.

14. Verificare che tutti gli aggregati siano restituiti:

```
storage failover show-giveback
```

Se il campo Stato giveback indica che non ci sono aggregati da restituire, vengono restituiti tutti gli aggregati. Se il giveback viene vetoato, il comando visualizza l'avanzamento del giveback e il sottosistema che ha vetoato l'operazione di giveback.

15. Se non vengono restituiti aggregati, attenersi alla seguente procedura:

- Esaminare la soluzione alternativa al veto per determinare se si desidera risolvere la condizione "veto" o ignorare il veto.
- Se necessario, risolvere la condizione "veto" descritta nel messaggio di errore, assicurandosi che tutte le operazioni identificate vengano terminate correttamente.
- Eseguire nuovamente il comando giveback di failover dello storage.

Se si decide di eseguire l'override della condizione "veto", impostare il parametro `-override-vetoes` su `true`.

16. Attendere almeno otto minuti per rendere effettive le seguenti condizioni:

- Il multipathing client (se implementato) è stabilizzato.
- I client vengono ripristinati dalla pausa in un'operazione di i/o che si verifica durante il giveback.

Il tempo di ripristino è specifico del client e potrebbe richiedere più di otto minuti, a seconda delle caratteristiche delle applicazioni client.

17. Verificare che l'aggiornamento sia stato completato correttamente per il nodo:

a. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

b. Verificare che lo stato di aggiornamento sia completo per il nodo:

```
system node upgrade-revert show -node nodenameB
```

Lo stato deve essere indicato come completo.

Se lo stato non è completo, dal nodo eseguire il comando `upgrade-revert upgrade` del nodo di sistema. Se il comando non completa l'aggiornamento, contattare il supporto tecnico.

a. Tornare al livello di privilegio admin:

```
set -privilege admin
```

18. Verificare che le porte del nodo siano in funzione:

```
network port show -node nodenameB
```

Eseguire questo comando su un nodo che è stato aggiornato a ONTAP 9.4.

L'esempio seguente mostra che tutte le porte dati del nodo sono in funzione:

```
cluster1::> network port show -node node1
```

						Speed
(Mbps)						
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	-----	-----	-----	-----	-----	
-----						
node1						
	e0M	Default	-	up	1500	auto/100
	e0a	Default	-	up	1500	auto/1000
	e0b	Default	-	up	1500	auto/1000
	e1a	Cluster	Cluster	up	9000	auto/10000
	e1b	Cluster	Cluster	up	9000	auto/10000
5 entries were displayed.						

19. Ripristinare i LIF al nodo:

```
network interface revert *
```

Questo comando restituisce i LIF migrati dal nodo.

```
cluster1::> network interface revert *  
8 entries were acted on.
```

20. Verificare che le LIF dei dati del nodo siano ripristinate correttamente al nodo e che siano in funzione:

```
network interface show
```

L'esempio seguente mostra che tutti i dati LIF ospitati dal nodo vengono ripristinati correttamente nel nodo e che il loro stato operativo è superiore:



```
cluster1::> network interface show
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
vs0					
	data001	up/up	192.0.2.120/24	node1	e0a
true					
	data002	up/up	192.0.2.121/24	node1	e0b
true					
	data003	up/up	192.0.2.122/24	node1	e0b
true					
	data004	up/up	192.0.2.123/24	node1	e0a
true					

4 entries were displayed.

21. Se in precedenza si è stabilito che questo nodo serve i client, verificare che il nodo stia fornendo servizio per ogni protocollo che in precedenza serviva:

```
system node run -node nodenameB -command uptime
```

I conteggi delle operazioni vengono azzerati durante l'aggiornamento.

L'esempio seguente mostra che il nodo aggiornato ha ripreso a servire i propri client NFS e iSCSI:

```
cluster1::> system node run -node node1 -command uptime
3:15pm up 0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. Se questo era l'ultimo nodo del cluster da aggiornare, attivare una notifica AutoSupport:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Questa notifica AutoSupport include un record dello stato del sistema appena prima dell'aggiornamento. Consente di salvare informazioni utili per la risoluzione dei problemi in caso di problemi con il processo di aggiornamento.

Se il cluster non è configurato per inviare messaggi AutoSupport, una copia della notifica viene salvata localmente.

23. Verificare che il nuovo software ONTAP sia in esecuzione su entrambi i nodi della coppia ha:

```
set -privilege advanced
```

```
system node image show
```

Nell'esempio seguente, image2 è la versione aggiornata di ONTAP ed è la versione predefinita su entrambi i nodi:

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node1	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

24. Riabilitare il giveback automatico sul nodo partner se era stato precedentemente disattivato:

```
storage failover modify -node nodenameA -auto-giveback true
```

25. Verificare che il cluster sia in quorum e che i servizi siano in esecuzione utilizzando `cluster show` e `cluster ring show` (livello di privilegi avanzati).

È necessario eseguire questo passaggio prima di aggiornare eventuali coppie ha aggiuntive.

26. Tornare al livello di privilegio admin:

```
set -privilege admin
```

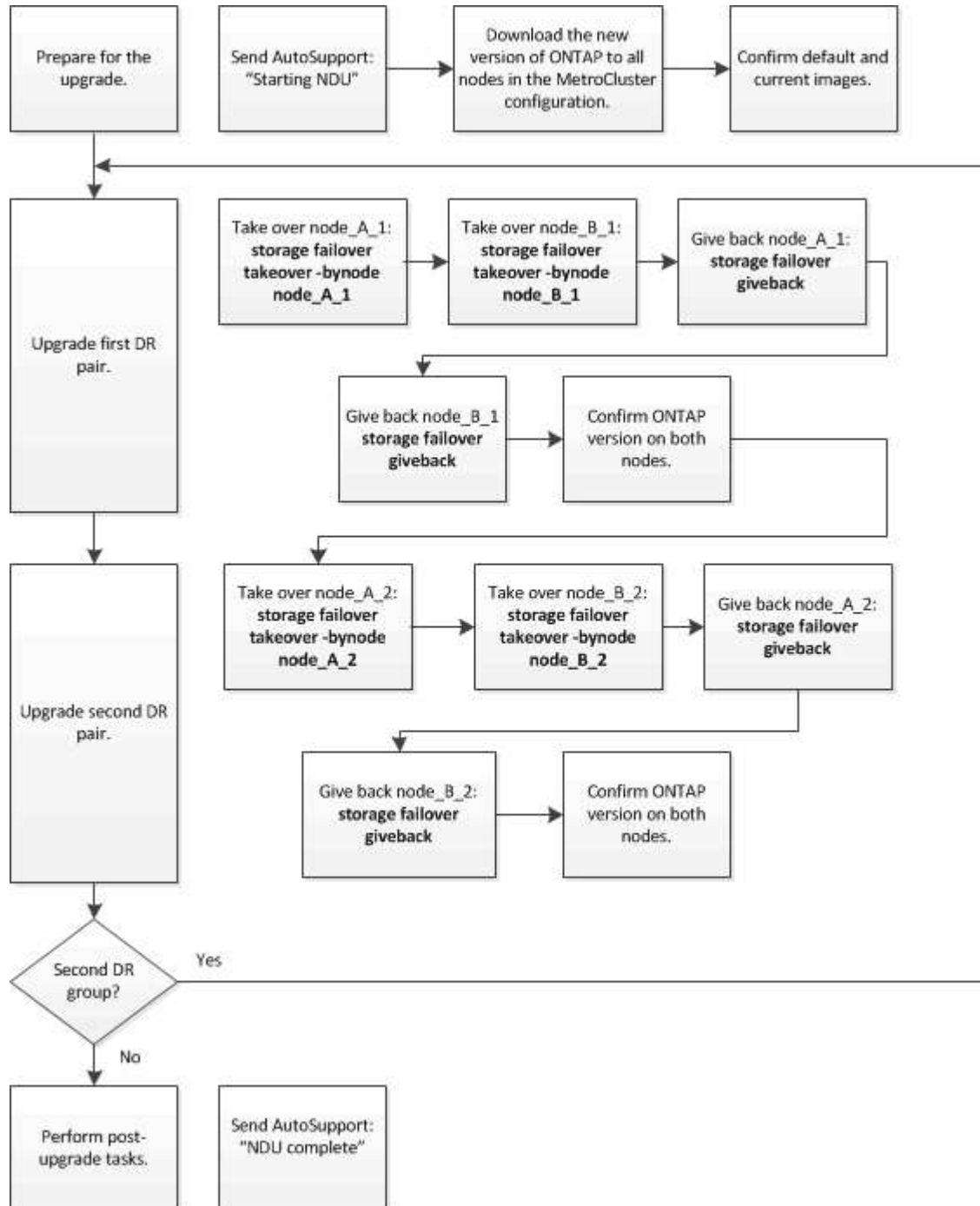
27. Aggiorna eventuali coppie ha aggiuntive.

**Upgrade manuale e senza interruzioni della ONTAP di una configurazione MetroCluster a quattro o otto nodi tramite la CLI**

L'aggiornamento manuale di una configurazione MetroCluster a quattro o otto nodi comporta la preparazione per l'aggiornamento, l'aggiornamento delle coppie di DR in ciascuno di uno o due gruppi DR contemporaneamente e l'esecuzione di task post-aggiornamento.

- Questa attività si applica alle seguenti configurazioni:

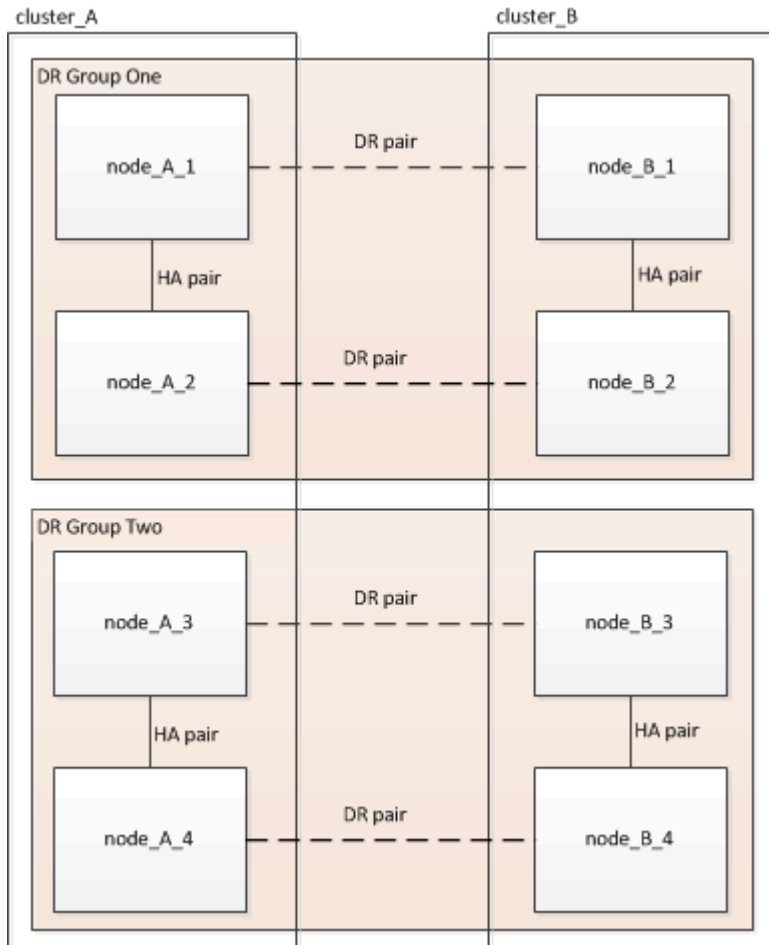
- Configurazioni MetroCluster FC o IP a quattro nodi con ONTAP 9.2 o versione precedente
- Configurazioni MetroCluster FC a otto nodi, indipendentemente dalla versione di ONTAP
- Se si dispone di una configurazione MetroCluster a due nodi, non utilizzare questa procedura.
- Le seguenti operazioni si riferiscono alle versioni precedenti e nuove di ONTAP.
  - Durante l'aggiornamento, la versione precedente è una versione precedente di ONTAP, con un numero di versione inferiore rispetto alla nuova versione di ONTAP.
  - Quando si esegue il downgrade, la versione precedente è una versione successiva di ONTAP, con un numero di versione superiore a quello della nuova versione di ONTAP.
- Questa attività utilizza il seguente flusso di lavoro di alto livello:



## Differenze durante l'aggiornamento del software ONTAP su una configurazione MetroCluster a otto o quattro nodi

Il processo di aggiornamento del software MetroCluster varia a seconda che vi siano otto o quattro nodi nella configurazione MetroCluster.

Una configurazione MetroCluster è costituita da uno o due gruppi DR. Ciascun gruppo di DR è costituito da due coppie ha, una coppia ha per ogni cluster MetroCluster. Un MetroCluster a otto nodi include due gruppi di DR:



Si aggiorna un gruppo DR alla volta.

### Per configurazioni MetroCluster a quattro nodi:

1. Aggiornamento DR Gruppo 1:
  - a. Aggiornare node\_A\_1 e node\_B\_1.
  - b. Aggiornare node\_A\_2 e node\_B\_2.

**Per le configurazioni MetroCluster a otto nodi, eseguire due volte la procedura di aggiornamento del gruppo di disaster recovery:**

1. Aggiornamento DR Gruppo 1:
  - a. Aggiornare node\_A\_1 e node\_B\_1.
  - b. Aggiornare node\_A\_2 e node\_B\_2.
2. Aggiornamento del gruppo DR 2:

- a. Aggiornare node\_A\_3 e node\_B\_3.
- b. Aggiornare node\_A\_4 e node\_B\_4.

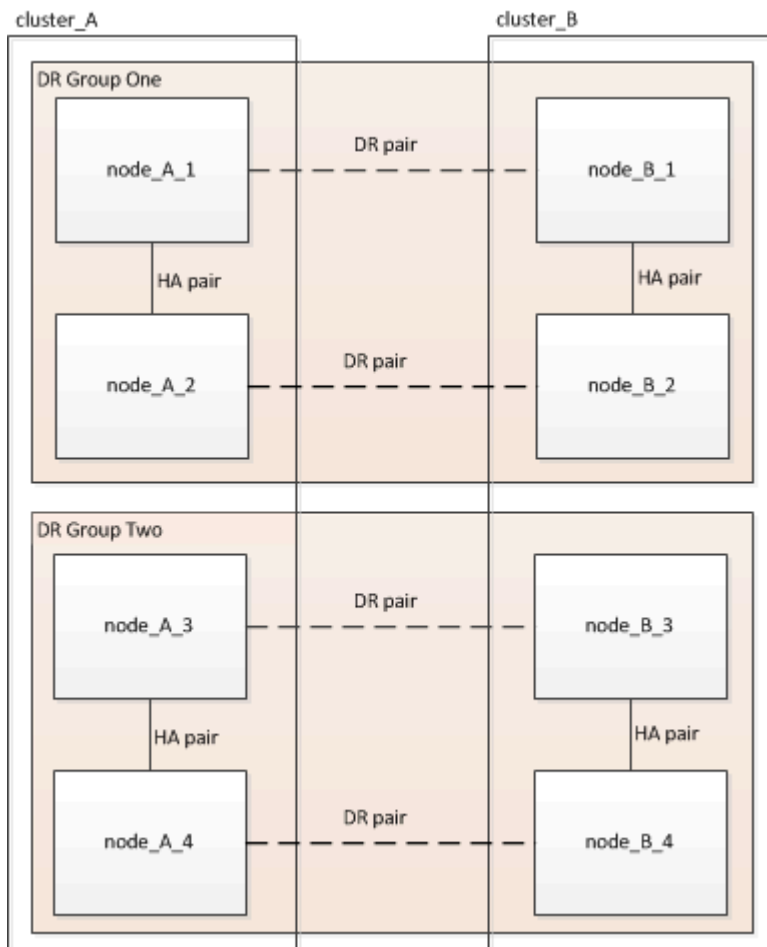
### Preparazione dell'aggiornamento di un gruppo DR MetroCluster

Prima di aggiornare il software ONTAP sui nodi, è necessario identificare le relazioni di DR tra i nodi, inviare un messaggio AutoSupport che si sta avviando un aggiornamento e confermare la versione di ONTAP in esecuzione su ogni nodo.

Devi avere "scaricato" e "installato" le immagini del software.

Questa attività deve essere ripetuta su ciascun gruppo di DR. Se la configurazione MetroCluster è composta da otto nodi, sono presenti due gruppi di DR. Pertanto, questa attività deve essere ripetuta su ciascun gruppo di DR.

Gli esempi forniti in questa attività utilizzano i nomi mostrati nell'illustrazione seguente per identificare i cluster e i nodi:



1. Identificare le coppie di DR nella configurazione:

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
(metrocluster node show)
dr-group-id cluster      node      dr-partner
-----
1           cluster_A    node_A_1  node_B_1
1           cluster_A    node_A_2  node_B_2
1           cluster_B    node_B_1  node_A_1
1           cluster_B    node_B_2  node_A_2
4 entries were displayed.

cluster_A::>
```

2. Impostare il livello di privilegio da admin a Advanced, immettendo **y** quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato (\*>).

3. Confermare la versione ONTAP su cluster\_A:

```
system image show
```

```
cluster_A::*> system image show
Node      Image      Is      Is      Version  Install
-----  -
node_A_1
  image1  true      true    X.X.X    MM/DD/YYYY TIME
  image2  false    false   Y.Y.Y    MM/DD/YYYY TIME
node_A_2
  image1  true      true    X.X.X    MM/DD/YYYY TIME
  image2  false    false   Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. Confermare la versione sul cluster\_B:

```
system image show
```

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_B_1					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_B::>
```

##### 5. Attivare una notifica AutoSupport:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Questa notifica AutoSupport include un record dello stato del sistema prima dell'aggiornamento. Salva informazioni utili sulla risoluzione dei problemi in caso di problemi con il processo di aggiornamento.

Se il cluster non è configurato per l'invio di messaggi AutoSupport, una copia della notifica viene salvata localmente.

##### 6. Per ciascun nodo del primo set, impostare l'immagine software ONTAP di destinazione come immagine predefinita:

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

Questo comando utilizza una query estesa per modificare l'immagine software di destinazione, installata come immagine alternativa, come immagine predefinita per il nodo.

##### 7. Verificare che l'immagine software ONTAP di destinazione sia impostata come immagine predefinita su cluster\_A:

```
system image show
```

Nell'esempio seguente, image2 è la nuova versione di ONTAP ed è impostata come immagine predefinita su ciascuno dei nodi del primo set:

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_A_1	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node_A_2	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

2 entries were displayed.

- a. Verificare che l'immagine software ONTAP di destinazione sia impostata come immagine predefinita su cluster\_B:

```
system image show
```

L'esempio seguente mostra che la versione di destinazione è impostata come immagine predefinita su ciascuno dei nodi del primo set:

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_A_1	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/YY/YYYY TIME
node_A_2	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

2 entries were displayed.

8. Determinare se i nodi da aggiornare attualmente servono client due volte per ciascun nodo:

```
system node run -node target-node -command uptime
```

Il comando uptime visualizza il numero totale di operazioni eseguite dal nodo per client NFS, CIFS, FC e iSCSI dall'ultimo avvio del nodo. Per ciascun protocollo, è necessario eseguire il comando due volte per determinare se i conteggi delle operazioni sono in aumento. Se sono in aumento, il nodo sta attualmente servendo i client per quel protocollo. Se non sono in aumento, il nodo non sta attualmente servendo client per quel protocollo.





È necessario prendere nota di ciascun protocollo che ha un aumento delle operazioni client in modo che, dopo l'aggiornamento del nodo, sia possibile verificare che il traffico client sia ripreso.

Questo esempio mostra un nodo con operazioni NFS, CIFS, FC e iSCSI. Tuttavia, il nodo attualmente serve solo client NFS e iSCSI.

```
cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

### Aggiornamento della prima coppia di DR in un gruppo di DR MetroCluster

È necessario eseguire un takeover e un giveback dei nodi nell'ordine corretto per fare in modo che la nuova versione di ONTAP sia la versione corrente del nodo.

Tutti i nodi devono eseguire la vecchia versione di ONTAP.

In questa attività, Node\_A\_1 e Node\_B\_1 vengono aggiornati.

Se il software ONTAP è stato aggiornato sul primo gruppo DR e ora si sta aggiornando il secondo gruppo DR in una configurazione MetroCluster A otto nodi, in questa attività si aggiornerà Node\_A\_3 e Node\_B\_3.

1. Se il software MetroCluster Tiebreaker è attivato, lo disattiva.
2. Per ciascun nodo della coppia ha, disattivare il giveback automatico:

```
storage failover modify -node target-node -auto-giveback false
```

Questo comando deve essere ripetuto per ogni nodo della coppia ha.

3. Verificare che il giveback automatico sia disattivato:

```
storage failover show -fields auto-giveback
```

Questo esempio mostra che il giveback automatico è stato disattivato su entrambi i nodi:

```
cluster_x::> storage failover show -fields auto-giveback
node      auto-giveback
-----
node_x_1  false
node_x_2  false
2 entries were displayed.
```

4. Assicurarsi che l'i/o non superi il ~50% per ogni controller e che l'utilizzo della CPU non superi il ~50% per controller.
5. Avviare un Takeover del nodo di destinazione su cluster\_A:

Non specificare il parametro `-option immediate`, perché è necessario un normale Takeover per i nodi che vengono presi in consegna per avviare la nuova immagine software.

- a. Assumere il controllo del partner DR su cluster\_A (Node\_A\_1):

```
storage failover takeover -ofnode node_A_1
```

Il nodo si avvia allo stato "Waiting for giveback" (in attesa di giveback).



Se AutoSupport è attivato, viene inviato un messaggio AutoSupport che indica che i nodi sono fuori dal quorum del cluster. È possibile ignorare questa notifica e procedere con l'aggiornamento.

- b. Verificare che l'acquisizione sia riuscita:

```
storage failover show
```

L'esempio seguente mostra che il rilevamento è riuscito. Node\_A\_1 si trova nello stato "Waiting for giveback" e Node\_A\_2 si trova nello stato "in Takeover".

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node_A_1	node_A_2	-	Waiting for giveback (HA mailboxes)
node_A_2	node_A_1	false	In takeover

2 entries were displayed.

6. Assumere il controllo del partner DR su cluster\_B (Node\_B\_1):

Non specificare il parametro `-option immediate`, perché è necessario un normale Takeover per i nodi che

vengono presi in consegna per avviare la nuova immagine software.

- a. Prendere il controllo del nodo\_B\_1:

```
storage failover takeover -ofnode node_B_1
```

Il nodo si avvia allo stato "Waiting for giveback" (in attesa di giveback).



Se AutoSupport è attivato, viene inviato un messaggio AutoSupport che indica che i nodi sono fuori dal quorum del cluster. È possibile ignorare questa notifica e procedere con l'aggiornamento.

- b. Verificare che l'acquisizione sia riuscita:

```
storage failover show
```

L'esempio seguente mostra che il rilevamento è riuscito. Node\_B\_1 è nello stato "Waiting for giveback" e Node\_B\_2 è nello stato "in Takeover".

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node_B_1	node_B_2	-	Waiting for giveback (HA mailboxes)
node_B_2	node_B_1	false	In takeover

2 entries were displayed.

7. Attendere almeno otto minuti per verificare le seguenti condizioni:

- Il multipathing client (se implementato) è stabilizzato.
- I client vengono ripristinati dalla pausa in i/o che si verifica durante il takeover.

Il tempo di ripristino è specifico del client e potrebbe richiedere più di otto minuti a seconda delle caratteristiche delle applicazioni client.

8. Restituire gli aggregati ai nodi di destinazione:

Dopo l'aggiornamento delle configurazioni MetroCluster IP a ONTAP 9.5 o versioni successive, gli aggregati si trovano in uno stato degradato per un breve periodo prima di risincronizzare e tornare a uno stato mirrorato.

- a. Restituire gli aggregati al partner DR su cluster\_A:

```
storage failover giveback -ofnode node_A_1
```

b. Restituire gli aggregati al partner DR su cluster\_B:

```
storage failover giveback -ofnode node_B_1
```

L'operazione di giveback restituisce prima l'aggregato root al nodo, quindi, al termine dell'avvio del nodo, restituisce gli aggregati non root.

9. Verificare che tutti gli aggregati siano stati restituiti eseguendo il seguente comando su entrambi i cluster:

```
storage failover show-giveback
```

Se il campo Stato giveback indica che non ci sono aggregati da restituire, tutti gli aggregati sono stati restituiti. Se il giveback viene veto, il comando visualizza l'avanzamento del giveback e il sottosistema che ha veto il giveback.

10. Se non sono stati restituiti aggregati, procedere come segue:

- a. Esaminare la soluzione alternativa al veto per determinare se si desidera risolvere la condizione “veto” o ignorare il veto.
- b. Se necessario, risolvere la condizione “veto” descritta nel messaggio di errore, assicurandosi che tutte le operazioni identificate vengano terminate correttamente.
- c. Immettere nuovamente il comando giveback per il failover dello storage.

Se si decide di eseguire l'override della condizione “veto”, impostare il parametro -override-vetoes su true.

11. Attendere almeno otto minuti per verificare le seguenti condizioni:

- Il multipathing client (se implementato) è stabilizzato.
- I client vengono ripristinati dalla pausa in i/o che si verifica durante il giveback.

Il tempo di ripristino è specifico del client e potrebbe richiedere più di otto minuti a seconda delle caratteristiche delle applicazioni client.

12. Impostare il livello di privilegio da admin a Advanced, immettendo **y** quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato (\*>).

13. Confermare la versione sul cluster\_A:

```
system image show
```

L'esempio seguente mostra che l'immagine di sistema 2 deve essere la versione predefinita e corrente su Node\_A\_1:

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_A_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_A_2					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

#### 14. Confermare la versione sul cluster\_B:

```
system image show
```

L'esempio seguente mostra che l'immagine di sistema 2 (ONTAP 9.0.0) è la versione predefinita e corrente sul nodo\_A\_1:

```
cluster_A::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_B_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

### Aggiornamento della seconda coppia di DR in un gruppo di DR MetroCluster

È necessario eseguire un takeover e un giveback del nodo nell'ordine corretto per fare in modo che la nuova versione di ONTAP sia la versione corrente del nodo.

La prima coppia DR deve essere stata aggiornata (Node\_A\_1 e Node\_B\_1).

In questa attività, Node\_A\_2 e Node\_B\_2 vengono aggiornati.

Se il software ONTAP è stato aggiornato sul primo gruppo DR e ora si sta aggiornando il secondo gruppo DR

in una configurazione MetroCluster A otto nodi, in questa attività si stanno aggiornando node\_A\_4 e node\_B\_4.

1. Eseguire la migrazione di tutti i file LIF dei dati lontano dal nodo:

```
network interface migrate-all -node nodenameA
```

2. Avviare un Takeover del nodo di destinazione su cluster\_A:

Non specificare il parametro `-option immediate`, perché è necessario un normale Takeover per i nodi che vengono presi in consegna per avviare la nuova immagine software.

- a. Assumere il controllo del partner DR su cluster\_A:

```
storage failover takeover -ofnode node_A_2 -option allow-version-mismatch
```



Il `allow-version-mismatch` L'opzione non è richiesta per gli aggiornamenti da ONTAP 9.0 a ONTAP 9.1 o per gli aggiornamenti delle patch.

Il nodo si avvia allo stato "Waiting for giveback" (in attesa di giveback).

Se AutoSupport è attivato, viene inviato un messaggio AutoSupport che indica che i nodi sono fuori dal quorum del cluster. È possibile ignorare questa notifica e procedere con l'aggiornamento.

- b. Verificare che l'acquisizione sia riuscita:

```
storage failover show
```

L'esempio seguente mostra che il rilevamento è riuscito. Node\_A\_2 è nello stato "Waiting for giveback" e Node\_A\_1 è nello stato "in Takeover".

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node_A_1	node_A_2	false	In takeover
node_A_2	node_A_1	-	Waiting for giveback (HA mailboxes)

2 entries were displayed.

3. Avviare un Takeover del nodo di destinazione su cluster\_B:

Non specificare il parametro `-option immediate`, perché è necessario un normale Takeover per i nodi che vengono presi in consegna per avviare la nuova immagine software.

a. Assumere il controllo del partner DR su cluster\_B (Node\_B\_2):

Se si sta eseguendo l'aggiornamento da...	Immettere questo comando...
ONTAP 9.2 o ONTAP 9.1	<pre>storage failover takeover -ofnode node_B_2</pre>
ONTAP 9.0 o Data ONTAP 8.3.x	<pre>storage failover takeover -ofnode node_B_2 -option allow- version-mismatch</pre> <div>  <p>Il <code>allow-version-mismatch</code> L'opzione non è richiesta per gli aggiornamenti da ONTAP 9.0 a ONTAP 9.1 o per gli aggiornamenti delle patch.</p> </div>

Il nodo si avvia allo stato "Waiting for giveback" (in attesa di giveback).



Se AutoSupport è attivato, viene inviato un messaggio AutoSupport che indica che i nodi non sono al di fuori del quorum del cluster. È possibile ignorare questa notifica e procedere con l'aggiornamento.

b. Verificare che l'acquisizione sia riuscita:

```
storage failover show
```

L'esempio seguente mostra che il rilevamento è riuscito. Node\_B\_2 è nello stato "Waiting for giveback" e Node\_B\_1 è nello stato "in Takeover".

```
cluster1::> storage failover show
```

Node	Partner	Takeover Possible	State Description
node_B_1	node_B_2	false	In takeover
node_B_2	node_B_1	-	Waiting for giveback (HA mailboxes)

2 entries were displayed.

4. Attendere almeno otto minuti per verificare le seguenti condizioni:

- Il multipathing client (se implementato) è stabilizzato.

- I client vengono ripristinati dalla pausa in i/o che si verifica durante il takeover.

Il tempo di ripristino è specifico del client e potrebbe richiedere più di otto minuti a seconda delle caratteristiche delle applicazioni client.

5. Restituire gli aggregati ai nodi di destinazione:

Dopo l'aggiornamento delle configurazioni MetroCluster IP a ONTAP 9.5, gli aggregati si trovano in uno stato degradato per un breve periodo prima della risincronizzazione e del ritorno a uno stato mirrorato.

a. Restituire gli aggregati al partner DR su cluster\_A:

```
storage failover giveback -ofnode node_A_2
```

b. Restituire gli aggregati al partner DR su cluster\_B:

```
storage failover giveback -ofnode node_B_2
```

L'operazione di giveback restituisce prima l'aggregato root al nodo, quindi, al termine dell'avvio del nodo, restituisce gli aggregati non root.

6. Verificare che tutti gli aggregati siano stati restituiti eseguendo il seguente comando su entrambi i cluster:

```
storage failover show-giveback
```

Se il campo Stato giveback indica che non ci sono aggregati da restituire, tutti gli aggregati sono stati restituiti. Se il giveback viene veto, il comando visualizza l'avanzamento del giveback e il sottosistema che ha veto il giveback.

7. Se non sono stati restituiti aggregati, procedere come segue:

- Esaminare la soluzione alternativa al veto per determinare se si desidera risolvere la condizione "veto" o ignorare il veto.
- Se necessario, risolvere la condizione "veto" descritta nel messaggio di errore, assicurandosi che tutte le operazioni identificate vengano terminate correttamente.
- Immettere nuovamente il comando giveback per il failover dello storage.

Se si decide di eseguire l'override della condizione "veto", impostare il parametro `-override-vetoes` su `true`.

8. Attendere almeno otto minuti per verificare le seguenti condizioni:

- Il multipathing client (se implementato) è stabilizzato.
- I client vengono ripristinati dalla pausa in i/o che si verifica durante il giveback.

Il tempo di ripristino è specifico del client e potrebbe richiedere più di otto minuti a seconda delle caratteristiche delle applicazioni client.

9. Impostare il livello di privilegio da admin a Advanced, immettendo **y** quando viene richiesto di continuare:



```
set -privilege advanced
```

Il prompt avanzato (\*>).

10. Confermare la versione sul cluster\_A:

```
system image show
```

L'esempio seguente mostra che l'immagine di sistema 2 (immagine ONTAP di destinazione) è la versione predefinita e corrente sul nodo\_A\_2:

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node_A_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_A_2					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

11. Confermare la versione sul cluster\_B:

```
system image show
```

L'esempio seguente mostra che l'immagine di sistema 2 (immagine ONTAP di destinazione) è la versione predefinita e corrente sul nodo\_B\_2:

```
cluster_B::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_B_1					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME
node_B_2					
	image1	false	false	X.X.X	MM/DD/YYYY TIME
	image2	true	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

```
cluster_A::>
```

12. Per ciascun nodo della coppia ha, attivare il giveback automatico:

```
storage failover modify -node target-node -auto-giveback true
```

Questo comando deve essere ripetuto per ogni nodo della coppia ha.

13. Verificare che il giveback automatico sia attivato:

```
storage failover show -fields auto-giveback
```

Questo esempio mostra che il giveback automatico è stato attivato su entrambi i nodi:

```
cluster_x::> storage failover show -fields auto-giveback
```

node	auto-giveback
-----	
node_x_1	true
node_x_2	true

2 entries were displayed.

#### Upgrade senza interruzioni di una configurazione MetroCluster a due nodi in ONTAP 9,2 o versione precedente

Le modalità di aggiornamento di una configurazione MetroCluster a due nodi variano a seconda della versione di ONTAP utilizzata. Se si utilizza ONTAP 9,2 o versioni precedenti, utilizzare questa procedura per eseguire un aggiornamento manuale senza interruzioni che include l'avvio di uno switchover negoziato, l'aggiornamento del cluster nel sito "failed", l'avvio dello switchback e la ripetizione del processo sul cluster nell'altro sito.

Se si possiede una configurazione MetroCluster a due nodi che esegue ONTAP 9,3 o versione successiva,

eseguire una [Upgrade automatico con System Manager](#).

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato), immettendo **y** quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato (\*>).

2. Sul cluster da aggiornare, installare la nuova immagine del software ONTAP come predefinita:

```
system node image update -package package_location -setdefault true  
-replace-package true
```

```
cluster_B::*> system node image update -package  
http://www.example.com/NewImage.tgz -setdefault true -replace-package  
true
```

3. Verificare che l'immagine software di destinazione sia impostata come immagine predefinita:

```
system node image show
```

L'esempio seguente mostra questo NewImage viene impostato come immagine predefinita:

```
cluster_B::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node_B_1					
	OldImage	false	true	X.X.X	MM/DD/YYYY TIME
	NewImage	true	false	Y.Y.Y	MM/DD/YYYY TIME

2 entries were displayed.

4. Se l'immagine software di destinazione non è impostata come immagine predefinita, modificarla:

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. Verificare che tutte le SVM del cluster si trovino in uno stato di integrità:

```
metrocluster vservers show
```

6. Sul cluster che non viene aggiornato, avviare uno switchover negoziato:

```
metrocluster switchover
```

L'operazione può richiedere alcuni minuti. È possibile utilizzare il comando MetroCluster Operation show per verificare che lo switchover sia stato completato.

Nell'esempio seguente, viene eseguito uno switchover negoziato sul cluster remoto ("cluster\_A"). In questo modo, il cluster locale ("cluster\_B") si arresta in modo da poterlo aggiornare.

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
      Vservers on cluster "cluster_B" and
      automatically re-start them on cluster
      "cluster_A". It will finally gracefully shutdown
      cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. Verificare che tutte le SVM del cluster si trovino in uno stato di integrità:

```
metrocluster vservers show
```

8. Risincronizzare gli aggregati di dati nel cluster "surviving":

```
metrocluster heal -phase aggregates
```

Dopo l'aggiornamento delle configurazioni MetroCluster IP a ONTAP 9.5 o versioni successive, gli aggregati si trovano in uno stato degradato per un breve periodo prima di risincronizzare e tornare a uno stato mirrorato.

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. Verificare che l'operazione di riparazione sia stata completata correttamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. Risincronizzare gli aggregati root sul cluster “surving”:

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. Verificare che l’operazione di riparazione sia stata completata correttamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. Sul cluster arrestato, avviare il nodo dal prompt DEL CARICATORE:

```
boot_ontap
```

13. Attendere il completamento del processo di avvio, quindi verificare che tutte le SVM del cluster si trovino in uno stato di integrità:

```
metrocluster vserver show
```

14. Eseguire uno switchback dal cluster “surving”:

```
metrocluster switchback
```

15. Verificare che lo switchback sia stato completato correttamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Verificare che tutte le SVM del cluster si trovino in uno stato di integrità:

```
metrocluster vserver show
```

17. Ripetere tutti i passaggi precedenti sull'altro cluster.

18. Verificare che la configurazione di MetroCluster sia corretta:

a. Controllare la configurazione:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component          Result
-----
nodes              ok
lifs               ok
config-replication ok
aggregates         ok
4 entries were displayed.
```

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

b. Per visualizzare risultati più dettagliati, utilizzare il comando MetroCluster check run:

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

c. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

d. Simulare l'operazione di switchover:

```
metrocluster switchover -simulate
```

e. Esaminare i risultati della simulazione dello switchover:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
  Operation: switchover
    State: successful
  Start time: MM/DD/YYYY TIME
    End time: MM/DD/YYYY TIME
    Errors: -
```

f. Tornare al livello di privilegio admin:

```
set -privilege admin
```

g. Ripetere questi passaggi secondari sull'altro cluster.

#### Al termine

Eseguire qualsiasi ["attività successive all'aggiornamento"](#).

#### Informazioni correlate

### Aggiornamento ONTAP con interruzione manuale dell'attività tramite la CLI

Se è possibile portare il cluster offline per eseguire l'aggiornamento a una nuova release di ONTAP, è possibile utilizzare il metodo di aggiornamento disruptive. Questo metodo prevede diversi passaggi: Disattivazione del failover dello storage per ciascuna coppia ha, riavvio di ciascun nodo del cluster e riabilitazione del failover dello storage.

- È necessario "scarica" e "installare" immagine del software.
- Se si opera in un ambiente SAN, tutti i client SAN devono essere spenti o sospesi fino al completamento dell'aggiornamento.

Se i client SAN non vengono arrestati o sospesi prima di un aggiornamento interrotto, i file system e le applicazioni client subiscono errori che potrebbero richiedere il ripristino manuale dopo il completamento dell'aggiornamento.

In un aggiornamento disgregativo, è necessario il downtime perché il failover dello storage è disattivato per ogni coppia ha e ogni nodo viene aggiornato. Quando il failover dello storage viene disattivato, ciascun nodo si comporta come un cluster a nodo singolo, ovvero i servizi di sistema associati al nodo vengono interrotti per tutto il tempo necessario al riavvio del sistema.

### Fasi

1. Impostare il livello di privilegio da admin a Advanced, immettendo **y** quando viene richiesto di continuare:

```
set -privilege advanced
```

Il prompt avanzato (\*>).

2. Impostare la nuova immagine del software ONTAP come immagine predefinita:

```
system image modify {-node * -iscurrent false} -isdefault true
```

Questo comando utilizza una query estesa per modificare l'immagine del software ONTAP di destinazione (che viene installata come immagine alternativa) come immagine predefinita per ciascun nodo.

3. Verificare che la nuova immagine del software ONTAP sia impostata come immagine predefinita:

```
system image show
```

Nell'esempio seguente, l'immagine 2 è la nuova versione di ONTAP e viene impostata come immagine predefinita su entrambi i nodi:



```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
-----					
node0					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	false	true	X.X.X	MM/DD/YYYY TIME
	image2	true	false	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

4. Eseguire una delle seguenti operazioni:

Se il cluster è costituito da...	Eseguire questa operazione...
Un nodo	Passare alla fase successiva.
Due nodi	<p>a. Disattivare la disponibilità elevata del cluster:</p> <pre>cluster ha modify -configured false</pre> <p>Invio y per continuare quando richiesto.</p> <p>b. Disattivare il failover dello storage per la coppia ha:</p> <pre>storage failover modify -node * -enabled false</pre>
Più di due nodi	<p>Disattivare il failover dello storage per ogni coppia ha nel cluster:</p> <pre>storage failover modify -node * -enabled false</pre>

5. Riavviare un nodo nel cluster:

```
system node reboot -node nodename -ignore-quorum-warnings
```



Non riavviare più di un nodo alla volta.

Il nodo avvia la nuova immagine ONTAP. Viene visualizzato il prompt di accesso di ONTAP, che indica che il processo di riavvio è stato completato.

6. Una volta riavviato il nodo o l'insieme di nodi con la nuova immagine ONTAP, impostare il livello di privilegio su Advanced:

```
set -privilege advanced
```

Inserire **y** quando viene richiesto di continuare

7. Verificare che il nuovo software sia in esecuzione:

```
system node image show
```

Nell'esempio seguente, image1 è la nuova versione di ONTAP ed è impostata come la versione corrente su node0:

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node1	image1	true	false	X.X.X	MM/DD/YYYY TIME
	image2	false	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

8. Verificare che l'aggiornamento sia stato completato correttamente:

- a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- b. Verificare che lo stato dell'aggiornamento sia completo per ciascun nodo:

```
system node upgrade-revert show -node nodename
```

Lo stato deve essere indicato come completo.

Se lo stato non è completo, ["Contatta il supporto NetApp"](#) immediatamente.

- a. Tornare al livello di privilegio admin:

```
set -privilege admin
```

9. Ripetere i passaggi da 2 a 8 per ogni nodo aggiuntivo.
10. Se il cluster è costituito da due o più nodi, abilitare il failover dello storage per ciascuna coppia ha nel cluster:

```
storage failover modify -node * -enabled true
```

11. Se il cluster è costituito da due soli nodi, abilitare la disponibilità elevata del cluster:

```
cluster ha modify -configured true
```

## Cosa fare dopo un aggiornamento di ONTAP

### Cosa fare dopo un aggiornamento di ONTAP

Dopo l'aggiornamento di ONTAP, è necessario eseguire diverse attività per verificare la disponibilità del cluster.

1. ["Verificare il cluster"](#).

Dopo l'upgrade di ONTAP, dovresti verificare la versione del cluster, la salute del cluster e la salute dello storage. Se si utilizza una configurazione MetroCluster FC, è inoltre necessario verificare che il cluster sia abilitato per lo switchover automatico non pianificato.

2. ["Verifica che tutte le LIF siano sulle porte home"](#).

Durante un riavvio, alcune LIF potrebbero essere state migrate alle porte di failover assegnate. Dopo l'aggiornamento di un cluster, è necessario abilitare e ripristinare le LIF che non si trovano sulle porte domestiche.

3. Verificare ["considerazioni particolari"](#) specifico per il tuo cluster.

Se nel cluster sono presenti determinate configurazioni, potrebbe essere necessario eseguire ulteriori passaggi dopo l'aggiornamento.

4. ["Aggiornamento del Disk Qualification Package \(DQP\)"](#).

Il DQP non viene aggiornato come parte di un aggiornamento del ONTAP.

### Verifica del cluster dopo l'aggiornamento di ONTAP

Dopo l'upgrade di ONTAP, verificare la versione del cluster, la salute del cluster e la salute dello storage. Per le configurazioni FC di MetroCluster, verifica anche che il cluster sia abilitato per uno switchover automatico e non pianificato.

## Verificare la versione del cluster

Una volta aggiornate tutte le coppie ha, è necessario utilizzare il comando `version` per verificare che tutti i nodi stiano eseguendo la release di destinazione.

La versione del cluster è la versione più bassa di ONTAP in esecuzione su qualsiasi nodo del cluster. Se la versione del cluster non è la release ONTAP di destinazione, è possibile aggiornare il cluster.

1. Verificare che la versione del cluster sia la release ONTAP di destinazione:

```
version
```

2. Se la versione del cluster non è la release ONTAP di destinazione, è necessario verificare lo stato di aggiornamento di tutti i nodi:

```
system node upgrade-revert show
```

## Verificare lo stato del cluster

Dopo aver aggiornato un cluster, è necessario verificare che i nodi siano integri e idonei a partecipare al cluster e che il cluster sia in quorum.

1. Verificare che i nodi del cluster siano online e idonei a partecipare al cluster:

```
cluster show
```

```
cluster1::> cluster show
Node                               Health  Eligibility
-----
node0                             true    true
node1                             true    true
```

Se un nodo non è integro o non è idoneo, controllare i registri EMS per verificare la presenza di errori e intraprendere un'azione correttiva.

2. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

3. Verificare i dettagli di configurazione per ciascun processo RDB.

- L'epoca del database relazionale e l'epoca del database devono corrispondere per ciascun nodo.
- Il master del quorum per squillo deve essere lo stesso per tutti i nodi.

Si noti che ogni squillo potrebbe avere un master di quorum diverso.

Per visualizzare questo processo RDB...	Immettere questo comando...
Applicazione di gestione	<code>cluster ring show -unitname mgmt</code>
Database di posizioni dei volumi	<code>cluster ring show -unitname vlodb</code>
Virtual-Interface Manager	<code>cluster ring show -unitname vifmgr</code>
Daemon di gestione SAN	<code>cluster ring show -unitname bcomd</code>

Questo esempio mostra il processo del database di localizzazione del volume:

```
cluster1::*> cluster ring show -unitname vlodb
```

Node	UnitName	Epoch	DB Epoch	DB Trnxs	Master	Online
node0	vlodb	154	154	14847	node0	master
node1	vlodb	154	154	14847	node0	secondary
node2	vlodb	154	154	14847	node0	secondary
node3	vlodb	154	154	14847	node0	secondary

4 entries were displayed.

4. Se si opera in un ambiente SAN, verificare che ciascun nodo si trovi in un quorum SAN:

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
```

Master	Cluster	Quorum	Availability
Operational			
Node	Node	Status	Status
cluster1-01	cluster1-01	in-quorum	true
operational	cluster1-02	in-quorum	true
operational			

2 entries were displayed.

## Informazioni correlate

["Amministrazione del sistema"](#)

### Verifica dell'abilitazione dello switchover non pianificato automatico (solo configurazioni MetroCluster FC)

Se il cluster si trova in una configurazione FC MetroCluster, devi verificare l'abilitazione dello switchover automatico non pianificato dopo l'upgrade del ONTAP.

Se si utilizza una configurazione IP MetroCluster, ignorare questa procedura.

#### Fasi

1. Controllare se è attivato lo switchover automatico non pianificato:

```
metrocluster show
```

Se è attivato lo switchover automatico non pianificato, nell'output del comando viene visualizzata la seguente istruzione:

```
AUSO Failure Domain  auso-on-cluster-disaster
```

2. Se l'istruzione non viene visualizzata, attivare uno switchover automatico non pianificato:

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster
```

3. Verificare che sia stato abilitato uno switchover non pianificato automatico:

```
metrocluster show
```

#### Informazioni correlate

["Gestione di dischi e aggregati"](#)

### Dopo l'aggiornamento di ONTAP, verificare che tutti i file LIFS si trovino sulle porte home

Durante il riavvio che si verifica durante il processo di aggiornamento di ONTAP, è possibile che alcune LIF vengano migrate dalle porte home alle porte di failover assegnate. Dopo un aggiornamento, devi abilitare e ripristinare le LIF che non si trovano nelle porte home.

#### Fasi

1. Visualizzare lo stato di tutti i LIF:

```
network interface show -fields home-port,curr-port
```

Se **Status Admin** è "Down" o **is home** è "false" per qualsiasi LIF, passare alla fase successiva.

2. Abilitare le LIF dei dati:

```
network interface modify {-role data} -status-admin up
```

### 3. Ripristinare le LIF alle porte home:

```
network interface revert *
```

### 4. Verificare che tutte le LIF si trovino nelle porte home:

```
network interface show
```

Questo esempio mostra che tutte le LIF per SVM vs0 si trovano sulle porte home.

```
cluster1::> network interface show -vserver vs0
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0	data001	up/up	192.0.2.120/24	node0	e0e	true
	data002	up/up	192.0.2.121/24	node0	e0f	true
	data003	up/up	192.0.2.122/24	node0	e2a	true
	data004	up/up	192.0.2.123/24	node0	e2b	true
	data005	up/up	192.0.2.124/24	node1	e0e	true
	data006	up/up	192.0.2.125/24	node1	e0f	true
	data007	up/up	192.0.2.126/24	node1	e2a	true
	data008	up/up	192.0.2.127/24	node1	e2b	true

8 entries were displayed.

## Configurazioni speciali

### Considerazioni speciali dopo un aggiornamento di ONTAP

Se il cluster è configurato con una delle seguenti funzionalità, potrebbe essere necessario eseguire ulteriori passaggi dopo l'aggiornamento del software ONTAP.

Chiedetevi...	Se la risposta è sì, eseguire questa operazione...
È stato eseguito l'aggiornamento da ONTAP 9,7 o versione precedente a ONTAP 9,8 o versione successiva?	<a href="#">Verificare la configurazione di rete</a> <a href="#">Rimuovere il servizio LIF EMS dai criteri di servizio di rete che non forniscono informazioni sulla destinazione EMS</a>
Il mio cluster è in una configurazione MetroCluster?	<a href="#">Verificare lo stato dello storage e della rete</a>
Si dispone di una configurazione SAN?	<a href="#">Verificare la configurazione DELLA SAN</a>

Chiedetevi...	Se la risposta è sì, eseguire questa operazione...
È stato eseguito l'aggiornamento da ONTAP 9,3 o versione precedente e si utilizza la crittografia dello storage NetApp?	<a href="#">Riconfigurare le connessioni del server KMIP</a>
Sono presenti mirror di condivisione del carico?	<a href="#">Spostare i volumi di origine mirrorati per la condivisione del carico</a>
Si dispone di account utente per l'accesso al Service Processor (SP) creati prima di ONTAP 9,9.1?	<a href="#">Verificare la modifica degli account che possono accedere al Service Processor</a>

**Verificare la configurazione di rete in seguito a un aggiornamento ONTAP da ONTAP 9,7x o versione precedente**

Dopo aver eseguito l'aggiornamento da ONTAP 9,7x o versione precedente a ONTAP 9,8 o versione successiva, è necessario verificare la configurazione di rete. Dopo l'aggiornamento, ONTAP monitora automaticamente la raggiungibilità di livello 2.

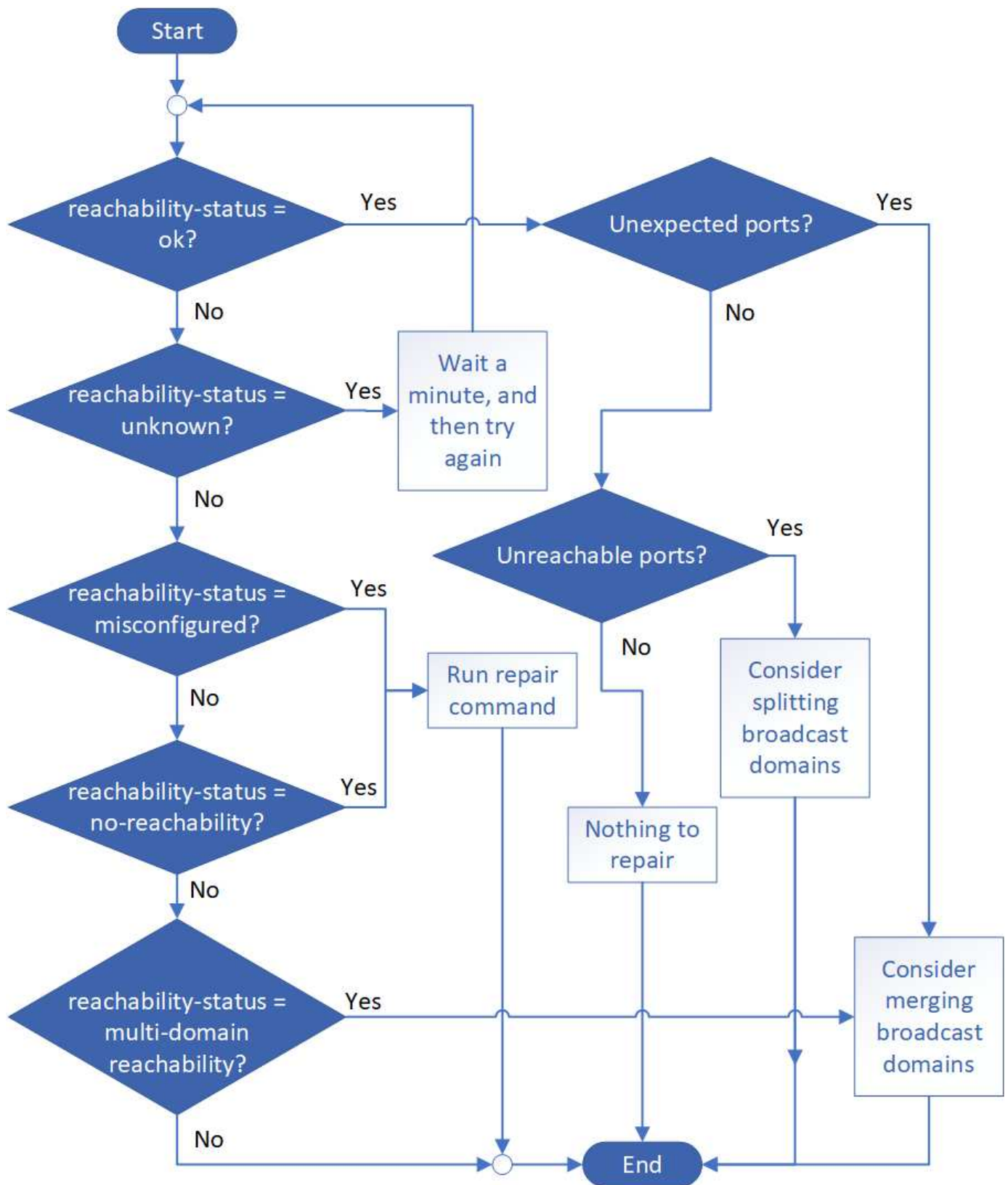
#### Fase

1. Verificare che ogni porta sia raggiungibile dal proprio dominio di trasmissione previsto:

```
network port reachability show -detail
```

L'output del comando contiene i risultati di raggiungibilità. Utilizzare il seguente albero decisionale e la seguente tabella per comprendere i risultati di raggiungibilità (stato di raggiungibilità) e determinare cosa, se necessario, fare in seguito.





stato di raggiungibilità	Descrizione
--------------------------	-------------

ok	<p>La porta ha una capacità di livello 2 rispetto al dominio di trasmissione assegnato.</p> <p>Se lo stato di raggiungibilità è "ok", ma ci sono "porte impreviste", considerare la possibilità di unire uno o più domini di broadcast. Per ulteriori informazioni, vedere <a href="#">"Unire i domini di broadcast"</a>.</p> <p>Se lo stato di raggiungibilità è "ok", ma ci sono "porte irraggiungibili", considerare la possibilità di suddividere uno o più domini di broadcast. Per ulteriori informazioni, vedere <a href="#">"Suddividere i domini di broadcast"</a>.</p> <p>Se lo stato di raggiungibilità è "ok" e non ci sono porte impreviste o irraggiungibili, la configurazione è corretta.</p>
riconfigurazione non corretta	<p>La porta non dispone di capacità di livello 2 rispetto al dominio di trasmissione assegnato; tuttavia, la porta dispone di capacità di livello 2 rispetto a un dominio di trasmissione diverso.</p> <p>È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta al dominio di trasmissione a cui è possibile accedere:</p> <pre>network port reachability repair -node -port</pre> <p>Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
nessuna raggiungibilità	<p>La porta non dispone di capacità di livello 2 per nessun dominio di trasmissione esistente.</p> <p>È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta a un nuovo dominio di trasmissione creato automaticamente in IPspace predefinito:</p> <pre>network port reachability repair -node -port</pre> <p>Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
raggiungibilità multi-dominio	<p>La porta ha una raggiungibilità di livello 2 per il dominio di broadcast assegnato; tuttavia, ha anche una raggiungibilità di livello 2 per almeno un altro dominio di broadcast.</p> <p>Esaminare la connettività fisica e la configurazione dello switch per determinare se non è corretta o se il dominio di trasmissione assegnato alla porta deve essere Unito a uno o più domini di trasmissione.</p> <p>Per ulteriori informazioni, vedere <a href="#">"Unire i domini di broadcast"</a> oppure <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
sconosciuto	<p>Se lo stato di raggiungibilità è "sconosciuto", attendere alcuni minuti e provare a eseguire nuovamente il comando.</p>

Dopo aver riparato una porta, è necessario controllare e risolvere le LIF e le VLAN spostate. Se la porta faceva parte di un gruppo di interfacce, è necessario comprendere anche cosa è successo a quel gruppo di

interfacce. Per ulteriori informazioni, vedere ["Riparare la raggiungibilità delle porte"](#).

#### Rimuovere il servizio LIF EMS dalle policy di servizio di rete

Se i messaggi del sistema di gestione degli eventi (EMS) sono stati impostati prima dell'aggiornamento da ONTAP 9.7 o versioni precedenti a ONTAP 9.8 o versioni successive, dopo l'aggiornamento, i messaggi EMS potrebbero non essere recapitati.

Durante l'aggiornamento, Management-ems, che è il servizio LIF EMS, viene aggiunto a tutte le policy di servizio esistenti. In questo modo, è possibile inviare messaggi EMS da una qualsiasi delle LIF associate a una qualsiasi delle policy di servizio. Se il LIF selezionato non è accessibile alla destinazione di notifica degli eventi, il messaggio non viene recapitato.

Per evitare questo problema, dopo l'aggiornamento, è necessario rimuovere il servizio LIF EMS dai criteri di servizio di rete che non forniscono la raggiungibilità alla destinazione.

#### Fasi

1. Identificare i LIF e i criteri di servizio di rete associati attraverso i quali è possibile inviare i messaggi EMS:

```
network interface show -fields service-policy -services management-ems
```

vserver	lif	service-policy
cluster-1	cluster_mgmt	default-management
cluster-1	node1-mgmt	default-management
cluster-1	node2-mgmt	default-management
cluster-1	inter_cluster	default-intercluster

4 entries were displayed.

2. Controllare ogni LIF per la connettività alla destinazione EMS:

```
network ping -lif lif_name -vserver svm_name -destination  
destination_address
```

Eseguire questa operazione su ciascun nodo.

## Esempi

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. Immettere il livello di privilegio avanzato:

```
set advanced
```

4. Per le LIF che non dispongono di raggiungibilità, rimuovere il servizio LIF ems di gestione dai criteri di servizio corrispondenti:

```
network interface service-policy remove-service -vserver svm_name
-policy service_policy_name -service management-ems
```

5. Verificare che la LIF ems di gestione sia ora associata solo alle LIF che forniscono la raggiungibilità alla destinazione EMS:

```
network interface show -fields service-policy -services management-ems
```

## Link correlati

["LIF e policy di servizio in ONTAP 9.6 e versioni successive"](#)

**Verificare lo stato della rete e dello storage per le configurazioni MetroCluster dopo un aggiornamento di ONTAP**

Dopo l'upgrade di un cluster ONTAP in una configurazione MetroCluster, occorre verificare lo stato di LIF, aggregati e volumi per ogni cluster.

1. Verifica dello stato della LIF:

```
network interface show
```

Durante il normale funzionamento, le LIF per le SVM di origine devono avere uno stato di amministrazione up e trovarsi sui nodi home. Non è necessario che le LIF per le SVM di destinazione siano attive o localizzate sui propri nodi domestici. Nello switchover, tutte le LIF hanno uno stato di amministrazione su, ma non devono essere collocate nei propri nodi domestici.

```

cluster1::> network interface show

```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
Cluster					
	cluster1-a1_clus1	up/up	192.0.2.1/24	cluster1-01	e2a
true					
	cluster1-a1_clus2	up/up	192.0.2.2/24	cluster1-01	e2b
true					
cluster1-01					
	clus_mgmt	up/up	198.51.100.1/24	cluster1-01	e3a
true					
	cluster1-a1_inet4_intercluster1	up/up	198.51.100.2/24	cluster1-01	e3c
true					
	...				

27 entries were displayed.

## 2. Verificare lo stato degli aggregati:

```
storage aggregate show -state !online
```

Questo comando visualizza tutti gli aggregati *non* online. Durante il normale funzionamento, tutti gli aggregati situati nel sito locale devono essere online. Tuttavia, se la configurazione MetroCluster è in switchover, gli aggregati root del sito di disaster recovery possono essere offline.

Questo esempio mostra un cluster in funzionamento normale:

```

cluster1::> storage aggregate show -state !online
There are no entries matching your query.

```

Questo esempio mostra un cluster nello switchover, in cui gli aggregati root del sito di disaster recovery

sono offline:

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
-----
aggr0_b1
          0B          0B    0% offline    0 cluster2-01
raid_dp,
mirror
degraded
aggr0_b2
          0B          0B    0% offline    0 cluster2-02
raid_dp,
mirror
degraded
2 entries were displayed.
```

### 3. Verificare lo stato dei volumi:

```
volume show -state !online
```

Questo comando visualizza tutti i volumi *non* online.

Se la configurazione MetroCluster è in funzione normale (non è in stato di switchover), l'output dovrebbe mostrare tutti i volumi di proprietà delle SVM secondarie del cluster (quelli con il nome SVM aggiunto con "-mc").

Questi volumi vengono online solo in caso di switchover.

Questo esempio mostra un cluster in condizioni di funzionamento normale, in cui i volumi del sito di disaster recovery non sono online.

```
cluster1::> volume show -state !online
(volume show)
Vserver   Volume      Aggregate    State    Type    Size
Available Used%
-----
vs2-mc    vol1        aggr1_b1     -        RW      -
-         -
vs2-mc    root_vs2    aggr0_b1     -        RW      -
-         -
vs2-mc    vol2        aggr1_b1     -        RW      -
-         -
vs2-mc    vol3        aggr1_b1     -        RW      -
-         -
vs2-mc    vol4        aggr1_b1     -        RW      -
-         -
5 entries were displayed.
```

#### 4. Verificare che non vi siano volumi incoerenti:

```
volume show -is-inconsistent true
```

Consultare l'articolo della Knowledge base ["Volume che mostra WAFL incoerente"](#) su come affrontare i volumi incoerenti.

#### Verificare la configurazione SAN dopo un aggiornamento

In seguito a un aggiornamento di ONTAP, in un ambiente SAN, verificare che ogni iniziatore connesso a una LIF prima che l'aggiornamento sia stato riconnesso con successo alla LIF.

##### 1. Verificare che ciascun iniziatore sia connesso al LIF corretto.

È necessario confrontare l'elenco degli iniziatori con quello creato durante la preparazione dell'aggiornamento.

Per...	Inserisci...
ISCSI	<pre>iscsi initiator show -fields igroup,initiator-name,tpgroup</pre>

Per...	Inserisci...
FC	<pre>fcf initiator show -fields igroup,wwpn,lif</pre>

#### Riconfigurare le connessioni del server KMIP dopo un aggiornamento da ONTAP 9,2 o versioni precedenti

Dopo l'aggiornamento da ONTAP 9,2 o versione precedente a ONTAP 9,3 o versione successiva, devi riconfigurare qualsiasi connessione server KMIP (External Key Management).

#### Fasi

1. Configurare la connettività del gestore delle chiavi:

```
security key-manager setup
```

2. Aggiungere i server KMIP:

```
security key-manager add -address key_management_server_ip_address
```

3. Verificare che i server KMIP siano connessi:

```
security key-manager show -status
```

4. Eseguire una query sui server delle chiavi:

```
security key-manager query
```

5. Creare una nuova chiave di autenticazione e una nuova passphrase:

```
security key-manager create-key -prompt-for-key true
```

La passphrase deve contenere almeno 32 caratteri.

6. Eseguire una query sulla nuova chiave di autenticazione:

```
security key-manager query
```

7. Assegnare la nuova chiave di autenticazione ai dischi con crittografia automatica (SED):



```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```



Assicurarsi di utilizzare la nuova chiave di autenticazione della query.

8. Se necessario, assegnare una chiave FIPS ai SED:

```
storage encryption disk modify -disk disk_id -fips-key-id  
fips_authentication_key_id
```

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

#### **Spostamento dei volumi di origine del mirroring della condivisione del carico dopo un aggiornamento di ONTAP**

Dopo l'aggiornamento di ONTAP, devi spostare di nuovo i volumi di origine del mirror per la condivisione del carico nelle loro posizioni pre-aggiornamento.

##### **Fasi**

1. Identificare la posizione in cui si sta spostando il volume di origine mirror per la condivisione del carico utilizzando il record creato prima di spostare il volume di origine mirror per la condivisione del carico.
2. Riportare il volume di origine mirror per la condivisione del carico nella posizione originale:

```
volume move start
```

#### **Modifica degli account utente che possono accedere al Service Processor**

Se sono stati creati account utente in ONTAP 9,8 o versioni precedenti che possono accedere al Service Processor (SP) con un ruolo non amministratore e si esegue l'aggiornamento a ONTAP 9.9.1 o versioni successive, qualsiasi valore non amministratore in `-role` il parametro è stato modificato in `admin`.

Per ulteriori informazioni, vedere ["Account che possono accedere al SP"](#).

#### **Aggiornare il pacchetto di Disk Qualification**

Dopo aver aggiornato il software ONTAP, è necessario scaricare e installare il pacchetto di qualifica dei dischi ONTAP (DQP). Il DQP non viene aggiornato come parte di un aggiornamento del ONTAP.

Il DQP contiene i parametri appropriati per l'interazione ONTAP con tutte le unità appena qualificate. Se la versione del DQP in uso non contiene informazioni relative a un'unità appena qualificata, ONTAP non disporrà delle informazioni necessarie per configurare correttamente l'unità.

È consigliabile aggiornare il DQP ogni trimestre. È inoltre necessario aggiornare il DQP per i seguenti motivi:

- Quando Aggiungi un nuovo tipo di disco o una nuova dimensione a un nodo del cluster

Ad esempio, se si dispone già di dischi da 1 TB e si aggiungono dischi da 2 TB, è necessario verificare la disponibilità dell'aggiornamento DQP più recente.

- Ogni volta che si aggiorna il firmware del disco
- Ogni volta che sono disponibili firmware del disco o file DQP più recenti

#### Informazioni correlate

- ["Download NetApp: Pacchetto di qualificazione dei dischi"](#)
- ["Download NetApp: Firmware del disco"](#)

## Aggiornamenti del firmware e del sistema

### Panoramica degli aggiornamenti del firmware e del sistema

A seconda della versione di ONTAP in uso, è possibile attivare gli aggiornamenti automatici del firmware e del sistema.

Versione di ONTAP	Cosa include gli aggiornamenti automatici
9.13.1 e versioni successive	<ul style="list-style-type: none"><li>• Database del fuso orario di ONTAP</li><li>• Firmware di storage per dispositivi storage, dischi e shelf di dischi</li><li>• Firmware SP/BMC per service processor e moduli BMC</li></ul>
9.10.1 e versioni successive	<ul style="list-style-type: none"><li>• Firmware di storage per dispositivi storage, dischi e shelf di dischi</li><li>• Firmware SP/BMC per service processor e moduli BMC</li></ul>
9.9.1 e versioni precedenti	Non supportato

Se si utilizza ONTAP 9.9.1 o versione precedente o se non si dispone di ["aggiornamenti automatici del sistema"](#) abilitato, è possibile ["eseguire gli aggiornamenti del firmware manualmente"](#).

Se si utilizza ONTAP 9.12.1 o versione precedente o se non si dispone di ["aggiornamenti automatici del sistema"](#) Attivato, è possibile aggiornare manualmente il database del fuso orario. Consultare l'articolo della Knowledge base, ["Come aggiornare le informazioni sul fuso orario in ONTAP 9"](#), per ulteriori informazioni.

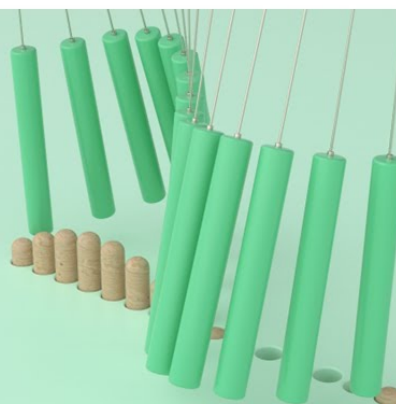
#### Video: Funzione di aggiornamento automatico del firmware

Dai un'occhiata alla funzione di aggiornamento automatico del firmware disponibile a partire da ONTAP 9.10.1.



## Automatic Firmware Update feature is available starting in ONTAP 9.10.1

By Jim Svesnik,  
Quality Assurance Engineer



### Come vengono pianificati gli aggiornamenti automatici per l'installazione

Tutti i nodi idonei dello stesso cluster sono raggruppati per assicurare gli update automatici. Il periodo di tempo durante il quale i nodi idonei vengono pianificati per l'aggiornamento automatico varia in base al livello di priorità dell'aggiornamento e alla percentuale di sistemi che richiedono l'aggiornamento nel proprio ambiente.

Ad esempio, se il 10% o meno del totale dei sistemi è idoneo per un aggiornamento non prioritario, l'aggiornamento viene pianificato per tutti i sistemi idonei entro 1 settimana. Tuttavia, se il 76% o più dei sistemi totali sono idonei per un aggiornamento non prioritario, l'aggiornamento viene scaglionato tra i sistemi idonei nel corso di 8 settimane. Questa installazione sfalsata consente di ridurre i rischi per l'ambiente generale in caso di problemi con un aggiornamento che deve essere risolto.

La percentuale dei sistemi totali programmati per gli aggiornamenti automatici per settimana è la seguente:

#### Per aggiornamenti critici

percentuale di sistemi che richiedono un aggiornamento	% di aggiornamenti che si verificano la settimana 1	% di aggiornamenti che si verificano la settimana 2
50% o inferiore	100%	
50-100%	30%	70%

#### Per aggiornamenti ad alta priorità

percentuale di sistemi che richiedono un aggiornamento	percentuale di aggiornamenti che si verificano per settimana			
	settimana 1	settimana 2	settimana 3	settimana 4
<b>25% o meno</b>	100%			
<b>26-50%</b>	30%	70%		
<b>50-100%</b>	10%	20%	30%	40%

#### Per gli aggiornamenti con priorità normale

percentuale di sistemi che richiedono un aggiornamento	percentuale di aggiornamenti che si verificano per settimana							
	settimana 1	settimana 2	settimana 3	settimana 4	settimana 5	settimana 6	settimana 7	settimana 8
<b>10% o meno</b>	100%							
<b>11-20%</b>	30%	70%						
<b>21-50%</b>	10%	20%	30%	40%				
<b>51-75%</b>	5%	10%	15%	20%	20%	30%		
<b>76-100%</b>	5%	5%	10%	10%	15%	15%	20%	20%

## Abilitare gli aggiornamenti automatici

A partire da ONTAP 9.10.1, è possibile attivare gli aggiornamenti automatici per consentire a ONTAP di scaricare e installare gli aggiornamenti del firmware senza alcun intervento.

A partire da ONTAP 9.13.1, questi aggiornamenti automatici includono anche aggiornamenti automatici del database del fuso orario.

### Prima di iniziare

È necessario disporre di un diritto di supporto corrente. Questo può essere validato su ["Sito di supporto NetApp"](#) Nella pagina **Dettagli sistema**.

### A proposito di questa attività

Per attivare gli aggiornamenti automatici, è necessario prima attivare AutoSupport con HTTPS. Se AutoSupport non è abilitato sul cluster o se AutoSupport è abilitato sul cluster con un altro protocollo di trasporto, durante questa procedura sarà possibile attivarlo con HTTPS.

## Fasi

1. In System Manager, fare clic su **Eventi**.
2. Nella sezione **Panoramica**, accanto a **attiva aggiornamento automatico**, fare clic su **azioni>attiva**.
3. Se non si dispone di AutoSupport con HTTPS attivato, selezionare per attivarlo.
4. Accettare i termini e le condizioni e selezionare **Salva**.


## Informazioni correlate

["Risolvere i problemi relativi all'erogazione dei messaggi AutoSupport su HTTP o HTTPS"](#)

## Modificare gli aggiornamenti automatici

Quando gli aggiornamenti automatici sono attivati, per impostazione predefinita, ONTAP rileva, scarica e installa automaticamente tutti gli aggiornamenti del firmware consigliati e, a partire da ONTAP 9.13.1, gli aggiornamenti del database del fuso orario di ONTAP. Se si desidera visualizzare gli aggiornamenti consigliati prima dell'installazione o se si desidera che i consigli vengano automaticamente disinstallati, è possibile modificare il comportamento predefinito in base alle proprie preferenze.

## Fasi

1. In System Manager, fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **aggiornamento automatico**, fare clic su  per visualizzare un elenco di azioni.
3. Fare clic su **Edit Automatic Update Settings** (Modifica impostazioni di aggiornamento automatico).
4. Specificare le azioni predefinite da eseguire per ciascun tipo di evento.

È possibile scegliere di aggiornare, visualizzare le notifiche o chiudere automaticamente gli aggiornamenti per ciascun tipo di evento.






Il database del fuso orario di ONTAP è controllato dal tipo di evento DEI FILE DI SISTEMA.

## Gestire gli aggiornamenti automatici consigliati

Il registro degli aggiornamenti automatici visualizza un elenco di suggerimenti e dettagli sugli aggiornamenti, tra cui una descrizione, una categoria, l'ora pianificata per l'installazione, lo stato ed eventuali errori. È possibile visualizzare il registro e decidere quale azione eseguire per ogni suggerimento.

## Fasi

1. Visualizza l'elenco dei consigli:

Impostazioni della vista dal cluster	Dalla scheda firmware Update (aggiornamento firmware)
a. Fare clic su <b>Cluster &gt; Settings</b> (Cluster > Impostazioni). b. Nella sezione <b>aggiornamento automatico</b> , fare clic su  , Quindi fare clic su <b>Visualizza tutti gli aggiornamenti automatici</b> .	a. Fare clic su <b>Cluster &gt; Overview</b> (Cluster > Panoramica). b. Nella sezione <b>Panoramica</b> , fare clic su <b>Altro</b>  , Quindi fare clic su <b>aggiornamento ONTAP</b> . c. Selezionare la scheda <b>aggiornamento firmware</b> . d. Nella scheda <b>aggiornamento firmware</b> , fare clic su <b>Altro</b>  , Quindi fare clic su <b>Visualizza tutti gli aggiornamenti automatici</b> .

2. Fare clic su  accanto alla descrizione per visualizzare un elenco di azioni che è possibile eseguire in base al suggerimento.

È possibile eseguire una delle seguenti azioni, a seconda dello stato del suggerimento:

Se l'aggiornamento è in questo stato...	È possibile...
Non è stato pianificato	<b>Update:</b> Avvia il processo di aggiornamento.  <b>Schedule:</b> Consente di impostare una data per l'avvio del processo di aggiornamento.  <b>Dismiss:</b> Elimina la raccomandazione dall'elenco.
È stato pianificato	<b>Update:</b> Avvia il processo di aggiornamento.  <b>Edit Schedule</b> (Modifica pianificazione): Consente di modificare la data pianificata per l'avvio del processo di aggiornamento.  <b>Annulla pianificazione:</b> Annulla la data pianificata.
È stato respinto	<b>Undismiss:</b> Riporta il suggerimento all'elenco.
È in corso di applicazione o di download	<b>Annulla:</b> Annulla l'aggiornamento.

## Aggiornare il firmware manualmente

A partire da ONTAP 9.9.1, se si è registrati con "[Active IQ Unified Manager](#)", È possibile ricevere avvisi in System Manager che informano quando gli aggiornamenti del firmware per i dispositivi supportati, come dischi, shelf di dischi, Service Processor (SP) o Baseboard Management Controller (BMC) sono in sospeso sul cluster.

Se si utilizza ONTAP 9.8 o non si è registrati a Active IQ Unified Manager, è possibile accedere al sito del supporto NetApp per scaricare gli aggiornamenti del firmware.

### **Prima di iniziare**

Per prepararsi a un aggiornamento del firmware senza problemi, è necessario riavviare il SP o il BMC prima dell'inizio dell'aggiornamento. È possibile utilizzare `system service-processor reboot-sp -node node_name` comando per riavviare.

### **Fasi**

Seguire la procedura appropriata in base alla propria versione di ONTAP e se si è registrati con Active IQ Unified Manager.

## ONTAP 9.9.1 e versioni successive con Active IQ

1. In System Manager, accedere a **Dashboard**.


Nella sezione **Health**, viene visualizzato un messaggio se sono presenti aggiornamenti del firmware consigliati per il cluster.

2. Fare clic sul messaggio di avviso.

La scheda **aggiornamento firmware** viene visualizzata nella pagina **aggiornamento**.


3. Fare clic su **Download dal sito di supporto NetApp** per l'aggiornamento del firmware che si desidera eseguire.

Viene visualizzato il NetApp Support Site.

4. Accedere al NetApp Support Site e scaricare il pacchetto di immagine del firmware necessario per l'aggiornamento.
5. Copiare i file su un server HTTP o FTP della rete o in una cartella locale.
6. In System Manager, fare clic su **Cluster > Panoramica**.
7. Nell'angolo destro del riquadro **Panoramica**, fare clic su **Altro**  E selezionare **aggiornamento ONTAP**.
8. Fare clic su **firmware Update** (aggiornamento firmware).
9. A seconda della versione di ONTAP in uso, procedere come segue:

ONTAP 9.9.1 e 9.10.0	ONTAP 9.10.1 e versioni successive
<ol style="list-style-type: none"><li>a. Selezionare <b>da Server</b> o <b>Client locale</b></li><li>b. Specificare l'URL del server o la posizione del file.</li></ol>	<ol style="list-style-type: none"><li>a. Nell'elenco degli aggiornamenti consigliati, selezionare <b>azioni</b>.</li><li>b. Fare clic su <b>Update</b> (Aggiorna) per installare l'aggiornamento immediatamente o su <b>Schedule</b> (programma) per pianificarlo in un secondo momento.  Se l'aggiornamento è già pianificato, è possibile eseguire le operazioni <b>Modifica</b> o <b>Annulla</b>.</li><li>c. Selezionare il pulsante <b>Update firmware</b> (Aggiorna firmware).</li></ol>

## ONTAP 9.8 e versioni successive senza Active IQ

1. Passare a ["Sito di supporto NetApp"](#) ed effettuare l'accesso.
2. Selezionare il pacchetto firmware che si desidera utilizzare per aggiornare il firmware del cluster.
3. Copiare i file su un server HTTP o FTP della rete o in una cartella locale.
4. In System Manager, fare clic su **Cluster > Panoramica**.
5. Nell'angolo destro del riquadro **Panoramica**, fare clic su **Altro**  E selezionare **aggiornamento ONTAP**.



6. Fare clic su **firmware Update** (aggiornamento firmware).
7. A seconda della versione di ONTAP in uso, procedere come segue:

ONTAP 9.8, 9.9.1 e 9.10.0	ONTAP 9.10.1 e versioni successive
<ol style="list-style-type: none"> <li>1. Selezionare <b>da Server o Client locale</b></li> <li>2. Specificare l'URL del server o la posizione del file.</li> </ol>	<ol style="list-style-type: none"> <li>1. Nell'elenco degli aggiornamenti consigliati, selezionare <b>azioni</b>.</li> <li>2. Fare clic su <b>Update</b> (Aggiorna) per installare l'aggiornamento immediatamente o su <b>Schedule</b> (programma) per pianificarlo in un secondo momento.  Se l'aggiornamento è già pianificato, è possibile eseguire le operazioni <b>Modifica</b> o <b>Annulla</b>.</li> <li>3. Selezionare il pulsante <b>Update firmware</b> (Aggiorna firmware).</li> </ol>

### Al termine

È possibile monitorare o verificare gli aggiornamenti in **Riepilogo aggiornamenti firmware**. Per visualizzare gli aggiornamenti disinstallati o non installati, fare clic su **Cluster > Impostazioni > aggiornamento automatico > Visualizza tutti gli aggiornamenti automatici**.

## Ripristina ONTAP

### Panoramica di Revert ONTAP

Per passare da un cluster a una release ONTAP precedente, è necessario eseguire una reversione.

Le informazioni contenute in questa sezione guideranno l'utente attraverso i passaggi da eseguire prima e dopo l'indirizzamento, incluse le risorse da leggere e i necessari controlli pre e post-indirizzamento da eseguire.



Se è necessario eseguire la transizione di un cluster da ONTAP 9.1 a ONTAP 9.0, è necessario utilizzare la procedura di downgrade documentata ["qui"](#).

### Ho bisogno di supporto tecnico per ripristinare?

È possibile eseguire il ripristino senza assistenza su cluster nuovi o di test. È necessario contattare il supporto tecnico per ripristinare i cluster di produzione. Se si verifica una delle seguenti condizioni, contattare il supporto tecnico:

- Ci si trova in un ambiente di produzione e il revert non riesce o si verificano problemi prima o dopo il revert, come ad esempio:
  - Il processo di revert non riesce e non può essere completato.
  - Il processo di revert termina, ma il cluster non è utilizzabile in un ambiente di produzione.
  - Il processo di revert termina e il cluster entra in produzione, ma non sei soddisfatto del suo comportamento.

- I volumi sono stati creati in ONTAP 9.5 o versione successiva ed è necessario ripristinare una versione precedente. I volumi che utilizzano la compressione adattiva devono essere decompressi prima di eseguire il ripristino.

## Percorsi di revert

La versione di ONTAP a cui è possibile ripristinare varia in base alla versione di ONTAP attualmente in esecuzione sui nodi. È possibile utilizzare `system image show` Per determinare la versione di ONTAP in esecuzione su ciascun nodo.

Queste linee guida si riferiscono solo alle release on-premise di ONTAP. Per informazioni sul ripristino di ONTAP nel cloud, vedere ["Ripristino o downgrade di Cloud Volumes ONTAP"](#).

Puoi ripristinare da...	Per...
ONTAP 9.14.1	ONTAP 9.13.1
ONTAP 9.13.1	ONTAP 9.12.1
ONTAP 9.12.1	ONTAP 9.11.1
ONTAP 9.11.1	ONTAP 9.10.1
ONTAP 9.10.1	ONTAP 9.9.1
ONTAP 9.9.1	ONTAP 9.8
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5
ONTAP 9.5	ONTAP 9.4
ONTAP 9.4	ONTAP 9.3
ONTAP 9.3	ONTAP 9.2
ONTAP 9.2	ONTAP 9.1
ONTAP 9.1 o ONTAP 9	Data ONTAP 8.3.x



Per passare da ONTAP 9.1 a 9.0, seguire la procedura ["processo di downgrade"](#) documentato qui.

## Cosa devo leggere prima di ripristinare?

### Risorse da rivedere prima di ripristinare

Prima di ripristinare ONTAP, è necessario confermare il supporto hardware ed esaminare le risorse per comprendere i problemi che potrebbero verificarsi o che è necessario risolvere.

1. Esaminare ["Note sulla versione di ONTAP 9"](#) per la release di destinazione.

La sezione "attenzione importante" descrive i potenziali problemi che è necessario conoscere prima di eseguire il downgrade o il reverting.

2. Verificare che la piattaforma hardware sia supportata nella release di destinazione.

["NetApp Hardware Universe"](#)

3. Verificare che il cluster e gli switch di gestione siano supportati nella release di destinazione.

Verificare che le versioni del software NX-OS (switch di rete cluster), IOS (switch di rete di gestione) e del file di configurazione di riferimento (RCF) siano compatibili con la versione di ONTAP a cui si esegue il ripristino.

["Download NetApp: Switch Ethernet Cisco"](#)

4. Se il cluster è configurato per LA SAN, verificare che la configurazione DELLA SAN sia completamente supportata.

Tutti i componenti SAN, inclusi la versione del software ONTAP di destinazione, il sistema operativo host e le patch, il software delle utility host richiesto, i driver e il firmware dell'adattatore, devono essere supportati.

["Tool di matrice di interoperabilità NetApp"](#)

### Considerazioni sul revert

Prima di iniziare una reversione del ONTAP, è necessario considerare i problemi e le limitazioni di revert.

- Il reversion è un'operazione di interruzione.

Durante la revisione non è possibile accedere al client. Se si sta ripristinando un cluster di produzione, assicurarsi di includere questa interruzione nella pianificazione.

- La revisione influisce su tutti i nodi del cluster.

La reversione interessa tutti i nodi nel cluster; tuttavia, la reversione deve essere eseguita e completata su ogni coppia ha prima che le altre coppie ha vengano ripristinate.

- La revisione è completa quando tutti i nodi eseguono la nuova release di destinazione.

Quando il cluster si trova in uno stato di versione mista, non inserire alcun comando che alteri l'operazione o la configurazione del cluster, a meno che non sia necessario per soddisfare i requisiti di reversione; sono consentite le operazioni di monitoraggio.



Se alcuni nodi sono stati ripristinati, ma non tutti, non tentare di aggiornare il cluster alla release di origine.

- Quando si ripristina un nodo, i dati memorizzati nella cache vengono cancellati in un modulo Flash cache.

Poiché nel modulo Flash cache non sono presenti dati memorizzati nella cache, il nodo serve le richieste di lettura iniziali dal disco, con conseguente riduzione delle prestazioni di lettura durante questo periodo. Il nodo ricompila la cache man mano che serve le richieste di lettura.

- Un LUN di cui viene eseguito il backup su nastro in esecuzione su ONTAP 9.x può essere ripristinato solo alla versione 9.x e successive e non a una versione precedente.
- Se la versione corrente di ONTAP supporta la funzionalità ACP in-band e si ripristina una versione di ONTAP che non supporta IBACP, il percorso alternativo dello shelf di dischi viene disattivato.
- Se LDAP viene utilizzato da una qualsiasi delle macchine virtuali di storage (SVM), la funzione di riferimento LDAP deve essere disattivata prima della revisione.
- Nei sistemi MetroCluster IP che utilizzano switch conformi a MetroCluster ma non validati da MetroCluster, la revisione da ONTAP 9.7 a 9.6 è un'interruzione, in quanto non è disponibile alcun supporto per i sistemi che utilizzano ONTAP 9.6 e versioni precedenti.

## Cose da verificare prima di ripristinare

Prima di eseguire il revert, è necessario verificare lo stato del cluster, lo stato dello storage e l'ora del sistema. È inoltre necessario eliminare tutti i processi del cluster in esecuzione e terminare correttamente tutte le sessioni SMB che non sono continuamente disponibili.

### Verificare lo stato del cluster

Prima di ripristinare il cluster, è necessario verificare che i nodi siano integri e idonei a partecipare al cluster e che il cluster sia in quorum.

1. Verificare che i nodi del cluster siano online e idonei a partecipare al cluster: `cluster show`

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node0                true    true
node1                true    true
```

Se un nodo non è integro o non è idoneo, controllare i registri EMS per verificare la presenza di errori e intraprendere un'azione correttiva.

2. Impostare il livello di privilegio su Advanced:

```
set -privilege advanced
```

Invio `y` per continuare.

3. Verificare i dettagli di configurazione per ciascun processo RDB.

- L'epoca del database relazionale e l'epoca del database devono corrispondere per ciascun nodo.
- Il master del quorum per squillo deve essere lo stesso per tutti i nodi.

Si noti che ogni squillo potrebbe avere un master di quorum diverso.

Per visualizzare questo processo RDB...	Immettere questo comando...
Applicazione di gestione	<code>cluster ring show -unitname mgmt</code>
Database di posizioni dei volumi	<code>cluster ring show -unitname vlodb</code>
Virtual-Interface Manager	<code>cluster ring show -unitname vifmgr</code>
Daemon di gestione SAN	<code>cluster ring show -unitname bcomd</code>

Questo esempio mostra il processo del database di localizzazione del volume:

```
cluster1::*> cluster ring show -unitname vlodb
Node      UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----
node0     vlodb      154          154      14847   node0      master
node1     vlodb      154          154      14847   node0      secondary
node2     vlodb      154          154      14847   node0      secondary
node3     vlodb      154          154      14847   node0      secondary
4 entries were displayed.
```

4. Tornare al livello di privilegio admin:

```
set -privilege admin
```

5. Se si opera in un ambiente SAN, verificare che ciascun nodo si trovi in un quorum SAN: `event log show -severity informational -message-name scsiblade.*`

Il messaggio di evento scsiblade più recente per ciascun nodo dovrebbe indicare che il blade scsi è in quorum.

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
Time              Node      Severity      Event
-----
MM/DD/YYYY TIME  node0     INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1     INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

## Informazioni correlate

## Verificare lo stato dello storage

Prima di ripristinare un cluster, verificare lo stato di dischi, aggregati e volumi.

1. Verificare lo stato del disco:

Per verificare la presenza di...	Eeguire questa operazione...
Dischi rotti	<ol style="list-style-type: none"><li>a. Visualizzare eventuali dischi rotti: <code>storage disk show -state broken</code></li><li>b. Rimuovere o sostituire eventuali dischi rotti.</li></ol>
Dischi in fase di manutenzione o ricostruzione	<ol style="list-style-type: none"><li>a. Visualizzare i dischi in stato di manutenzione, in sospenso o di ricostruzione: <code>`storage disk show -state maintenance</code></li></ol>
pending	<code>reconstructing`</code> .. Prima di procedere, attendere il completamento dell'operazione di manutenzione o ricostruzione.

2. Verificare che tutti gli aggregati siano online visualizzando lo stato dello storage fisico e logico, inclusi gli aggregati di storage: `storage aggregate show -state !online`

Questo comando visualizza gli aggregati *non* online. Tutti gli aggregati devono essere online prima e dopo l'esecuzione di un aggiornamento o di una revisione importante.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verificare che tutti i volumi siano online visualizzando tutti i volumi *non* online: `volume show -state !online`

Tutti i volumi devono essere online prima e dopo l'esecuzione di un aggiornamento o di una revisione importante.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verificare che non vi siano volumi incoerenti: `volume show -is-inconsistent true`

Consultare l'articolo della Knowledge base "[Volume che mostra WAFL incoerente](#)" su come affrontare i volumi incoerenti.

## Informazioni correlate

"[Gestione di dischi e aggregati](#)"

## Verifica dell'ora del sistema

Prima di eseguire il ripristino, verificare che NTP sia configurato e che l'ora sia sincronizzata nel cluster.

1. Verificare che il cluster sia associato a un server NTP: `cluster time-service ntp server show`
2. Verificare che ogni nodo abbia la stessa data e ora: `cluster date show`

```
cluster1::> cluster date show
Node      Date              Timezone
-----
node0     4/6/2013 20:54:38 GMT
node1     4/6/2013 20:54:38 GMT
node2     4/6/2013 20:54:38 GMT
node3     4/6/2013 20:54:38 GMT
4 entries were displayed.
```

## Verificare che non siano in esecuzione lavori

Prima di ripristinare il software ONTAP, è necessario verificare lo stato dei processi del cluster. Se sono presenti processi di aggregato, volume, NDMP (dump o ripristino) o Snapshot (ad esempio creazione, eliminazione, spostamento, modifica, replica, e montare i job) in esecuzione o in coda, è necessario consentire il completamento dei job o interrompere le voci in coda.

1. Esaminare l'elenco di tutti i processi di aggregato, volume o Snapshot in esecuzione o in coda: `job show`

```
cluster1::> job show
Job ID Name              Owning
      Vserver      Node      State
-----
8629  Vol Reaper        cluster1  -      Queued
      Description: Vol Reaper Job
8630  Certificate Expiry Check
      cluster1  -      Queued
      Description: Certificate Expiry Check
.
.
.
```

2. Eliminare qualsiasi processo di copia Snapshot, volume o aggregato in esecuzione o in coda: `job delete -id job_id`

```
cluster1::> job delete -id 8629
```

3. Verificare che nessun processo di aggregazione, volume o Snapshot sia in esecuzione o in coda: `job`

show

In questo esempio, tutti i processi in esecuzione e in coda sono stati eliminati:

```
cluster1::> job show
```

Job ID	Name	Owning Vserver	Node	State
9944	SnapMirrorDaemon_7_2147484678	cluster1	node1	Dormant
Description: Snapmirror Daemon for 7_2147484678				
18377	SnapMirror Service Job	cluster1	node0	Dormant
Description: SnapMirror Service Job				

2 entries were displayed

### Sessioni SMB che devono essere terminate

Prima di eseguire il ripristino, è necessario identificare e terminare correttamente tutte le sessioni SMB che non sono continuamente disponibili.

Le condivisioni SMB a disponibilità continua, a cui accedono i client Hyper-V o Microsoft SQL Server utilizzando il protocollo SMB 3.0, non devono essere interrotte prima dell'aggiornamento o del downgrade.

1. Identificare eventuali sessioni SMB stabilite che non sono continuamente disponibili: `vserver cifs session show -continuously-available No -instance`

Questo comando visualizza informazioni dettagliate sulle sessioni SMB che non hanno disponibilità continua. Prima di procedere con il downgrade di ONTAP, è necessario interrommarli.



```
cluster1::> vserver cifs session show -continuously-available No
-instance

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
Workstation IP address: 203.0.113.20
Authentication Mechanism: NTLMv2
Windows User: CIFSLAB\user1
UNIX User: nobody
Open Shares: 1
Open Files: 2
Open Other: 0
Connected Time: 8m 39s
Idle Time: 7m 45s
Protocol Version: SMB2_1
Continuously Available: No
1 entry was displayed.
```

2. Se necessario, identificare i file aperti per ogni sessione SMB identificata: `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1

Node:      node1
Vserver:   vs1
Connection: 4160072788
Session:    1
File       File       Open Hosting
Continuously
ID         Type        Mode Volume          Share              Available
-----
-----
1          Regular    rw   vol10             homedirshare       No
Path: \TestDocument.docx
2          Regular    rw   vol10             homedirshare       No
Path: \file1.txt
2 entries were displayed.
```

## Autenticazione NVMe in-band

Se si torna da ONTAP 9.12.1 o versione successiva a ONTAP 9.12.0 o versione precedente, è necessario

"disattiva l'autenticazione in banda" prima di tornare indietro. Se l'autenticazione in banda mediante DH-HMAC-CHAP non è disattivata, l'operazione di revert avrà esito negativo.

## Quali altri elementi devo controllare prima di ripristinare?

### Controlli di pre-revert

A seconda dell'ambiente in uso, è necessario prendere in considerazione alcuni fattori prima del ripristino. Per iniziare, consulta la tabella riportata di seguito per scoprire le considerazioni speciali da prendere in considerazione.

Chiedetevi...	Se la risposta è sì, eseguire questa operazione...
Il cluster esegue SnapMirror?	<ul style="list-style-type: none"><li>• <a href="#">Esaminare le considerazioni relative al ripristino dei sistemi con le relazioni sincroni di SnapMirror</a></li><li>• <a href="#">Esaminare i requisiti di review per le relazioni di SnapMirror e SnapVault</a></li></ul>
Il cluster esegue SnapLock?	<a href="#">Impostare i periodi di autocommit</a>
Si dispone di volumi FlexClone in due parti?	<a href="#">Condivisione inversa dei blocchi fisici</a>
Si dispone di volumi FlexGroup?	<a href="#">Disattiva la funzionalità qtree</a>
I server CIFS sono in modalità workgroup?	<a href="#">Spostare o eliminare i server CIFS in modalità gruppo di lavoro</a>
Sono presenti volumi deduplicati?	<a href="#">Verificare che il volume contenga spazio libero sufficiente</a>
Sono disponibili copie Snapshot?	<a href="#">Preparare le copie Snapshot</a>
Si torna a ONTAP 8.3.x?	<a href="#">Identificare gli account utente che utilizzano la funzione hash SHA-2</a>
La protezione anti-ransomware è configurata per ONTAP 9.11.1 o versioni successive?	<a href="#">Controllare le licenze anti-ransomware</a>
L'accesso multiprotocollo S3 è configurato per ONTAP 9.12.1 o versioni successive?	<a href="#">Rimuovere la configurazione del bucket S3 NAS</a>
Il trunking di sessione NFSv4,1 è configurato per ONTAP 9.14.1 o versione successiva?	<a href="#">Rimuovere la configurazione trunking sessione NFSv4,1</a>

### Controlli pre-revert MetroCluster

A seconda della configurazione di MetroCluster, è necessario prendere in considerazione alcuni fattori prima del ripristino. Per iniziare, consulta la tabella riportata di seguito per scoprire le considerazioni speciali da prendere in considerazione.

Chiedetevi...	Se la risposta è sì, eseguire questa operazione...
Si dispone di una configurazione MetroCluster a due o quattro nodi?	<a href="#">Disattiva lo switchover automatico non pianificato</a>

Chiedetevi...	Se la risposta è sì, eseguire questa operazione...
Si dispone di una configurazione MetroCluster IP o fabric-attached a quattro o otto nodi con ONTAP 9.12.1 o versione successiva?	<a href="#">Disattivare IPSec</a>

## SnapMirror

### Considerazioni per il ripristino dei sistemi con le relazioni sincroni di SnapMirror

Prima di eseguire il ripristino da ONTAP 9.6 a ONTAP 9.5, è necessario conoscere le considerazioni relative alle relazioni sincroni di SnapMirror.

Prima di eseguire il ripristino, è necessario eseguire le seguenti operazioni se si dispone di relazioni sincroni di SnapMirror:

- È necessario eliminare qualsiasi relazione sincrona di SnapMirror in cui il volume di origine sta fornendo dati utilizzando NFSv4 o SMB.

ONTAP 9.5 non supporta NFSv4 e SMB.

- È necessario eliminare qualsiasi relazione sincrona di SnapMirror in una distribuzione a cascata con mirror.

Un'implementazione a cascata di mirror non è supportata per le relazioni sincroni di SnapMirror in ONTAP 9.5.

- Se le copie Snapshot comuni in ONTAP 9.5 non sono disponibili durante il ripristino, è necessario inizializzare la relazione sincrona di SnapMirror dopo il ripristino.

Dopo due ore di aggiornamento a ONTAP 9.6, le copie Snapshot comuni di ONTAP 9.5 vengono sostituite automaticamente dalle copie Snapshot comuni di ONTAP 9.6. Pertanto, non è possibile risincronizzare la relazione sincrona di SnapMirror dopo il ripristino se le copie Snapshot comuni da ONTAP 9.5 non sono disponibili.

### Requisiti di revirsione per le relazioni SnapMirror e SnapVault

Il comando revert-to del nodo di sistema segnala eventuali relazioni SnapMirror e SnapVault che devono essere eliminate o riconfigurate per il completamento del processo di reversione. Tuttavia, è necessario conoscere questi requisiti prima di iniziare la revisione.

- Tutte le relazioni mirror di SnapVault e data Protection devono essere interrotte e poi interrotte.

Una volta completata la reversione, è possibile risincronizzare e riprendere queste relazioni se esiste una copia Snapshot comune.

- Le relazioni di SnapVault non devono contenere i seguenti tipi di criteri di SnapMirror:
  - mirror asincrono

È necessario eliminare qualsiasi relazione che utilizzi questo tipo di criterio.

- MirrorAndVault

Se esiste una di queste relazioni, modificare la policy di SnapMirror in mirror-vault.

- Tutte le relazioni mirror di condivisione del carico e i volumi di destinazione devono essere cancellati.
- Le relazioni di SnapMirror con i volumi di destinazione FlexClone devono essere eliminate.
- La compressione di rete deve essere disattivata per ciascun criterio SnapMirror.
- La regola `all_source_snapshot` deve essere rimossa da qualsiasi policy SnapMirror di tipo `async-mirror`.



Le operazioni SFSR (Single file Snapshot Restore) e PFSR (Partial file Snapshot Restore) sono obsolete nel volume root.

- Tutte le operazioni di ripristino di un singolo file e Snapshot attualmente in esecuzione devono essere completate prima di poter procedere con la revisione.

È possibile attendere il completamento dell'operazione di ripristino oppure interromperla.

- Tutte le operazioni di ripristino incomplete di un singolo file e Snapshot devono essere rimosse utilizzando il comando di ripristino di `snapmirror`.

### **Impostare i periodi di autocommit per i volumi SnapLock prima del ripristino**

Per eseguire il ripristino da ONTAP 9, il valore del periodo di autocommit per i volumi SnapLock deve essere impostato in ore, non in giorni. Prima di tentare di ripristinare, è necessario controllare il valore di autocommit per i volumi SnapLock e modificarlo da giorni a ore, se necessario.

1. Verificare che nel cluster vi siano volumi SnapLock con periodi di autocommit non supportati: `volume snaplock show -autocommit-period *days`
2. Modificare i periodi di autocommit non supportati in ore: `volume snaplock modify -vserver vservers_name -volume volume_name -autocommit-period value hours`

### **Reverse physical block sharing in volumi FlexClone divisi**

Se un volume FlexClone è stato diviso dal volume padre, è necessario annullare la condivisione di qualsiasi blocco fisico tra il clone e il volume padre prima di tornare da ONTAP 9.4 o versione successiva a una versione precedente di ONTAP.

Questa attività è applicabile solo ai sistemi AFF quando è stato eseguito il split su uno qualsiasi dei volumi FlexClone.

1. Accedere al livello di privilegio avanzato: `set -privilege advanced`
2. Identificare i volumi FlexClone divisi con blocchi fisici condivisi: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
```

Node	Vserver	Volume	Aggregate
node1	vs1	vol_clone1	aggr1
node2	vs2	vol_clone2	aggr2

2 entries were displayed.

3. Annullare la condivisione fisica dei blocchi in tutti i volumi FlexClone divisi nel cluster: `volume clone sharing-by-split undo start-all`
4. Verificare che non vi siano volumi FlexClone divisi con blocchi fisici condivisi: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
```

This table is currently empty.

### Disattivare la funzionalità qtree nei volumi FlexGroup prima di eseguire il ripristino

I qtree per i volumi FlexGroup non sono supportati prima di ONTAP 9.3. È necessario disattivare la funzionalità qtree sui volumi FlexGroup prima di passare da ONTAP 9.3 a una versione precedente di ONTAP.

La funzionalità qtree viene attivata quando si crea un qtree o se si modificano gli attributi Security-style e oplock-mode del qtree predefinito.

1. Identificare ed eliminare tutti i qtree non predefiniti in ogni volume FlexGroup abilitati con la funzionalità qtree:
  - a. Accedere al livello di privilegio avanzato: `set -privilege advanced`
  - b. Verificare se un volume FlexGroup è abilitato con la funzionalità qtree.

Per ONTAP 9.6 o versioni successive, utilizzare: `volume show -is-qtree-caching-enabled true`

Per ONTAP 9.5 o versioni precedenti, utilizzare: `volume show -is-flexgroup-qtree-enabled true`

```
cluster1::*> volume show -is-flexgroup-qtree-enabled true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
vs0	fg	-	online	RW	320MB
220.4MB	31%				

- c. Eliminare tutti i qtree non predefiniti in ogni volume FlexGroup abilitati con la funzionalità qtree:

```
volume qtree delete -vserver svm_name -volume volume_name -qtree qtree_name
```

Se la funzionalità qtree è attivata perché sono stati modificati gli attributi del qtree predefinito e se non si dispone di qtree, è possibile saltare questo passaggio.

```
cluster1::*> volume qtree delete -vserver vs0 -volume fg -qtree qtree4
WARNING: Are you sure you want to delete qtree qtree4 in volume fg
vserver vs0? {y|n}: y
[Job 38] Job is queued: Delete qtree qtree4 in volume fg vserver vs0.
```

2. Disattivare la funzionalità qtree su ogni volume FlexGroup: `volume flexgroup qtree-disable -vserver svm_name -volume volume_name`

```
cluster1::*> volume flexgroup qtree-disable -vserver vs0 -volume fg
```

3. Identificare ed eliminare le copie Snapshot attivate con la funzionalità qtree.

- a. Verificare se le copie Snapshot sono attivate con la funzionalità qtree: `volume snapshot show -vserver vserver_name -volume volume_name -fields is-flexgroup-qtree-enabled`

```
cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-
flexgroup-qtree-enabled
vserver volume snapshot is-flexgroup-qtree-enabled
-----
vs0      fg      fg_snap1 true
vs0      fg      daily.2017-09-27_0010 true
vs0      fg      daily.2017-09-28_0010 true
vs0      fg      snapmirror.0241f354-a865-11e7-a1c0-
00a098a71764_2147867740.2017-10-04_124524 true
```

- b. Eliminare tutte le copie Snapshot attivate con la funzionalità qtree: `volume snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot_name -force true -ignore-owners true`

Le copie Snapshot che devono essere eliminate includono le copie Snapshot regolari e le copie Snapshot eseguite per le relazioni SnapMirror. Se è stata creata una relazione SnapMirror per i volumi FlexGroup con un cluster di destinazione che esegue ONTAP 9.2 o versioni precedenti, è necessario eliminare tutte le copie Snapshot eseguite quando il volume FlexGroup di origine è stato abilitato per la funzionalità qtree.

```
cluster1::> volume snapshot delete -vserver vs0 -volume fg -snapshot
daily.2017-09-27_0010 -force true -ignore-owners true
```

## Informazioni correlate

["Gestione dei volumi FlexGroup"](#)

### Identificare e spostare i server SMB in modalità workgroup

Prima di eseguire un revert, è necessario eliminare tutti i server SMB in modalità gruppo di lavoro o spostarli in un dominio. La modalità Workgroup non è supportata nelle versioni di ONTAP precedenti a ONTAP 9.

1. Identificare i server SMB con uno stile di autenticazione del gruppo di lavoro: `vserver cifs show`
2. Spostare o eliminare i server identificati:

Se stai andando a...	Quindi utilizzare questo comando....
Spostare il server SMB dal gruppo di lavoro a un dominio Active Directory:	<code>vserver cifs modify -vserver vserver_name -domain domain_name</code>
Eliminare il server SMB	<code>vserver cifs delete -vserver vserver_name</code>

3. Se il server SMB è stato eliminato, immettere il nome utente del dominio, quindi la password utente.

## Informazioni correlate

["Gestione delle PMI"](#)

### Verificare che i volumi deduplicati dispongano di spazio libero sufficiente prima di eseguire il ripristino

Prima di eseguire il ripristino da qualsiasi versione di ONTAP 9, è necessario assicurarsi che i volumi contengano spazio libero sufficiente per l'operazione di revert.

Il volume deve disporre di spazio sufficiente per contenere i risparmi ottenuti attraverso il rilevamento inline di blocchi di zero. Consultare l'articolo della Knowledge base ["Come verificare i risparmi di spazio derivanti da deduplica, compressione e compattazione in ONTAP 9"](#).

Se sono state attivate sia la deduplica che la compressione dei dati su un volume che si desidera ripristinare, è necessario ripristinare la compressione dei dati prima di ripristinare la deduplica.

1. Utilizzare il comando `Volume Efficiency show` con l'opzione `-fields` per visualizzare l'avanzamento delle operazioni di efficienza in esecuzione sui volumi.

Il seguente comando visualizza l'avanzamento delle operazioni di efficienza: `volume efficiency show -fields vserver,volume,progress`

2. Utilizzare il comando di arresto dell'efficienza del volume con l'opzione `-all` per arrestare tutte le operazioni di deduplica attive e in coda.

Il seguente comando interrompe tutte le operazioni di deduplica attive e in coda sul volume Vola: `volume efficiency stop -vserver vs1 -volume Vola -all`

3. Utilizzare il comando `set -Privilege Advanced` per accedere al livello di privilegio avanzato.

4. Utilizza il comando `revert-to` per l'efficienza del volume con l'opzione `-version` per eseguire il downgrade dei metadati di efficienza di un volume a una versione specifica di ONTAP.

Il seguente comando ripristina i metadati di efficienza sul volume `volA` in ONTAP 9.x:

```
volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x
```



Il comando `revert-to` per l'efficienza dei volumi ripristina i volumi presenti nel nodo su cui viene eseguito questo comando. Questo comando non ripristina i volumi tra i nodi.

5. Utilizza il comando di visualizzazione dell'efficienza del volume con l'opzione `-op-status` per monitorare l'avanzamento del downgrade.

Il seguente comando monitora e visualizza lo stato del downgrade:

```
volume efficiency show -vserver vs1 -op-status Downgrading
```

6. Se il `revert` non riesce, utilizzare il comando di visualizzazione dell'efficienza del volume con l'opzione `-instance` per verificare il motivo dell'errore di `revert`.

Il seguente comando visualizza informazioni dettagliate su tutti i campi:

```
volume efficiency show -vserver vs1 -volume vol1 - instance
```

7. Una volta completata l'operazione di `revert`, tornare al livello di privilegio `admin`: `set -privilege admin`

["Gestione dello storage logico"](#)

## Preparare le copie Snapshot prima di eseguire il ripristino

Prima di tornare a una release precedente di ONTAP, è necessario disattivare tutti i criteri di copia Snapshot ed eliminare le copie Snapshot create dopo l'aggiornamento alla release corrente.

Se si esegue il ripristino in un ambiente SnapMirror, è necessario prima eliminare le seguenti relazioni mirror:

- Tutte le relazioni mirror di condivisione del carico
- Qualsiasi relazione di mirroring della protezione dei dati creata in ONTAP 8.3.x.
- Tutte le relazioni di mirroring della protezione dei dati se il cluster è stato ricreato in ONTAP 8.3.x.
  - a. Disattivare le policy di copia Snapshot per tutti i dati SVM: `volume snapshot policy modify -vserver * -enabled false`
  - b. Disattivare le policy di copia Snapshot per gli aggregati di ciascun nodo:
    - i. Identificare gli aggregati del nodo utilizzando il comando `run-nodenodenameaggr status`.
    - ii. Disattivare il criterio di copia Snapshot per ciascun aggregato: `run -node nodename aggr options aggr_name nosnap on`
    - iii. Ripetere questo passaggio per ogni nodo rimanente.
  - c. Disattivare le policy di copia Snapshot per ogni volume root del nodo:
    - i. Identificare il volume root del nodo utilizzando il comando `run-nodenamevol status`.

Il volume root viene identificato dalla parola `root` nella colonna `Options` dell'output del comando di



stato vol.

```
vs1::> run -node node1 vol status
```

Volume State	Status	Options
vol0 online	raid_dp, flex 64-bit	root, nvfail=on

- i. Disattivare il criterio di copia Snapshot sul volume root: `run -node nodename vol options root_volume_name nosnap on`
  - ii. Ripetere questo passaggio per ogni nodo rimanente.
- d. Eliminare tutte le copie Snapshot create dopo l'aggiornamento alla release corrente:
- i. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
  - ii. Disattivare le snapshot: `snapshot policy modify -vserver * -enabled false`
  - iii. Eliminare le copie Snapshot più recenti del nodo: `volume snapshot prepare-for-revert -node nodename`

Questo comando elimina le copie Snapshot più recenti su ogni volume di dati, aggregato root e volume root.

Se non è possibile eliminare le copie Snapshot, il comando non riesce e segnala eventuali azioni necessarie da eseguire prima di poter eliminare le copie Snapshot. Prima di passare alla fase successiva, è necessario completare le azioni richieste ed eseguire nuovamente il comando di preparazione per l'indirizzamento dello snapshot del volume.

```
cluster1::*> volume snapshot prepare-for-revert -node node1
```

```
Warning: This command will delete all Snapshot copies that have the  
format used by the current version of ONTAP. It will fail if any  
Snapshot copy polices are enabled, or  
if any Snapshot copies have an owner. Continue? {y|n}: y
```

- i. Verificare che le copie Snapshot siano state eliminate: `volume snapshot show -node nodename`

Se rimangono copie Snapshot di una versione più recente, forzarne l'eliminazione: `volume snapshot delete {-fs-version 9.0 -node nodename -is-constituent true} -ignore-owners -force`

- ii. Ripetere questo passaggio c per ogni nodo rimanente.
- iii. Tornare al livello di privilegio admin: `set -privilege admin`



È necessario eseguire questi passaggi su entrambi i cluster nella configurazione MetroCluster.

## Identificare gli account utente che utilizzano la funzione hash SHA-2

Se si esegue il ripristino da ONTAP 9.1 o ONTAP 9.0 a ONTAP 8.3.x, gli utenti dell'account SHA-2 non possono più essere autenticati con le proprie password. Prima di eseguire il ripristino, è necessario identificare gli account utente che utilizzano la funzione hash SHA-2, in modo che, dopo il ripristino, sia possibile ripristinarne le password per utilizzare il tipo di crittografia (MD5) supportato dalla release a cui si esegue il ripristino.

1. Passare all'impostazione dei privilegi avanzata: `set -privilege advanced`
2. Identificare gli account utente che utilizzano la funzione SHA-2: `security login show -vserver * -username * -application * -authentication-method password -hash-function !md5`
3. Conservare l'output del comando per l'utilizzo dopo il revert.



Durante l'indirizzamento, viene richiesto di eseguire il comando `Advanced security login password-prepare-to-downgrade`. Per reimpostare la propria password per utilizzare la funzione hash MD5. Se la password non è crittografata con MD5, il comando richiede una nuova password e la crittografa con MD5, consentendo l'autenticazione della credenziale dopo il revert.

## Controllare la licenza Autonomous ransomware Protection prima di eseguire il ripristino da ONTAP 9.11.1 o versione successiva

Se è stata configurata la protezione ransomware autonoma (ARP) e si passa da ONTAP 9.11.1 o versione successiva a ONTAP 9.10.1 o versione precedente, potrebbero verificarsi messaggi di avviso e funzionalità ARP limitate.

In ONTAP 9.11.1, la licenza anti-ransomware ha sostituito la licenza per la gestione delle chiavi multi-tenant (MTKM). Se il sistema dispone della licenza `Anti_ransomware` ma non della licenza `MT_EK_MGMT`, durante il revert viene visualizzato un avviso che informa che ARP non può essere abilitato sui nuovi volumi al momento del revert.

I volumi con protezione esistente continueranno a funzionare normalmente dopo il ripristino e lo stato ARP può essere visualizzato utilizzando l'interfaccia CLI di ONTAP. System Manager non può visualizzare lo stato ARP senza la licenza MTKM.

Pertanto, se si desidera che ARP continui dopo aver eseguito il ripristino a ONTAP 9.10.1, assicurarsi che la licenza MTKM sia installata prima di eseguire il ripristino. ["Scopri di più sulle licenze ARP."](#)

## Rimuovere la configurazione del bucket S3 NAS prima di tornare da ONTAP 9.12.1 o versione successiva

Se è stato configurato l'accesso client S3 per i dati NAS, prima di passare da ONTAP 9.12.1 o versione successiva a ONTAP 9.11.1 o versione precedente, è necessario utilizzare l'interfaccia a riga di comando (CLI) di ONTAP per rimuovere la configurazione del bucket NAS e rimuovere eventuali mappature dei nomi (da S3 utenti a utenti Windows o Unix).

### A proposito di questa attività

Le seguenti attività vengono completate in background durante il processo di revert.

- Rimuovere tutte le creazioni di oggetti singleton parzialmente completate (ovvero tutte le voci nelle directory nascoste).
- Rimuovere tutte le directory nascoste; potrebbe esserci una per ogni volume accessibile dalla directory principale dell'esportazione mappata dal bucket S3 NAS.
- Rimuovere la tabella di caricamento.
- Eliminare tutti i valori default-unix-user e default-Windows-user per tutti i server S3 configurati.

## Fasi

1. Rimuovere la configurazione della benna S3 NAS:

```
vserver object-store-server bucket delete -vserver _svm_name_ -bucket
_s3_nas_bucket_name_
```

2. Rimuovi mapping dei nomi per UNIX:

```
vserver name-mapping delete -vserver _svm_name_ -direction s3-unix
```

3. Rimuovere le mappature dei nomi per Windows:

```
vserver name-mapping delete -vserver _svm_name_ -direction s3-win
```

4. Rimozione dei protocolli S3 dalla SVM:

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

## Rimuovere la configurazione trunking sessione NFSv4,1 prima di tornare da ONTAP 9.14.1 o versioni successive

Se è stato attivato il trunking per le connessioni client e si torna a una versione precedente di ONTAP 9.14.1, è necessario disattivare il trunking su qualsiasi server NFSv4,1 prima di eseguire il ripristino.

Quando si accede a `revert-to` viene visualizzato un messaggio di avviso che avvisa di disattivare il trunking prima di procedere.

Dopo aver ripristinato una versione precedente di ONTAP, i client che utilizzano connessioni trunked tornano a utilizzare una singola connessione. Il loro throughput di dati sarà influenzato, ma non ci sarà alcuna interruzione. Il comportamento dell'indirizzamento è identico alla modifica dell'opzione trunking NFSv4,1 per la SVM da abilitato a disabilitato.

## Fasi

1. Disattivare il trunking sul server NFSv4,1:

```
vserver nfs modify -vserver svm_name -v4.1-trunking disabled
```

2. Verificare che NFS sia configurato come desiderato:

```
vserver nfs show -vserver svm_name
```

## **Disattivare lo switchover automatico non pianificato prima di ripristinare le configurazioni MetroCluster a due e quattro nodi**

Prima di ripristinare una configurazione MetroCluster a due o quattro nodi, è necessario disattivare lo switchover automatico non pianificato (USO).

1. Su entrambi i cluster in MetroCluster, disattivare lo switchover automatico non pianificato: `metrocluster modify -auto-switchover-failure-domain auso-disabled`

### **Informazioni correlate**

["Gestione MetroCluster e disaster recovery"](#)

## **Disattivare IPSec prima di ripristinare le configurazioni MetroCluster**

Prima di ripristinare una configurazione MetroCluster, è necessario disattivare IPSec.

Non è possibile ripristinare ONTAP in una configurazione MetroCluster che esegue ONTAP 9.12.1 con IPSec attivato. Viene eseguito un controllo prima del ripristino per assicurarsi che non vi siano configurazioni IPSec all'interno della configurazione MetroCluster. Prima di continuare con l'indirizzamento, è necessario rimuovere le configurazioni IPsec presenti e disattivare IPsec. Se IPSec è attivato, anche se non sono stati configurati criteri utente, viene bloccato il ripristino di ONTAP.

## **Scaricare e installare l'immagine del software ONTAP**

È necessario prima scaricare il software ONTAP dal sito del supporto NetApp, quindi installarlo.

### **Scaricare l'immagine del software**

Per eseguire il downgrade o il ripristino da ONTAP 9.4 e versioni successive, è possibile copiare l'immagine del software ONTAP dal sito del supporto NetApp in una cartella locale. Per eseguire il downgrade o il ripristino a ONTAP 9.3 o versioni precedenti, è necessario copiare l'immagine del software ONTAP su un server HTTP o FTP sulla rete.

Tenere presenti le seguenti importanti informazioni:

- Le immagini software sono specifiche dei modelli di piattaforma.

È necessario ottenere l'immagine corretta per il cluster. Le immagini software, le informazioni sulla versione del firmware e il firmware più recente per il modello di piattaforma sono disponibili sul sito del supporto NetApp.

- Le immagini software includono la versione più recente del firmware di sistema disponibile al momento del rilascio di una determinata versione di ONTAP.
- Se si esegue il downgrade di un sistema con crittografia dei volumi NetApp da ONTAP 9.5 o versioni successive, è necessario scaricare l'immagine del software ONTAP per i paesi senza restrizioni, che include crittografia dei volumi NetApp.

Se si utilizza l'immagine del software ONTAP per i paesi con restrizioni per eseguire il downgrade o il

ripristino di un sistema con crittografia dei volumi NetApp, il sistema esegue una panoramica e si perde l'accesso ai volumi.

- a. Individuare il software ONTAP di destinazione in "[Download di software](#)" Area del NetApp Support Site.
- b. Copiare l'immagine del software.
  - Per ONTAP 9.3 o versioni precedenti, copiare l'immagine software (ad esempio, 93\_q\_image.tgz) dal sito del supporto NetApp nella directory sul server HTTP o sul server FTP da cui verrà servita l'immagine.
  - Per ONTAP 9.4 o versioni successive, copiare l'immagine software (ad esempio, 97\_q\_image.tgz) dal sito di supporto NetApp nella directory sul server HTTP o FTP da cui verrà servita l'immagine o in una cartella locale.

## Installare l'immagine software

È necessario installare l'immagine software di destinazione sui nodi del cluster.

- Se si esegue il downgrade o il ripristino di un sistema con crittografia dei volumi NetApp da ONTAP 9.5 o versioni successive, è necessario aver scaricato l'immagine del software ONTAP per i paesi non soggetti a restrizioni, che includono crittografia dei volumi NetApp.

Se si utilizza l'immagine del software ONTAP per i paesi con restrizioni per eseguire il downgrade o il ripristino di un sistema con crittografia dei volumi NetApp, il sistema esegue una panoramica e si perde l'accesso ai volumi.

- a. Impostare il livello di privilegio su Advanced (avanzato), immettendo **y** quando viene richiesto di continuare: `set -privilege advanced`

Il prompt avanzato (\*>).

- b. Installare l'immagine software sui nodi.

Questo comando scarica e installa contemporaneamente l'immagine software su tutti i nodi. Per scaricare e installare l'immagine su ogni nodo, non specificare il parametro `-background`.

- Se si esegue il downgrade o si ripristina una configurazione non MetroCluster o una configurazione MetroCluster a due nodi: `system node image update -node * -package location -replace-package true -setdefault true -background true`

Questo comando utilizza una query estesa per modificare l'immagine software di destinazione, installata come immagine alternativa, come immagine predefinita per il nodo.

- Se si esegue il downgrade o il ripristino di una configurazione MetroCluster a quattro o otto nodi, è necessario eseguire il seguente comando su entrambi i cluster: `system node image update -node * -package location -replace-package true true -background true -setdefault false`

Questo comando utilizza una query estesa per modificare l'immagine software di destinazione, che viene installata come immagine alternativa su ciascun nodo.

- c. Invio **y** per continuare quando richiesto.
- d. Verificare che l'immagine software sia stata scaricata e installata su ciascun nodo: `system node image show-update-progress -node *`

Questo comando visualizza lo stato corrente del download e dell'installazione dell'immagine software. Continuare ad eseguire questo comando fino a quando tutti i nodi non riportano uno stato di esecuzione di Exited e uno stato di uscita di Success.

Il comando di aggiornamento dell'immagine del nodo di sistema può non riuscire e visualizzare messaggi di errore o di avviso. Dopo aver risolto eventuali errori o avvisi, è possibile eseguire nuovamente il comando.

Questo esempio mostra un cluster a due nodi in cui l'immagine software viene scaricata e installata correttamente su entrambi i nodi:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:    After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

## Ripristinare un cluster ONTAP

Per portare il cluster offline per tornare a una versione precedente di ONTAP, è necessario disattivare il failover dello storage e le LIF dei dati, gestire le precondizioni di reversione, ripristinare le configurazioni del cluster e del file system su un nodo, quindi ripetere il processo per ciascun nodo aggiuntivo del cluster.

È necessario completare l'indirizzamento ["verifiche"](#) e ["controlli preliminari"](#).

Il ripristino di un cluster richiede che il cluster venga disattivato per tutta la durata della reversione.

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`

Inserire **y** quando viene richiesto di continuare.

2. Verificare che il software ONTAP di destinazione sia installato: `system image show`

L'esempio seguente mostra che la versione 9.1 è installata come immagine alternativa su entrambi i nodi:

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	true	true	9.2	MM/DD/YYYY TIME
	image2	false	false	9.1	MM/DD/YYYY TIME
node1	image1	true	true	9.2	MM/DD/YYYY TIME
	image2	false	false	9.1	MM/DD/YYYY TIME

4 entries were displayed.

3. Disattivare tutte le LIF dei dati nel cluster: `network interface modify {-role data} -status -admin down`
4. Determinare se si dispone di relazioni FlexCache tra cluster: `flexcache origin show-caches -relationship-type inter-cluster`
5. Se sono presenti flexcache tra cluster, disattivare il ciclo di vita dei dati sul cluster di cache: `network interface modify -vserver vserver_name -lif lif_name -status-admin down`
6. Se il cluster è costituito da due soli nodi, disattivare il cluster ha: `cluster ha modify -configured false`
7. Disattiva il failover dello storage per i nodi della coppia ha da uno dei nodi: `storage failover modify -node nodename -enabled false`

È necessario disattivare il failover dello storage una sola volta per la coppia ha. Quando si disattiva il failover dello storage per un nodo, anche il failover dello storage viene disattivato sul partner del nodo.

8. Accedi al nodo che desideri ripristinare.

Per ripristinare un nodo, è necessario accedere al cluster attraverso la LIF di gestione dei nodi del nodo.

9. Impostare l'immagine software ONTAP di destinazione del nodo come immagine predefinita: `system image modify -node nodename -image target_image -isdefault true`
10. Verificare che l'immagine del software ONTAP di destinazione sia impostata come immagine predefinita per il nodo che si sta ripristinando: `system image show`

Il seguente esempio mostra che la versione 9.1 è impostata come immagine predefinita su node0:

```
cluster1::*> system image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0	image1	false	true	9.2	MM/DD/YYYY TIME
	image2	true	false	9.1	MM/DD/YYYY TIME
node1	image1	true	true	9.2	MM/DD/YYYY TIME
	image2	false	false	9.1	MM/DD/YYYY TIME

4 entries were displayed.

11. Se il cluster è costituito da due soli nodi, verificare che il nodo non sia dotato di epsilon:

a. Verificare se il nodo contiene attualmente epsilon: `cluster show -node nodename`

L'esempio seguente mostra che il nodo contiene epsilon:

```
cluster1::*> cluster show -node node1
```

```
Node: node1
UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
Epsilon: true
Eligibility: true
Health: true
```

a. Se il nodo contiene epsilon, contrassegnare epsilon come false sul nodo in modo che epsilon possa essere trasferito al partner del nodo: `cluster modify -node nodenameA -epsilon false`

b. Trasferire epsilon al partner del nodo contrassegnando epsilon true sul nodo partner: `cluster modify -node nodenameB -epsilon true`

12. Verificare che il nodo sia pronto per la reversione: `system node revert-to -node nodename -check-only true -version 9.x`

Il parametro di sola verifica identifica eventuali precondizioni da risolvere prima del ripristino, come ad esempio i seguenti esempi:

- Disattivazione del failover dello storage
- Disattivazione del criterio Snapshot
- Eliminazione delle copie Snapshot create dopo l'aggiornamento alla versione successiva di ONTAP

13. Verificare che tutte le condizioni preliminari siano state soddisfatte: `system node revert-to -node nodename -check-only true -version 9.x`

14. Ripristinare la configurazione del cluster del nodo: `system node revert-to -node nodename -version 9.x`



L'opzione `-version` si riferisce alla release di destinazione. Ad esempio, se il software installato e verificato è ONTAP 9.1, il valore corretto dell'opzione `-version` è 9.1.

La configurazione del cluster viene ripristinata e l'utente viene disconnesso dalla shell del clustershell.

15. Accedi nuovamente alla shell clustershell, quindi passa al nodeshell: `run -node nodename`

Dopo aver effettuato nuovamente l'accesso alla shell clustershell, potrebbero essere necessari alcuni minuti prima che sia pronto ad accettare il comando nodeshell. Quindi, se il comando non riesce, attendere alcuni minuti e riprovare.

16. Ripristinare la configurazione del file system del nodo: `revert_to 9.x`

Questo comando verifica che la configurazione del file system del nodo sia pronta per essere ripristinata, quindi la ripristina. Se vengono identificate delle precondizioni, è necessario affrontarle ed eseguire nuovamente il comando `revert_to`.



L'utilizzo di una console di sistema per monitorare il processo di revert consente di visualizzare maggiori dettagli rispetto a quelli visualizzati in un nodeshell.

Se AUTOBOOT è true, al termine del comando, il nodo si riavvierà in ONTAP.

Se L'OPZIONE AUTOBOOT è false, al termine del comando viene visualizzato il prompt DEL CARICATORE. Invoia `yes` per ripristinare, quindi utilizzare `boot_ontap` per riavviare manualmente il nodo.

17. Una volta riavviato il nodo, verificare che il nuovo software sia in esecuzione: `system node image show`

Nell'esempio seguente, image1 è la nuova versione di ONTAP ed è impostata come la versione corrente su node0:

```
cluster1::*> system node image show
```

Node	Image	Is Default	Is Current	Version	Install Date
node0					
	image1	true	true	X.X.X	MM/DD/YYYY TIME
	image2	false	false	Y.Y.Y	MM/DD/YYYY TIME
node1					
	image1	true	false	X.X.X	MM/DD/YYYY TIME
	image2	false	true	Y.Y.Y	MM/DD/YYYY TIME

4 entries were displayed.

18. verificare che lo stato di revert sia completo per ciascun nodo: `system node upgrade-revert show -node nodename`

Lo stato deve essere "completo", "non necessario" o "non sono state restituite voci di tabella".

19. Ripetere [\[step-6\]](#) attraverso [\[step-16\]](#) Sull'altro nodo della coppia ha.

20. Se il cluster è costituito da due soli nodi, riabilitare il cluster ha: `cluster ha modify -configured`

true

21. Riabilitare il failover dello storage su entrambi i nodi se era stato precedentemente disattivato: `storage failover modify -node nodename -enabled true`
22. Ripetere [\[step-5\]](#) attraverso [\[step-19\]](#) Per ogni coppia ha aggiuntiva e per entrambi i cluster nella configurazione MetroCluster.

## Cosa devo fare dopo il ripristino del cluster?

### Verificare lo stato di salute del cluster e dello storage dopo il downgrade o il revert

Dopo il downgrade o il ripristino di un cluster, è necessario verificare che i nodi siano integri e idonei a partecipare al cluster e che il cluster sia in quorum. È inoltre necessario verificare lo stato di dischi, aggregati e volumi.

#### Verificare lo stato del cluster

1. Verificare che i nodi del cluster siano online e idonei a partecipare al cluster: `cluster show`

```
cluster1::> cluster show
Node                      Health  Eligibility
-----
node0                     true   true
node1                     true   true
```

Se un nodo non è integro o non è idoneo, controllare i registri EMS per verificare la presenza di errori e intraprendere un'azione correttiva.

2. Impostare il livello di privilegio su Advanced:

```
set -privilege advanced
```

Invio `y` per continuare.

3. Verificare i dettagli di configurazione per ciascun processo RDB.

- L'epoca del database relazionale e l'epoca del database devono corrispondere per ciascun nodo.
- Il master del quorum per squillo deve essere lo stesso per tutti i nodi.

Si noti che ogni squillo potrebbe avere un master di quorum diverso.

Per visualizzare questo processo RDB...	Immettere questo comando...
Applicazione di gestione	<code>cluster ring show -unitname mgmt</code>
Database di posizioni dei volumi	<code>cluster ring show -unitname vl原因</code>
Virtual-Interface Manager	<code>cluster ring show -unitname vifmgr</code>

Per visualizzare questo processo RDB...	Immettere questo comando...
Daemon di gestione SAN	<code>cluster ring show -unitname bcomd</code>

Questo esempio mostra il processo del database di localizzazione del volume:

```
cluster1::*> cluster ring show -unitname vlodb
```

Node	UnitName	Epoch	DB Epoch	DB Trnxs	Master	Online
node0	vlodb	154	154	14847	node0	master
node1	vlodb	154	154	14847	node0	secondary
node2	vlodb	154	154	14847	node0	secondary
node3	vlodb	154	154	14847	node0	secondary

4 entries were displayed.

4. Tornare al livello di privilegio admin: `set -privilege admin`
5. Se si opera in un ambiente SAN, verificare che ciascun nodo si trovi in un quorum SAN: `event log show -severity informational -message-name scsiblade.*`

Il messaggio di evento scsiblade più recente per ciascun nodo dovrebbe indicare che il blade scsi è in quorum.

```
cluster1::*> event log show -severity informational -message-name
scsiblade.*
```

Time	Node	Severity	Event
MM/DD/YYYY TIME	node0	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...
MM/DD/YYYY TIME	node1	INFORMATIONAL	scsiblade.in.quorum: The scsi-blade ...

## Informazioni correlate

["Amministrazione del sistema"](#)

### Verificare lo stato dello storage

Dopo aver ripristinato o eseguito il downgrade di un cluster, è necessario verificare lo stato di dischi, aggregati e volumi.

1. Verificare lo stato del disco:

Per verificare la presenza di...	Eeguire questa operazione...
Dischi rotti	a. Visualizzare eventuali dischi rotti: <code>storage disk show -state broken</code> b. Rimuovere o sostituire eventuali dischi rotti.
Dischi in fase di manutenzione o ricostruzione	a. Visualizzare i dischi in stato di manutenzione, in sospeso o di ricostruzione: <code>storage disk show -state maintenance</code>
pending	reconstructing` .. Prima di procedere, attendere il completamento dell'operazione di manutenzione o ricostruzione.

- Verificare che tutti gli aggregati siano online visualizzando lo stato dello storage fisico e logico, inclusi gli aggregati di storage: `storage aggregate show -state !online`

Questo comando visualizza gli aggregati *non* online. Tutti gli aggregati devono essere online prima e dopo l'esecuzione di un aggiornamento o di una revisione importante.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

- Verificare che tutti i volumi siano online visualizzando tutti i volumi *non* online: `volume show -state !online`

Tutti i volumi devono essere online prima e dopo l'esecuzione di un aggiornamento o di una revisione importante.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

- Verificare che non vi siano volumi incoerenti: `volume show -is-inconsistent true`

Consultare l'articolo della Knowledge base ["Volume che mostra WAFL incoerente"](#) su come affrontare i volumi incoerenti.

## Informazioni correlate

["Gestione di dischi e aggregati"](#)

## Abilitare lo switchover automatico per le configurazioni MetroCluster

In questo argomento vengono fornite informazioni relative alle attività aggiuntive da eseguire dopo la revisione delle configurazioni MetroCluster.

- Attivare lo switchover automatico non pianificato: `metrocluster modify -auto-switchover -failure-domain auto-on-cluster-disaster`

2. Convalidare la configurazione MetroCluster: `metrocluster check run`

### Abilitare e ripristinare le LIF alle porte home dopo un revert

Durante un riavvio, alcune LIF potrebbero essere state migrate alle porte di failover assegnate. Dopo aver ripristinato un cluster, è necessario abilitare e ripristinare le LIF non presenti nelle porte domestiche.

Il comando di revert dell'interfaccia di rete riporta un LIF che non si trova attualmente sulla porta home alla porta home, a condizione che la porta home sia operativa. Quando viene creata la LIF, viene specificata la porta home di LIF; è possibile determinare la porta home di una LIF utilizzando il comando `show` dell'interfaccia di rete.

1. Visualizzare lo stato di tutti i LIF: `network interface show`

Questo esempio mostra lo stato di tutte le LIF per una macchina virtuale di storage (SVM).

```
cluster1::> network interface show -vserver vs0
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
vs0					
	data001	down/down	192.0.2.120/24	node0	e0e
true					
	data002	down/down	192.0.2.121/24	node0	e0f
true					
	data003	down/down	192.0.2.122/24	node0	e2a
true					
	data004	down/down	192.0.2.123/24	node0	e2b
true					
	data005	down/down	192.0.2.124/24	node0	e0e
false					
	data006	down/down	192.0.2.125/24	node0	e0f
false					
	data007	down/down	192.0.2.126/24	node0	e2a
false					
	data008	down/down	192.0.2.127/24	node0	e2b
false					

8 entries were displayed.

Se viene visualizzato un LIF con lo stato Status Admin (Amministratore stato) su Down (inattivo) o con lo stato is home (iniziale) su false, passare alla fase successiva.

2. Abilitare le LIF dei dati: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

### 3. Ripristinare le LIF alle porte home: `network interface revert *`

Questo comando ripristina tutte le LIF alle porte home.

```
cluster1::> network interface revert *
8 entries were acted on.
```

### 4. Verificare che tutte le LIF si trovino nelle porte home: `network interface show`

Questo esempio mostra che tutte le LIF per SVM vs0 si trovano sulle porte home.

```
cluster1::> network interface show -vserver vs0
```

Current Is	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Port
vs0	data001	up/up	192.0.2.120/24	node0	e0e
true	data002	up/up	192.0.2.121/24	node0	e0f
true	data003	up/up	192.0.2.122/24	node0	e2a
true	data004	up/up	192.0.2.123/24	node0	e2b
true	data005	up/up	192.0.2.124/24	node1	e0e
true	data006	up/up	192.0.2.125/24	node1	e0f
true	data007	up/up	192.0.2.126/24	node1	e2a
true	data008	up/up	192.0.2.127/24	node1	e2b

```
8 entries were displayed.
```

## Attiva le policy di copia Snapshot dopo il ripristino

Dopo aver eseguito il ripristino di una versione precedente di ONTAP, è necessario

attivare i criteri di copia Snapshot per iniziare nuovamente la creazione delle copie Snapshot.

Si stanno riattivando le pianificazioni Snapshot disattivate prima di tornare a una versione precedente di ONTAP.

1. Abilitare le policy di copia Snapshot per tutti i dati SVM:

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. Per ciascun nodo, attivare il criterio di copia Snapshot del volume root utilizzando il comando `run-nodenamevol optionsroot_vol_namenosnap off`.

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

### Verificare l'accesso del client (SMB e NFS)

Per i protocolli configurati, verificare l'accesso dai client SMB e NFS per verificare che il cluster sia accessibile.

### Verificare le voci del firewall IPv6

Una nuova versione da qualsiasi versione di ONTAP 9 potrebbe comportare la mancanza di voci predefinite del firewall IPv6 per alcuni servizi nelle policy firewall. Verificare che le voci del firewall richieste siano state ripristinate nel sistema.

1. Verificare che tutti i criteri firewall siano corretti confrontandoli con quelli predefiniti: `system services firewall policy show`

Nell'esempio seguente vengono illustrati i criteri predefiniti:

```
cluster1::*> system services firewall policy show
```

Policy	Service	Action	IP-List
-----			
cluster	dns	allow	0.0.0.0/0
	http	allow	0.0.0.0/0
	https	allow	0.0.0.0/0
	ndmp	allow	0.0.0.0/0
	ntp	allow	0.0.0.0/0
	rsh	allow	0.0.0.0/0
	snmp	allow	0.0.0.0/0
	ssh	allow	0.0.0.0/0
	telnet	allow	0.0.0.0/0
data	dns	allow	0.0.0.0/0, ::/0
	http	deny	0.0.0.0/0, ::/0
	https	deny	0.0.0.0/0, ::/0
	ndmp	allow	0.0.0.0/0, ::/0
	ntp	deny	0.0.0.0/0, ::/0
	rsh	deny	0.0.0.0/0, ::/0
.			
.			
.			

2. Aggiungere manualmente eventuali voci di firewall IPv6 predefinite mancanti creando una nuova policy  
firewall:system services firewall policy create

```
cluster1::*> system services firewall policy create -policy newIPv6  
-service ssh -action allow -ip-list ::/0
```

3. Applicare il nuovo criterio alla LIF per consentire l'accesso a un servizio di rete:network interface  
modify

```
cluster1::*> network interface modify -vserver VS1 -lif LIF1  
-firewall-policy newIPv6
```

### Ripristinare la funzione hash della password al tipo di crittografia supportato

Se si è eseguito il ripristino da ONTAP 9.1 o ONTAP 9.0 a ONTAP 8.3.x, gli utenti dell'account SHA-2 non possono più essere autenticati con le proprie password. Le password devono essere reimpostate per utilizzare il tipo di crittografia MDS.

1. Impostare una password temporanea per ciascun account utente SHA-2 [identificato prima del ripristino](#):



```
security login password -username user_name -vserver vserver_name
```

2. Comunicare la password temporanea agli utenti interessati e fare in modo che accedano tramite una console o una sessione SSH per modificare le password come richiesto dal sistema.

### **Considerazioni sull'aggiornamento manuale del firmware SP**

Se la funzionalità di aggiornamento automatico SP è attivata (impostazione predefinita), il downgrade o il ripristino a ONTAP 8.3.x non richiede un aggiornamento manuale del firmware SP. Il firmware SP viene aggiornato automaticamente alla versione più recente compatibile supportata dalla versione di ONTAP a cui si è eseguito il ripristino o il downgrade.

Se la funzionalità di aggiornamento automatico del SP è disattivata (non consigliata), una volta completato il processo di revert o downgrade del ONTAP, è necessario aggiornare manualmente il firmware del SP a una versione supportata per la versione del ONTAP a cui si è eseguito il ripristino o il downgrade.

["Matrice di supporto BIOS/ONTAP di NetApp"](#)

["Download NetApp: Firmware di sistema e diagnostica"](#)

### **Modifica degli account utente che possono accedere al Service Processor**

Se sono stati creati account utente su ONTAP 9.8 o versioni precedenti, è stato eseguito l'aggiornamento a ONTAP 9.9.1 o versioni successive (quando `-role` il parametro viene modificato in `admin`), quindi di nuovo a ONTAP 9.8 o versione precedente, la `-role` il parametro viene ripristinato al valore originale. Tuttavia, è necessario verificare che i valori modificati siano accettabili.

Durante il revert, se il ruolo di un utente SP è stato cancellato, viene registrato il messaggio "rbac.spuser.role.notfound" EMS message.

Per ulteriori informazioni, vedere ["Account che possono accedere al SP"](#).

# Amministrazione del cluster

## Gestione del cluster con System Manager

### Panoramica sull'amministrazione con System Manager

System Manager è un'interfaccia di gestione grafica basata su HTML5 che consente di utilizzare un browser Web per gestire i sistemi di storage e gli oggetti di storage (come dischi, volumi e Tier di storage) ed eseguire attività di gestione comuni relative ai sistemi di storage.

Le procedure descritte in questa sezione consentono di gestire il cluster con Gestione di sistema in ONTAP 9.7 e versioni successive.



- System Manager è incluso nel software ONTAP come servizio Web, abilitato per impostazione predefinita e accessibile tramite un browser.
- Il nome di Gestore di sistema è stato modificato a partire da ONTAP 9.6. In ONTAP 9.5 e nelle versioni precedenti era chiamato Gestore di sistema di OnCommand. A partire da ONTAP 9.6 e versioni successive, si chiama Gestore di sistema.
- Se si utilizza la gestione di sistema classica (disponibile solo in ONTAP 9.7 e versioni precedenti), fare riferimento a. ["System Manager Classic \(ONTAP da 9.0 a 9.7\)"](#)

Utilizzando la dashboard di System Manager, è possibile visualizzare informazioni immediate su avvisi e notifiche importanti, l'efficienza e la capacità dei livelli e dei volumi di storage, i nodi disponibili in un cluster, lo stato dei nodi in una coppia ha, le applicazioni e gli oggetti più attivi, e le metriche delle performance di un cluster o di un nodo.

System Manager consente di eseguire numerose attività comuni, ad esempio:

- Creare un cluster, configurare una rete e impostare i dettagli di supporto per il cluster.
- Configurare e gestire oggetti storage, come dischi, Tier locali, volumi, qtree, e quote.
- Configurare protocolli, come SMB e NFS, ed eseguire il provisioning della condivisione dei file.
- Configurare protocolli come FC, FCoE, NVMe e iSCSI per l'accesso a blocchi.
- Creare e configurare componenti di rete, come subnet, domini di broadcast, interfacce di gestione e dati e gruppi di interfacce.
- Impostare e gestire le relazioni di mirroring e vaulting.
- Eseguire operazioni di gestione del cluster, dei nodi di storage e delle macchine virtuali di storage (VM di storage).
- Creare e configurare le VM di storage, gestire gli oggetti storage associati alle VM di storage e gestire i servizi di VM di storage.
- Monitorare e gestire le configurazioni ad alta disponibilità (ha) in un cluster.
- Configurare i service processor per accedere, gestire, monitorare e amministrare il nodo in remoto, indipendentemente dallo stato del nodo.

## Terminologia di System Manager

Per alcune funzionalità delle chiavi ONTAP, System Manager utilizza una terminologia diversa da CLI.

- **Tier locale** – un set di dischi fisici a stato solido o dischi rigidi su cui memorizzare i dati. Potresti conoscere questi come aggregati. Infatti, se si utilizza l'interfaccia CLI di ONTAP, si vedrà comunque il termine *aggregate* utilizzato per rappresentare un Tier locale.
- **Tier cloud** – storage nel cloud utilizzato da ONTAP quando si desidera avere alcuni dati off-premise per uno dei diversi motivi. Se stai pensando alla parte cloud di un FabricPool, l'hai già capito. E se utilizzi un sistema StorageGRID, il tuo cloud potrebbe non essere off-premise. (Un'esperienza on-premise simile al cloud si chiama *cloud privato*).
- **Storage VM** – una macchina virtuale in esecuzione in ONTAP che fornisce servizi di storage e dati ai client. Potresti sapere che si tratta di un *SVM* o di un *vserver*.
- **Interfaccia di rete** - Indirizzo e proprietà assegnati a una porta di rete fisica. Questo potrebbe essere un'interfaccia logica (LIF).
- **Pause** - azione che interrompe le operazioni. Prima di ONTAP 9.8, in altre versioni di Gestore di sistema potrebbe essere stato fatto riferimento a *quiesce*.

## Utilizzare System Manager per accedere a un cluster

Se si preferisce utilizzare un'interfaccia grafica invece dell'interfaccia della riga di comando (CLI) per accedere e gestire un cluster, è possibile farlo utilizzando Gestione di sistema, che è incluso in ONTAP come servizio Web, è attivato per impostazione predefinita ed è accessibile tramite un browser.



A partire da ONTAP 9.12.1, System Manager è completamente integrato con BlueXP.

Con BlueXP, puoi gestire la tua infrastruttura multicloud ibrida da un singolo piano di controllo mantenendo la familiare dashboard di System Manager.

Vedere ["Integrazione di System Manager con BlueXP"](#).

### A proposito di questa attività

È possibile utilizzare un'interfaccia di rete per la gestione del cluster (LIF) o un'interfaccia di rete per la gestione dei nodi (LIF) per accedere a System Manager. Per un accesso ininterrotto a System Manager, è necessario utilizzare un'interfaccia di rete per la gestione del cluster (LIF).

### Prima di iniziare

- È necessario disporre di un account utente del cluster configurato con il ruolo "admin" e i tipi di applicazione "http" e "console".
- È necessario abilitare i cookie e i dati del sito nel browser.

### Fasi

1. Puntare il browser Web sull'indirizzo IP dell'interfaccia di rete per la gestione del cluster:

- Se si utilizza IPv4: **`https://cluster-mgmt-LIF`**
- Se si utilizza IPv6: **`https://[cluster-mgmt-LIF]`**



Solo HTTPS è supportato per l'accesso tramite browser di System Manager.

Se il cluster utilizza un certificato digitale autofirmato, il browser potrebbe visualizzare un avviso che indica che il certificato non è attendibile. È possibile riconoscere il rischio di continuare l'accesso o installare un certificato digitale firmato dall'autorità di certificazione (CA) sul cluster per l'autenticazione del server.

2. **Opzionale:** se è stato configurato un banner di accesso mediante l'interfaccia CLI, leggere il messaggio visualizzato nella finestra di dialogo **Avviso** e scegliere l'opzione desiderata per procedere.


Questa opzione non è supportata nei sistemi in cui è attivata l'autenticazione SAML (Security Assertion Markup Language).



- Se non si desidera continuare, fare clic su **Annulla** e chiudere il browser.
- Se si desidera continuare, fare clic su **OK** per accedere alla pagina di accesso di System Manager.

3. Accedere a System Manager utilizzando le credenziali di amministratore del cluster.



A partire da ONTAP 9.11.1, quando si accede a Gestore di sistema, è possibile specificare le impostazioni internazionali. Le impostazioni internazionali specificano alcune impostazioni di localizzazione, ad esempio lingua, valuta, formato data e ora e impostazioni simili. Per ONTAP 9.10.1 e versioni precedenti, le impostazioni internazionali di Gestione sistema vengono rilevate dal browser. Per modificare le impostazioni internazionali di System Manager, è necessario modificare le impostazioni internazionali del browser.

4. **Opzionale:** A partire da ONTAP 9.12.1, è possibile specificare le proprie preferenze per l'aspetto di Gestore di sistema:
  - a. Nell'angolo in alto a destra di System Manager, fare clic su  per gestire le opzioni utente.
  - b. Posizionare l'interruttore a levetta **System Theme** (tema sistema) in base alle proprie preferenze:

Alternare la posizione	Impostazione dell'aspetto
 (sinistra)	Tema chiaro (sfondo chiaro con testo scuro)
Sistema operativo (centrale)	Per impostazione predefinita, viene utilizzata la preferenza per il tema impostata per le applicazioni del sistema operativo (di solito l'impostazione del tema per il browser utilizzato per accedere a System Manager).
 (destra)	Tema scuro (sfondo scuro con testo chiaro)

#### Informazioni correlate

["Gestione dell'accesso ai servizi Web"](#)

["Accesso ai file di log, core dump e MIB di un nodo mediante un browser Web"](#)

## Abilitare le nuove funzioni aggiungendo le chiavi di licenza

Nelle versioni precedenti a ONTAP 9.10.1, le funzioni di ONTAP sono abilitate con chiavi di licenza e le funzioni di ONTAP 9.10.1 e versioni successive sono abilitate con un file di licenza NetApp. È possibile aggiungere chiavi di licenza e file di licenza NetApp utilizzando Gestione sistema.

A partire da ONTAP 9.10.1, si utilizza Gestione di sistema per installare un file di licenza NetApp per abilitare più funzionalità con licenza contemporaneamente. L'utilizzo di un file di licenza NetApp semplifica l'installazione delle licenze, in quanto non è più necessario aggiungere chiavi di licenza per funzionalità separate. È possibile scaricare il file di licenza NetApp dal sito di supporto NetApp.

Se si dispone già di chiavi di licenza per alcune funzioni e si sta eseguendo l'aggiornamento a ONTAP 9.10.1, è possibile continuare a utilizzare tali chiavi di licenza.


#### Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. In **licenze**, selezionare ➔.
3. Selezionare **Sfoglia**. Scegliere il file di licenza NetApp scaricato.
4. Se si desidera aggiungere chiavi di licenza, selezionare **Usa chiavi di licenza di 28 caratteri** e immettere le chiavi.

## Scaricare una configurazione del cluster

A partire da ONTAP 9.11.1, è possibile utilizzare Gestione sistema per scaricare la configurazione di un cluster.

#### Fasi

1. Fare clic su **Cluster > Overview** (Cluster > Panoramica).
2. Fare clic su  **More** per visualizzare il menu a discesa.
3. Selezionare **Download Configuration** (Scarica configurazione).
4. Selezionare le coppie ha, quindi fare clic su **Download**.

La configurazione viene scaricata come foglio di calcolo Excel.

- Il primo foglio contiene i dettagli del cluster.
- Gli altri fogli contengono i dettagli del nodo.

## Assegnare tag a un cluster

A partire da ONTAP 9.14.1, puoi utilizzare System Manager per assegnare tag a un cluster e identificare gli oggetti appartenenti a una categoria, ad esempio progetti o centri di costo.

#### A proposito di questa attività

È possibile assegnare un tag a un cluster. Innanzitutto, è necessario definire e aggiungere il tag. Quindi, è anche possibile modificare o eliminare il tag.

È possibile aggiungere tag durante la creazione di un cluster o aggiungerli in un secondo momento.

È possibile definire un tag specificando una chiave e associando un valore utilizzando il formato `"key:value"`. Ad esempio: `"dept:engineering"` o `"location:san-jose"`.

Quando si creano tag, è necessario tenere in considerazione quanto segue:

- Le chiavi hanno una lunghezza minima di un carattere e non possono essere nulle. I valori possono essere nulli.
- Una chiave può essere associata a più valori separando i valori con una virgola, ad esempio, "location:san-jose,toronto"
- I tag possono essere utilizzati per più risorse.
- I tasti devono iniziare con una lettera minuscola.

## Fasi


Per gestire i tag, procedere come segue:

1. In System Manager, fare clic su **Cluster** per visualizzare la pagina di panoramica.

I tag sono elencati nella sezione **Tag**.

2. Fare clic su **Gestisci tag** per modificare i tag esistenti o aggiungerne di nuovi.

È possibile aggiungere, modificare o eliminare i tag.

Per eseguire questa azione...	Eseguire questa procedura...
Aggiungere un tag	<ol style="list-style-type: none"> <li>a. Fare clic su <b>Aggiungi tag</b>.</li> <li>b. Specificare una chiave e il suo valore o i suoi valori (separare più valori con virgole).</li> <li>c. Fare clic su <b>Save</b> (Salva).</li> </ol>
Modificare un tag	<ol style="list-style-type: none"> <li>a. Modificare il contenuto nei campi <b>chiave</b> e <b>valori (facoltativo)</b>.</li> <li>b. Fare clic su <b>Save</b> (Salva).</li> </ol>
Eliminare un tag	<ol style="list-style-type: none"> <li>a. Fare clic su  accanto al tag che si desidera eliminare.</li> </ol>

## Visualizzare e inviare i casi di supporto

A partire da ONTAP 9.9.1, è possibile visualizzare i casi di supporto da Active IQ associati al cluster. È inoltre possibile copiare i dettagli del cluster necessari per inviare un nuovo caso di supporto sul sito del supporto NetApp. A partire da ONTAP 9.10.1, è possibile attivare la registrazione telemetrica, che aiuta il personale di supporto a risolvere i problemi.



Per ricevere avvisi sugli aggiornamenti del firmware, è necessario essere registrati presso Active IQ Unified Manager. Fare riferimento a. ["Risorse di documentazione Active IQ Unified Manager"](#).

## Fasi

1. In System Manager, selezionare **Support**.

Viene visualizzato un elenco di casi di supporto aperti associati a questo cluster.

2. Fare clic sui seguenti collegamenti per eseguire le procedure:

- **Numero del caso:** Visualizza i dettagli del caso.
- **Vai al sito del supporto NetApp:** Vai alla pagina **My AutoSupport** del sito del supporto NetApp per visualizzare gli articoli della Knowledge base o inviare un nuovo caso di supporto.
- **Visualizza i miei casi:** Accedere alla pagina **i miei casi** sul sito del supporto NetApp.
- **Visualizza dettagli cluster:** Consente di visualizzare e copiare le informazioni necessarie per l'invio di un nuovo caso.

## Abilitare la registrazione di telemetria

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per attivare la registrazione della telemetria. Quando è consentita la registrazione della telemetria, ai messaggi registrati da System Manager viene assegnato un identificatore di telemetria specifico che indica l'esatto processo che ha attivato il messaggio. Tutti i messaggi emessi relativi a tale processo hanno lo stesso identificativo, che consiste nel nome del flusso di lavoro operativo e in un numero (ad esempio "add-volume-1941290").

In caso di problemi di performance, è possibile attivare la registrazione della telemetria, che consente al personale di supporto di identificare più facilmente il processo specifico per il quale è stato emesso un messaggio. Quando si aggiungono identificatori di telemetria ai messaggi, il file di registro viene ingrandito solo leggermente.

### Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Nella sezione **UI Settings** (Impostazioni interfaccia utente), fare clic sulla casella di controllo **Allow Telemetry logging** (Consenti registrazione telemetria).



## Gestire il limite massimo di capacità di una VM di storage in System Manager

A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per attivare un limite massimo di capacità per una VM di storage e impostare una soglia per attivare avvisi quando lo storage utilizzato raggiunge una determinata percentuale della capacità massima.

### Abilitare un limite massimo di capacità per una VM di storage

A partire da ONTAP 9.13.1, è possibile specificare la capacità massima che può essere allocata per tutti i volumi in una VM di storage. È possibile abilitare la capacità massima quando si aggiunge una VM di storage o quando si modifica una VM di storage esistente.

### Fasi

1. Selezionare **Storage > Storage VM**.
2. Eseguire una delle seguenti operazioni:
  - Per aggiungere una VM di storage, fare clic su .
  - Per modificare una VM di storage, fare clic su  Accanto al nome della VM di storage, quindi fare clic su **Edit** (Modifica).
3. Immettere o modificare le impostazioni per la VM di storage, quindi selezionare la casella di controllo "Enable maximum Capacity limit" (Abilita limite massimo di capacità).

4. Specificare la dimensione massima della capacità.
5. Specificare la percentuale della capacità massima che si desidera utilizzare come soglia per attivare gli avvisi.
6. Fare clic su **Save** (Salva).

## Modificare il limite massimo di capacità di una VM di storage

A partire da ONTAP 9.13.1, è possibile modificare il limite di capacità massima di una VM di storage esistente, se [è stato attivato il limite massimo di capacità](#) già.

### Fasi

1. Selezionare **Storage > Storage VM**.
2. Fare clic su  Accanto al nome della VM di storage, quindi fare clic su **Edit** (Modifica).

La casella di controllo "Enable maximum Capacity limit" (Abilita limite massimo di capacità) è già selezionata.

3. Eseguire una delle seguenti operazioni:

Azione	Fasi
Disattivare il limite di capacità massima	<ol style="list-style-type: none"> <li>1. Deselezionare la casella di controllo.</li> <li>2. Fare clic su <b>Save</b> (Salva).</li> </ol>
Modificare il limite di capacità massima	<ol style="list-style-type: none"> <li>1. Specificare la nuova dimensione massima della capacità. Non è possibile specificare una dimensione inferiore allo spazio già allocato nella VM di storage.</li> <li>2. Specificare la nuova percentuale della capacità massima che si desidera utilizzare come soglia per attivare gli avvisi.</li> <li>3. Fare clic su <b>Save</b> (Salva).</li> </ol>

### Informazioni correlate

- ["Visualizzare il limite massimo di capacità di una VM di storage"](#)
- ["Misurazioni della capacità in System Manager"](#)
- ["Gestire i limiti di capacità SVM utilizzando l'interfaccia CLI di ONTAP"](#)

## Monitorare la capacità in System Manager

Con System Manager, è possibile monitorare la quantità di capacità di storage utilizzata e la quantità ancora disponibile per un cluster, un Tier locale o una VM di storage.

Con ogni versione di ONTAP, System Manager fornisce informazioni di monitoraggio della capacità più affidabili:

- A partire da ONTAP 9.10.1, System Manager consente di visualizzare i dati storici sulla capacità del cluster e le proiezioni relative alla quantità di capacità che verrà utilizzata o disponibile in futuro. È inoltre possibile monitorare la capacità dei volumi e dei Tier locali.
- A partire da ONTAP 9.12.1, System Manager visualizza la quantità di capacità impegnata per un Tier



locale.

- A partire da ONTAP 9.13.1, è possibile attivare un limite massimo di capacità per una VM di storage e impostare una soglia per attivare avvisi quando lo storage utilizzato raggiunge una determinata percentuale della capacità massima.



Le misurazioni della capacità utilizzata vengono visualizzate in modo diverso a seconda della versione di ONTAP in uso. Scopri di più in ["Misurazioni della capacità in System Manager"](#).

## Visualizzare la capacità di un cluster

È possibile visualizzare le misurazioni della capacità di un cluster nella dashboard di System Manager.

### Prima di iniziare

Per visualizzare i dati relativi alla capacità nel cloud, è necessario disporre di un account presso Active IQ Digital Advisor ed essere connessi.

### Fasi

1. In System Manager, fare clic su **Dashboard**.
2. Nella sezione **capacità**, è possibile visualizzare quanto segue:

- Capacità totale utilizzata del cluster
- Capacità totale disponibile del cluster
- Percentuali di capacità utilizzata e disponibile.
- Rapporto di riduzione dei dati.
- Quantità di capacità utilizzata nel cloud.
- Cronologia dell'utilizzo della capacità.
- Proiezione dell'utilizzo della capacità



In System Manager, le rappresentazioni della capacità non tengono conto delle capacità del Tier storage root (aggregato).

3. Fare clic sul grafico per visualizzare ulteriori dettagli sulla capacità del cluster.

Le misurazioni della capacità vengono visualizzate in due diagrammi a barre:

- Il grafico in alto mostra la capacità fisica: La dimensione dello spazio fisico utilizzato, riservato e disponibile.
- Il grafico in basso mostra la capacità logica: La dimensione dei dati del client, le copie Snapshot e i cloni e lo spazio logico totale utilizzato.

Sotto i grafici a barre sono riportate le misurazioni per la riduzione dei dati:

- Rapporto di riduzione dei dati solo per i dati del client (copie Snapshot e cloni non inclusi).
- Rapporto complessivo di riduzione dei dati.

Per ulteriori informazioni, vedere ["Misurazioni della capacità in System Manager"](#).

## Visualizzare la capacità di un Tier locale

È possibile visualizzare i dettagli sulla capacità dei Tier locali. A partire da ONTAP 9.12.1, la vista **capacità** include anche la quantità di capacità impegnata per un Tier locale, consentendo di determinare se è necessario aggiungere capacità al Tier locale per soddisfare la capacità impegnata ed evitare di esaurire lo spazio libero.

### Fasi

1. Fare clic su **Storage > Tier**.
2. Selezionare il nome del Tier locale.
3. Nella pagina **Panoramica**, nella sezione **capacità**, la capacità viene visualizzata in un grafico a barre con tre misurazioni:
  - Capacità utilizzata e riservata
  - Capacità disponibile
  - Capacità impegnata (a partire da ONTAP 9.12.1)
4. Fare clic sul grafico per visualizzare i dettagli sulla capacità del Tier locale.

Le misurazioni della capacità vengono visualizzate in due diagrammi a barre:

- Il grafico a barre superiore visualizza la capacità fisica: La dimensione dello spazio fisico utilizzato, riservato e disponibile.
- Il grafico a barre inferiore mostra la capacità logica: La dimensione dei dati del client, le copie Snapshot e i cloni e il totale dello spazio logico utilizzato.

Sotto i grafici a barre sono riportati i rapporti di misurazione per la riduzione dei dati:

- Rapporto di riduzione dei dati solo per i dati del client (copie Snapshot e cloni non inclusi).
- Rapporto complessivo di riduzione dei dati.

Per ulteriori informazioni, vedere ["Misurazioni della capacità in System Manager"](#).

### Azioni facoltative

- Se la capacità impegnata è superiore alla capacità del Tier locale, è possibile aggiungere capacità al Tier locale prima che esaurisca lo spazio libero. Vedere ["Aggiunta di capacità a un Tier locale \(aggiunta di dischi a un aggregato\)"](#).
- È inoltre possibile visualizzare lo storage utilizzato da volumi specifici nel Tier locale selezionando la scheda **Volumes**.

## Visualizzare la capacità dei volumi in una VM di storage

È possibile visualizzare la quantità di storage utilizzata dai volumi in una VM di storage e la quantità di capacità ancora disponibile. La misurazione totale dello storage utilizzato e disponibile viene chiamata "capacità su più volumi".

### Fasi

1. Selezionare **Storage > Storage VM**.
2. Fare clic sul nome della VM di storage.
3. Scorrere fino alla sezione **capacità**, che mostra un grafico a barre con le seguenti misurazioni:

- **Fisico utilizzato:** Somma dello storage fisico utilizzato in tutti i volumi di questa VM di storage.
- **Disponibile:** Somma della capacità disponibile in tutti i volumi di questa VM di storage.
- **Logica utilizzata:** Somma dello storage logico utilizzato in tutti i volumi di questa VM di storage.

Per ulteriori informazioni sulle misurazioni, vedere ["Misurazioni della capacità in System Manager"](#).

## Visualizzare il limite massimo di capacità di una VM di storage

A partire da ONTAP 9.13.1, è possibile visualizzare il limite massimo di capacità di una VM di storage.

### Prima di iniziare

È necessario ["Abilitare il limite massimo di capacità di una VM di storage"](#) prima di visualizzarlo.

### Fasi

1. Selezionare **Storage > Storage VM**.

È possibile visualizzare le misurazioni della capacità massima in due modi:

- Nella riga relativa alla VM di storage, visualizzare la colonna **capacità massima** che contiene un grafico a barre che mostra la capacità utilizzata, la capacità disponibile e la capacità massima.
- Fare clic sul nome della VM di storage. Nella scheda **Panoramica**, scorrere per visualizzare i valori di soglia di avviso relativi alla capacità massima, alla capacità allocata e alla capacità nella colonna di sinistra.

### Informazioni correlate

- ["Modificare il limite massimo di capacità di una VM di storage"](#)
- ["Misurazioni della capacità in System Manager"](#)

## Visualizzare le configurazioni hardware per determinare i problemi

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per visualizzare la configurazione dell'hardware sulla rete e determinare lo stato dei sistemi hardware e le configurazioni di cablaggio.

### Fasi

Per visualizzare le configurazioni hardware, attenersi alla seguente procedura:

1. In System Manager, selezionare **Cluster > hardware**.
2. Passare il mouse sui componenti per visualizzare lo stato e altri dettagli.

È possibile visualizzare diversi tipi di informazioni:

- [Informazioni sui controller](#)
- [Informazioni sugli shelf di dischi](#)
- [Informazioni sugli switch storage](#)

3. A partire da ONTAP 9.12.1, è possibile visualizzare le informazioni sul cablaggio in Gestione sistema. Fare clic sulla casella di controllo **Mostra cavi** per visualizzare il cablaggio, quindi passare il mouse su un cavo per visualizzare le informazioni di connettività.

- [Informazioni sul cablaggio](#)

### **Informazioni sui controller**

È possibile visualizzare quanto segue:

## Nodi

### Nodi:

- È possibile visualizzare la vista anteriore e posteriore.
- Per i modelli con shelf di dischi interno, è anche possibile visualizzare il layout del disco nella vista frontale.
- È possibile visualizzare le seguenti piattaforme:

Piattaforma	Supportato in Gestione di sistema nella versione ONTAP...						
	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9.8 (solo modalità di anteprima)
AFF A150	Sì	Sì					
AFF A220	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AFF A250	Sì	Sì	Sì	Sì	Sì	Sì	
AFF A300	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AFF A320	Sì	Sì	Sì	Sì	Sì	Sì	
AFF A400	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AFF A700	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AFF A700	Sì	Sì	Sì	Sì	Sì	Sì	
AFF A800	Sì	Sì	Sì	Sì	Sì	Sì	
AFF C190	Sì	Sì	Sì	Sì	Sì	Sì	Sì
AFF C250	Sì	Sì	Sì e#42;	Sì e#42;	Sì e#42;		
AFF C400	Sì	Sì	Sì e#42;	Sì e#42;	Sì e#42;		
AFF C800	Sì	Sì	Sì e#42;	Sì e#42;	Sì e#42;		
ASAA150	Sì	Sì					
ASAA250	Sì	Sì					
ASAA400	Sì	Sì					

ASA A800	Sì	Sì					
ASA A900	Sì	Sì					
ASA C250	Sì	Sì					
ASA C400	Sì	Sì					
ASA C800	Sì	Sì					
FAS500f	Sì	Sì	Sì	Sì	Sì	Sì	
FAS2720	Sì	Sì	Sì	Sì			
FAS2750	Sì	Sì	Sì	Sì			
FAS8300	Sì	Sì	Sì	Sì			
FAS8700	Sì	Sì	Sì	Sì			
FAS9000	Sì	Sì	Sì	Sì			
FAS9500	Sì	Sì	Sì	Sì			

## Porte

### Porte:

- Se la porta non è disponibile, viene evidenziata in rosso.
- Quando si passa il puntatore del mouse sulla porta, è possibile visualizzare lo stato di una porta e altri dettagli.
- Non è possibile visualizzare le porte della console.

### Note:

- Per ONTAP 9.10.1 e versioni precedenti, le porte SAS vengono evidenziate in rosso quando sono disattivate.
- A partire da ONTAP 9.11.1, le porte SAS verranno evidenziate in rosso solo se si trovano in uno stato di errore o se una porta cablata utilizzata diventa offline. Le porte vengono visualizzate in bianco se non sono in linea e non sono cablate.

## FRU

### FRU:

Le informazioni sulle FRU vengono visualizzate solo quando lo stato di una FRU non è ottimale.

- PSU guasti nei nodi o nello chassis.

- Temperature elevate rilevate nei nodi.
- Ventole guaste sui nodi o sullo chassis.

#### Schede adattatore

##### Schede adattatore:

- Se sono state inserite schede esterne, negli slot vengono visualizzati i campi relativi ai numeri di parte definiti.
- Le porte vengono visualizzate sulle schede.
- Per una scheda supportata, è possibile visualizzare le immagini di tale scheda. Se la scheda non è presente nell'elenco dei codici prodotto supportati, viene visualizzata una grafica generica.

## Informazioni sugli shelf di dischi

È possibile visualizzare quanto segue:

#### Shelf di dischi

##### Shelf di dischi:

- È possibile visualizzare le viste anteriore e posteriore.
- È possibile visualizzare i seguenti modelli di shelf di dischi:

Se il sistema è in esecuzione...	Quindi, è possibile utilizzare System Manager per visualizzare...
ONTAP 9.9.1 e versioni successive	Tutti gli shelf che <i>non</i> sono stati designati come "fine del servizio" o "fine della disponibilità"
ONTAP 9.8	DS4243, DS486, DS212C, DS2246, DS224C, E NS224

#### Porte per shelf

##### Porte shelf:

- È possibile visualizzare lo stato della porta.
- Se la porta è collegata, è possibile visualizzare le informazioni sulla porta remota.

#### FRU dello shelf

##### FRU shelf:

- Vengono visualizzate le informazioni relative al guasto della PSU.

## Informazioni sugli switch storage

È possibile visualizzare quanto segue:

## Switch storage

### Switch storage:

- Il display mostra gli switch che fungono da switch storage utilizzati per collegare gli shelf ai nodi.
- A partire da ONTAP 9.9.1, System Manager visualizza le informazioni relative a uno switch che agisce sia come switch storage che come cluster, che possono essere condivise anche tra i nodi di una coppia ha.
- Vengono visualizzate le seguenti informazioni:
  - Nome dello switch
  - Indirizzo IP
  - Numero di serie
  - Versione SNMP
  - Versione del sistema
- È possibile visualizzare i seguenti modelli di switch storage:

Se il sistema è in esecuzione...	Quindi, è possibile utilizzare System Manager per visualizzare...
ONTAP 9.11.1 o versione successiva	Cisco Nexus 3232C Cisco Nexus 9336C-FX2 Mellanox SN2100
ONTAP 9.9.1 e 9.10.1	Cisco Nexus 3232C Cisco Nexus 9336C-FX2
ONTAP 9.8	Cisco Nexus 3232C

## Porte dello switch di storage

### Porte dello switch di storage

- Vengono visualizzate le seguenti informazioni:
  - Nome dell'identità
  - Indice di identità
  - Stato
  - Connessione remota
  - Altri dettagli

## Informazioni sul cablaggio

A partire da ONTAP 9.12.1, è possibile visualizzare le seguenti informazioni sul cablaggio:

- **Cablaggio** tra controller, switch e shelf quando non vengono utilizzati bridge di storage
- **Connettività** che mostra gli ID e gli indirizzi MAC delle porte su entrambe le estremità del cavo



## Gestire i nodi con System Manager

Con System Manager è possibile aggiungere nodi a un cluster e rinominarli. È inoltre possibile riavviare, sostituire e restituire i nodi.

### Aggiungere nodi a un cluster

È possibile aumentare le dimensioni e le funzionalità del cluster aggiungendo nuovi nodi.

#### Prima di iniziare

I nuovi nodi dovrebbero essere già stati cablati al cluster.

#### A proposito di questa attività

Esistono procedure separate per l'utilizzo di Gestione sistema in ONTAP 9,7 o ONTAP 9,8 e versioni successive.

#### Procedura ONTAP 9,8 e successive

##### Aggiunta di nodi a un cluster con Gestione sistema (ONTAP 9,8 e versioni successive)

###### Fasi

1. Selezionare **Cluster > Overview** (Cluster > Panoramica).

I nuovi controller vengono visualizzati come nodi collegati alla rete del cluster ma non nel cluster.

2. Selezionare **Aggiungi**.
  - I nodi vengono aggiunti al cluster.
  - Lo storage viene allocato implicitamente.

#### Procedura ONTAP 9,7

##### Aggiunta di nodi a un cluster con Gestione sistema (ONTAP 9,7)

###### Fasi


1. Selezionare **(ritorna alla versione classica)**.
2. Selezionare **configurazioni > espansione cluster**.

System Manager rileva automaticamente i nuovi nodi.
3. Selezionare **passa alla nuova esperienza**.
4. Selezionare **Cluster > Overview** per visualizzare i nuovi nodi.

### Arrestare, riavviare o modificare il Service Processor

Al riavvio o all'arresto di un nodo, il partner ha eseguito automaticamente un takeover.

#### Fasi

1. Selezionare **Cluster > Overview** (Cluster > Panoramica).
2. In **nodi**, selezionare .
3. Selezionare il nodo, quindi selezionare **Arresta il sistema, Riavvia o Modifica Service Processor**.


Se un nodo è stato riavviato ed è in attesa di giveback, è disponibile anche l'opzione **Giveback**.

Se si seleziona **Modifica Service Processor**, è possibile scegliere **Manuale** per immettere l'indirizzo IP, la maschera di sottorete e il gateway oppure è possibile scegliere **DHCP** per la configurazione dinamica dell'host.

## Rinomina nodi

A partire da ONTAP 9.14.1, è possibile rinominare un nodo dalla pagina di panoramica del cluster.

### Fasi

1. Selezionare **Cluster**. Viene visualizzata la pagina di panoramica del cluster.
2. Scorri verso il basso fino alla sezione **nodi**.
3. Accanto al nodo che si desidera rinominare, selezionare  e selezionare **Rinomina**.
4. Modificare il nome del nodo, quindi selezionare **Rinomina**.

## Gestione delle licenze

### Panoramica delle licenze ONTAP

Una licenza è un record di una o più autorizzazioni software. A partire da ONTAP 9.10.1, tutte le licenze vengono fornite come file di licenza NetApp (NLF), che è un singolo file che abilita più funzioni. A partire da maggio 2023, tutti i sistemi AFF (sia A-series che C-series) e i sistemi FAS vengono venduti con la suite software ONTAP One o la suite software ONTAP base; a partire da giugno 2023, tutti i sistemi ASA vengono venduti con ONTAP One per SAN. Ogni suite software viene fornita come un unico NLF, sostituendo i pacchetti NLF separati introdotti per la prima volta in ONTAP 9.10.1.

### Licenze incluse con ONTAP ONE

ONTAP One contiene tutte le funzionalità disponibili con licenza. Contiene una combinazione dei contenuti del precedente bundle Core, del bundle Data Protection, del bundle Security and Compliance, del bundle Hybrid Cloud e del bundle Encryption, come mostrato nella tabella. La crittografia non è disponibile nei paesi con restrizioni.

Nome del bundle precedente	Chiavi ONTAP incluse
Bundle principale	FlexClone
	SnapRestore
	NFS, SMB, S3
	FC, iSCSI
	NVME-of
Bundle di sicurezza e conformità	Protezione ransomware autonoma
	MTKM
	SnapLock

Bundle di data Protection	SnapMirror (asincrono, sincrono, business continuity)
	SnapCenter
	S3 SnapMirror per destinazioni NetApp
Bundle cloud ibrido	SnapMirror Cloud
	S3 SnapMirror per destinazioni non NetApp
Bundle di crittografia	Crittografia dei volumi NetApp
	Modulo Trusted Platform

## Licenze non incluse in ONTAP ONE

ONTAP One non include i servizi erogati nel cloud di NetApp, come ad esempio:

- Tiering BlueXP
- Cloud Insights
- Backup BlueXP
- Governance dei dati

## ONTAP uno per i sistemi esistenti

Se si dispone di sistemi esistenti che sono attualmente supportati da NetApp ma non sono stati aggiornati a ONTAP One, le licenze esistenti su tali sistemi sono ancora valide e continuano a funzionare come previsto. Ad esempio, se la licenza SnapMirror è già installata su sistemi esistenti, non è necessario eseguire l'aggiornamento a ONTAP One per ottenere una nuova licenza SnapMirror. Tuttavia, se non si dispone di una licenza SnapMirror installata su un sistema esistente, l'unico modo per ottenere tale licenza è eseguire l'aggiornamento a ONTAP One a un costo aggiuntivo.

A partire da giugno 2023, è possibile utilizzare anche i sistemi ONTAP che utilizzano chiavi di licenza di 28 caratteri "[Eseguire l'aggiornamento al bundle di compatibilità ONTAP One o ONTAP base](#)".

## Licenze incluse con ONTAP base

ONTAP base è una suite software opzionale alternativa a ONTAP One per i sistemi ONTAP. È per casi d'utilizzo specifici in cui non sono richieste tecnologie di data Protection come SnapMirror e SnapCenter, nonché funzionalità di sicurezza come il ransomware autonomo, come i sistemi non di produzione per ambienti di test o sviluppo dedicati. Non è possibile aggiungere licenze aggiuntive alla ONTAP base. Per licenze aggiuntive, come SnapMirror, è necessario eseguire l'aggiornamento a ONTAP One.

Nome del bundle precedente	Chiavi ONTAP incluse
Bundle principale	FlexClone
	SnapRestore
	NFS, SMB, S3
	FC, iSCSI
	NVME-of

Bundle di crittografia	Crittografia dei volumi NetApp
	Modulo Trusted Platform

## Licenze incluse in ONTAP One per SAN

ONTAP One per SAN è disponibile per i sistemi ASA serie A e C-series. Questa è l'unica suite software disponibile per SAN. ONTAP ONE per SAN contiene le seguenti licenze:

Chiavi ONTAP incluse
FlexClone
SnapRestore
FC, iSCSI
NVME-of
MTKM
SnapLock
SnapMirror (asincrono, sincrono, business continuity)
SnapCenter
SnapMirror Cloud
Crittografia dei volumi NetApp
Modulo Trusted Platform

## Altri metodi di distribuzione delle licenze

In ONTAP 8.2 fino a ONTAP 9.9.1, le chiavi di licenza vengono fornite sotto forma di stringhe di 28 caratteri ed è disponibile una chiave per funzione ONTAP. Utilizzare l'interfaccia CLI di ONTAP per installare le chiavi di licenza se si utilizza ONTAP 8,2 tramite ONTAP 9,9.1.



ONTAP 9.10.1 supporta l'installazione di chiavi di licenza di 28 caratteri utilizzando Gestione di sistema o CLI. Tuttavia, se è installata una licenza NLF per una funzione, non è possibile installare una chiave di licenza di 28 caratteri sul file di licenza NetApp per la stessa funzione. Per informazioni sull'installazione di NLF o chiavi di licenza con System Manager, vedere ["Installare le licenze ONTAP"](#).

## Informazioni correlate

["Come ottenere una licenza ONTAP One quando il sistema dispone già di NLF"](#)

["Come verificare le autorizzazioni software ONTAP e le relative chiavi di licenza utilizzando il sito di assistenza"](#)

["NetApp: Stato del rischio di licenza ONTAP"](#)

## Scaricare i file di licenza NetApp (NLF) dal sito del supporto NetApp

Se il sistema esegue ONTAP 9.10.1 o versione successiva, è possibile aggiornare i file di licenza bundle sui sistemi esistenti scaricando NLF per ONTAP ONE o ONTAP Core dal

sito di supporto NetApp.



Le licenze SnapMirror Cloud e S3 SnapMirror non sono incluse in ONTAP ONE. Fanno parte del pacchetto di compatibilità ONTAP One, che è possibile ottenere gratuitamente se si dispone di ONTAP One e. "[da richiedere separatamente](#)".

## Fasi

È possibile scaricare i file di licenza di ONTAP ONE per sistemi con pacchetti di file di licenza NetApp esistenti e per sistemi con chiavi di licenza di 28 caratteri che sono stati convertiti in file di licenza NetApp su sistemi che eseguono ONTAP 9.10.1 e versioni successive. A pagamento, puoi anche aggiornare i sistemi da ONTAP base a ONTAP One.

### Aggiornare l'NLF esistente

1. Contatta il tuo team di vendita NetApp e richiedi il bundle del file di licenza che desideri aggiornare o convertire (ad esempio, da ONTAP base a ONTAP One o bundle core e data Protection in ONTAP One).

Una volta elaborata la richiesta, l'utente riceverà un'e-mail da [netappsw@netapp.com](mailto:netappsw@netapp.com) con l'oggetto "notifica della licenza software NetApp per SO# [numero SO]" e l'e-mail includerà un allegato PDF che include il numero di serie della licenza.

2. Accedere a. "[Sito di supporto NetApp](#)".
3. Selezionare **sistemi > licenze software**.
4. Dal menu, scegliere **numero di serie**, inserire il numero di serie ricevuto e fare clic su **Nuova ricerca**.
5. Individuare il pacchetto di licenze che si desidera convertire.
6. Fare clic su **Ottieni file di licenza NetApp** per ogni pacchetto di licenze e scaricare i file NLF quando sono disponibili.
7. "[Installare](#)" Il file ONTAP ONE.

### Aggiornamento NLF convertito dalla chiave di licenza

1. Accedere a. "[Sito di supporto NetApp](#)".
2. Selezionare **sistemi > licenze software**.
3. Dal menu, scegliere **numero di serie**, inserire il numero di serie del sistema e fare clic su **Nuova ricerca**.
4. Individuare la licenza che si desidera convertire e, nella colonna **idoneità**, fare clic su **Controlla**.
5. In **Check Eligibility Form**, fare clic su **generate Licenses for 9,10.x e versioni successive**.
6. Chiudere il modulo **verifica idoneità**.

È necessario attendere almeno 2 ore per la generazione delle licenze.

7. Ripetere i passaggi da 1 a 3.
8. Individuare la licenza di ONTAP One, fare clic su **Ottieni file di licenza NetApp** e scegliere il metodo di distribuzione.
9. "[Installare](#)" Il file ONTAP ONE.

## Installare le licenze ONTAP

È possibile installare i file di licenza NetApp (NLF) e le chiavi di licenza utilizzando Gestione sistema, il metodo preferito per l'installazione di NLF, oppure utilizzare la CLI di ONTAP per installare le chiavi di licenza. In ONTAP 9.10.1 e versioni successive, le funzioni sono abilitate con un file di licenza NetApp e nelle versioni precedenti a ONTAP 9.10.1, le funzioni ONTAP sono abilitate con chiavi di licenza.

### Fasi

Se lo hai già fatto ["File di licenza NetApp scaricati"](#) O chiavi di licenza, puoi usare System Manager o la CLI di ONTAP per installare NLF e chiavi di licenza di 28 caratteri.

#### Gestione di sistema - ONTAP 9,8 e versioni successive

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. In **licenze**, selezionare ➔.
3. Selezionare **Sfoglia**. Scegliere il file di licenza NetApp scaricato.
4. Se si desidera aggiungere chiavi di licenza, selezionare **Usa chiavi di licenza di 28 caratteri e** immettere le chiavi.

#### Gestore di sistema - ONTAP 9,7 e versioni precedenti

1. Selezionare **Configurazione > Cluster > licenze**.
2. In **licenze**, selezionare ➔.
3. Nella finestra **pacchetti**, fare clic su **Aggiungi**.
4. Nella finestra di dialogo **Aggiungi pacchetti di licenza**, fare clic su **Scegli file** per selezionare il file di licenza NetApp scaricato, quindi fare clic su **Aggiungi** per caricare il file nel cluster.

### CLI

1. Aggiungere una o più chiavi di licenza:

```
system license add
```

Nell'esempio seguente vengono installate le licenze dal nodo locale `"/mroot/etc/lic_file"` se il file esiste in questa posizione:

```
cluster1::> system license add -use-license-file true
```

Nell'esempio seguente viene aggiunto al cluster un elenco di licenze con le chiavi  
AA

```
cluster1::> system license add -license-code  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBB BBBB BBBB BBBB BBBB BBBB BBBB BBBB
```

## Informazioni correlate

["Pagina man per il comando di aggiunta della licenza di sistema"](#).

## Gestire le licenze ONTAP

Puoi utilizzare Gestione sistema o l'interfaccia CLI di ONTAP per visualizzare e gestire le licenze installate nel sistema, inclusa la visualizzazione del numero seriale della licenza, la verifica dello stato di una licenza e la rimozione di una licenza.

### Consente di visualizzare i dettagli di una licenza

#### Fasi

La modalità di visualizzazione dei dettagli di una licenza dipende dalla versione di ONTAP in uso e dall'utilizzo di System Manager o dell'interfaccia a riga di comando di ONTAP.

#### Gestione di sistema - ONTAP 9,8 e versioni successive

1. Per visualizzare i dettagli relativi a una licenza di funzione specifica, selezionare **Cluster > Impostazioni**.
2. In **licenze**, selezionare ➔.
3. Selezionare **funzioni**.
4. Individuare la funzione concessa in licenza che si desidera visualizzare e selezionare ▼ per visualizzare i dettagli della licenza.

#### Gestore di sistema - ONTAP 9,7 e versioni precedenti

1. Selezionare **Configurazione > Cluster > licenze**.
2. Nella finestra **Licenses**, eseguire l'azione appropriata:
3. Fare clic sulla scheda **Dettagli**.

#### CLI

1. Visualizzare i dettagli relativi a una licenza installata:

```
system license show
```

### Eliminare una licenza

### Gestione di sistema - ONTAP 9,8 e versioni successive

1. Per eliminare una licenza, selezionare **Cluster > Impostazioni**.
2. In **licenze**, selezionare ➔.
3. Selezionare **funzioni**.
4. Selezionare la funzione concessa in licenza che si desidera eliminare e **Elimina chiave legacy**.

### Gestore di sistema - ONTAP 9,7 e versioni precedenti

1. Selezionare **Configurazione > Cluster > licenze**.
2. Nella finestra **Licenses**, eseguire l'azione appropriata:

Se si desidera...	Eseguire questa operazione...
Eliminare un pacchetto di licenza specifico su un nodo o una licenza master	Fare clic sulla scheda <b>Dettagli</b> .
Eliminare un pacchetto di licenza specifico in tutti i nodi del cluster	Fare clic sulla scheda <b>pacchetti</b> .

3. Selezionare il pacchetto di licenza software che si desidera eliminare, quindi fare clic su **Delete** (Elimina).

È possibile eliminare un solo pacchetto di licenza alla volta.

4. Selezionare la casella di controllo di conferma, quindi fare clic su **Elimina**.

### CLI

1. Eliminare una licenza:

```
system license delete
```

Nell'esempio riportato di seguito viene eliminata una licenza denominata CIFS e il numero di serie 1-81-000000000000000000123456 dal cluster:

```
cluster1::> system license delete -serial-number 1-81-  
000000000000000000123456 -package CIFS
```

Nell'esempio riportato di seguito vengono eliminate dal cluster tutte le licenze sotto il Core Bundle con licenza installata per il numero di serie 123456789:

```
cluster1::> system license delete { -serial-number 123456789  
-installed-license "Core Bundle" }
```

### Informazioni correlate



## Tipi di licenza e metodo concesso in licenza

La comprensione dei tipi di licenza e del metodo concesso in licenza consente di gestire le licenze in un cluster.

### Tipi di licenza

Un pacchetto può avere uno o più dei seguenti tipi di licenza installati nel cluster. Il `system license show` il comando visualizza il tipo o i tipi di licenza installati per un pacchetto.

- Licenza standard (`license`)

Una licenza standard è una licenza con blocco a nodo. Viene emesso per un nodo con un numero di serie di sistema specifico (noto anche come *numero di serie del controller*). Una licenza standard è valida solo per il nodo che ha il numero seriale corrispondente.

L'installazione di una licenza standard bloccata da nodo consente a un nodo di accedere alla funzionalità concessa in licenza. Affinché il cluster utilizzi la funzionalità concessa in licenza, è necessario che almeno un nodo sia concesso in licenza per tale funzionalità. L'utilizzo della funzionalità concessa in licenza su un nodo che non dispone di diritti per tale funzionalità potrebbe essere fuori conformità.

- Licenza del sito (`site`)

Una licenza di sito non è legata a un numero seriale di sistema specifico. Quando si installa una licenza di sito, tutti i nodi del cluster hanno diritto alla funzionalità concessa in licenza. Il `system license show` il comando visualizza le licenze del sito sotto il numero di serie del cluster.

Se il cluster dispone di una licenza di sito e si rimuove un nodo dal cluster, il nodo non dispone della licenza di sito e non ha più diritto alla funzionalità concessa in licenza. Se si aggiunge un nodo a un cluster che dispone di una licenza di sito, il nodo avrà automaticamente diritto alla funzionalità concessa dalla licenza di sito.

- Licenza di valutazione (`demo`)

Una licenza di valutazione è una licenza temporanea che scade dopo un determinato periodo di tempo (indicato da `system license show` comando). Consente di provare alcune funzionalità software senza acquistare alcun diritto. Si tratta di una licenza a livello di cluster e non è legata a un numero seriale specifico di un nodo.

Se il cluster dispone di una licenza di valutazione per un pacchetto e si rimuove un nodo dal cluster, il nodo non dispone della licenza di valutazione.

### Metodo concesso in licenza

È possibile installare sia una licenza a livello di cluster (il `site` oppure `demo` e una licenza bloccata dal nodo (il `license` digitare) per un pacchetto. Pertanto, un pacchetto installato può avere diversi tipi di licenza nel cluster. Tuttavia, per il cluster, esiste un solo *metodo concesso in licenza* per un pacchetto. Il `licensed method` campo di `system license status show` il comando visualizza i diritti utilizzati per un pacchetto. Il comando determina il metodo concesso in licenza come segue:

- Se un pacchetto ha un solo tipo di licenza installato nel cluster, il tipo di licenza installato è il metodo concesso in licenza.
- Se un pacchetto non dispone di licenze installate nel cluster, il metodo concesso in licenza è `none`.
- Se nel cluster sono installati più tipi di licenza, il metodo concesso in licenza viene determinato nel seguente ordine di priorità del tipo di licenza: `site`, `license`, e `demo`.

Ad esempio:

- Se si dispone di una licenza per sito, di una licenza standard e di una licenza di valutazione per un pacchetto, il metodo concesso in licenza per il pacchetto nel cluster è `site`.
- Se si dispone di una licenza standard e di una licenza di valutazione per un pacchetto, il metodo concesso in licenza per il pacchetto nel cluster è `license`.
- Se si dispone solo di una licenza di valutazione per un pacchetto, il metodo concesso in licenza per il pacchetto nel cluster è `demo`.

## Comandi per la gestione delle licenze

È possibile utilizzare l'interfaccia CLI di ONTAP `system license` comandi per gestire le licenze delle funzioni per il cluster. Si utilizza `system feature-usage` comandi per monitorare l'utilizzo delle funzioni.

Nella tabella seguente sono elencati alcuni dei comandi CLI più comuni per la gestione delle licenze e i collegamenti alle pagine man dei comandi per ulteriori informazioni.

Se si desidera...	Utilizzare questo comando...
Visualizzare tutti i pacchetti che richiedono licenze e il relativo stato di licenza corrente, inclusi i seguenti: <ul style="list-style-type: none"> <li>• Il nome del pacchetto</li> <li>• Il metodo concesso in licenza</li> <li>• La data di scadenza, se applicabile</li> </ul>	<a href="#">"stato di visualizzazione della licenza di sistema"</a>
Visualizzare o rimuovere le licenze scadute o inutilizzate	<a href="#">"pulizia della licenza di sistema"</a>
Visualizza il riepilogo dell'utilizzo delle funzionalità nel cluster in base al nodo	<a href="#">"riepilogo delle funzioni del sistema"</a>
Visualizzazione dello stato di utilizzo delle funzioni nel cluster per nodo e per settimana	<a href="#">"cronologia degli eventi di utilizzo delle funzioni del sistema"</a>

Se si desidera...	Utilizzare questo comando...
Visualizzare lo stato del rischio di licenza per ciascun pacchetto di licenza	<a href="#">"diritti della licenza di sistema-risk show"</a>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

["Articolo della Knowledge base: Panoramica sulle licenze di ONTAP 9.10.1 e versioni successive"](#)

["Utilizzare Gestione sistema per installare un file di licenza NetApp"](#)

## Gestione del cluster con la CLI

### Panoramica sull'amministrazione con la CLI

È possibile amministrare i sistemi ONTAP con l'interfaccia a riga di comando (CLI). È possibile utilizzare le interfacce di gestione di ONTAP, accedere al cluster, gestire i nodi e molto altro ancora.

Attenersi alle seguenti procedure nei seguenti casi:

- Vuoi conoscere la gamma di funzionalità di amministratore di ONTAP.
- Si desidera utilizzare la CLI, non System Manager o uno strumento di scripting automatico.

#### Informazioni correlate

Per informazioni dettagliate sulla sintassi e l'utilizzo della CLI, consultare <http://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr/GUID-5CB10C70-AC11-41C0-8C16-B4D0DF916E9B.html> [Riferimento alla pagina di manuale di ONTAP 9"] documentazione.

## Amministratori di cluster e SVM

### Amministratori di cluster e SVM

Gli amministratori dei cluster amministrano l'intero cluster e le macchine virtuali dello storage (SVM, precedentemente note come Vserver) in esso contenute. Gli amministratori di SVM amministrano solo le proprie SVM di dati.

Gli amministratori dei cluster possono amministrare l'intero cluster e le relative risorse. Possono anche configurare le SVM dei dati e delegare l'amministrazione SVM agli amministratori SVM. Le funzionalità specifiche di cui dispongono gli amministratori dei cluster dipendono dai ruoli di controllo degli accessi. Per impostazione predefinita, un amministratore del cluster con il nome dell'account "admin" o il nome del ruolo dispone di tutte le funzionalità per la gestione del cluster e delle SVM.

Gli amministratori di SVM possono amministrare solo le proprie risorse di storage e di rete SVM, come volumi, protocolli, LIF e servizi. Le funzionalità specifiche di cui dispongono gli amministratori SVM dipendono dai ruoli di controllo degli accessi assegnati dagli amministratori del cluster.



L'interfaccia della riga di comando (CLI) di ONTAP continua a utilizzare il termine *Vserver* nell'output, e. `vserver` poiché il nome di un comando o di un parametro non è stato modificato.

## Gestire l'accesso a System Manager

È possibile attivare o disattivare l'accesso di un browser Web a System Manager. È inoltre possibile visualizzare il log di System Manager.

È possibile controllare l'accesso di un browser Web a System Manager utilizzando `vserver services web modify -name sysmgr -vserver cluster_name -enabled[true|false]`.

La registrazione di System Manager viene registrata in `/mroot/etc/log/mlog/sysmgr.log` File del nodo che ospita la LIF di gestione del cluster al momento dell'accesso a System Manager. È possibile visualizzare i file di log utilizzando un browser. Il log di Gestione sistema è incluso anche nei messaggi AutoSupport.

## Che cos'è il server di gestione del cluster

Il server di gestione del cluster, chiamato anche *adminSVM*, è un'implementazione SVM (Storage Virtual Machine) specializzata che presenta il cluster come una singola entità gestibile. Oltre a fungere da dominio amministrativo di livello più elevato, il server di gestione del cluster possiede risorse che non appartengono logicamente a una SVM di dati.

Il server di gestione del cluster è sempre disponibile sul cluster. È possibile accedere al server di gestione del cluster tramite la console o la LIF di gestione del cluster.

In caso di guasto della porta della rete domestica, la LIF di gestione del cluster esegue automaticamente il failover su un altro nodo del cluster. A seconda delle caratteristiche di connettività del protocollo di gestione in uso, il failover potrebbe essere notato o meno. Se si utilizza un protocollo senza connessione (ad esempio, SNMP) o si dispone di una connessione limitata (ad esempio HTTP), non si noterà il failover. Tuttavia, se si utilizza una connessione a lungo termine (ad esempio SSH), sarà necessario riconnettersi al server di gestione del cluster dopo il failover.

Quando si crea un cluster, vengono configurate tutte le caratteristiche della LIF di gestione del cluster, inclusi l'indirizzo IP, la netmask, il gateway e la porta.

A differenza di un SVM di dati o di un SVM di nodo, un server di gestione del cluster non dispone di un volume root o di volumi utente host (anche se può ospitare volumi di sistema). Inoltre, un server di gestione del cluster può avere solo LIF del tipo di gestione del cluster.

Se si esegue `vserver show` il server di gestione del cluster viene visualizzato nell'elenco di output del comando.

## Tipi di SVM

Un cluster è costituito da quattro tipi di SVM, che consentono di gestire il cluster, le sue risorse e l'accesso ai dati ai client e alle applicazioni.

Un cluster contiene i seguenti tipi di SVM:

- SVM amministratore

Il processo di installazione del cluster crea automaticamente la SVM amministrativa per il cluster. La SVM amministrativa rappresenta il cluster.

- SVM del nodo

Un nodo SVM viene creato quando il nodo si unisce al cluster e il nodo SVM rappresenta i singoli nodi del cluster.

- SVM di sistema (avanzato)

Viene creata automaticamente una SVM di sistema per le comunicazioni a livello di cluster in un IPSpace.

- SVM dei dati

Un SVM di dati rappresenta i dati che servono le SVM. Dopo la configurazione del cluster, un amministratore del cluster deve creare SVM di dati e aggiungere volumi a queste SVM per facilitare l'accesso ai dati dal cluster.

Un cluster deve disporre di almeno una SVM di dati per fornire i dati ai propri client.



Se non diversamente specificato, il termine SVM si riferisce a una SVM (data-serving).

Nella CLI, le SVM vengono visualizzate come Vserver.

## Accedere al cluster utilizzando la CLI (solo amministratori del cluster)

### Accedere al cluster utilizzando la porta seriale

È possibile accedere al cluster direttamente da una console collegata alla porta seriale di un nodo.

#### Fasi

1. Nella console, premere Invio.

Il sistema risponde con la richiesta di accesso.

2. Al prompt di accesso, eseguire una delle seguenti operazioni:

Per accedere al cluster con...	Immettere il seguente nome account...
L'account cluster predefinito	<b>admin</b>
Un account utente amministrativo alternativo	<i>username</i>

Il sistema risponde con la richiesta della password.

3. Immettere la password per l'account amministratore o amministrativo, quindi premere Invio.

### Accedere al cluster utilizzando SSH

È possibile inviare richieste SSH al cluster per eseguire attività amministrative. SSH è

attivato per impostazione predefinita.

### Di cosa hai bisogno

- È necessario disporre di un account utente configurato per l'utilizzo `ssh` come metodo di accesso.

Il `-application` del parametro `security login commands` specifica il metodo di accesso per un account utente. Il `security login` "[pagine man](#)" contengono informazioni aggiuntive.

- Se si utilizza un account utente di dominio Active Directory (ad) per accedere al cluster, è necessario configurare un tunnel di autenticazione per il cluster tramite una VM di storage abilitata CIFS e aggiungere anche l'account utente di dominio ad al cluster con `ssh` come metodo di accesso e `domain` come metodo di autenticazione.
- Se si utilizzano connessioni IPv6, IPv6 deve essere già configurato e abilitato sul cluster e i criteri firewall devono essere già configurati con gli indirizzi IPv6.

Il `network options ipv6 show` Il comando indica se IPv6 è attivato. Il `system services firewall policy show` visualizza i criteri del firewall.

### A proposito di questa attività

- È necessario utilizzare un client OpenSSH 5.7 o successivo.
- È supportato solo il protocollo SSH v2; SSH v1 non è supportato.
- ONTAP supporta un massimo di 64 sessioni SSH simultanee per nodo.

Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

- ONTAP supporta solo gli algoritmi di crittografia AES e 3DES (noti anche come *cifrari*) per SSH.

AES è supportato con 128, 192 e 256 bit di lunghezza della chiave. 3DES ha una lunghezza della chiave di 56 bit come nel DES originale, ma viene ripetuto tre volte.

- Quando la modalità FIPS è attiva, i client SSH devono negoziare con gli algoritmi a chiave pubblica ECDSA (Elliptic Curve Digital Signature Algorithm) per consentire la connessione.
- Se si desidera accedere all'interfaccia utente di ONTAP da un host Windows, è possibile utilizzare un'utilità di terze parti, ad esempio `putty`.
- Se si utilizza un nome utente Windows ad per accedere a ONTAP, utilizzare le stesse lettere maiuscole o minuscole utilizzate al momento della creazione del nome utente e del nome di dominio ad in ONTAP.

I nomi utente E i nomi di dominio AD non sono sensibili al maiuscolo/minuscolo. Tuttavia, i nomi utente ONTAP distinguono tra maiuscole e minuscole. La mancata corrispondenza tra il nome utente creato in ONTAP e il nome utente creato in ad comporta un errore di accesso.

### Opzioni di autenticazione SSH

- A partire da ONTAP 9.3, è possibile "[Abilitare l'autenticazione a più fattori SSH](#)" per gli account dell'amministratore locale.

Quando l'autenticazione a più fattori SSH è attivata, gli utenti vengono autenticati utilizzando una chiave pubblica e una password.

- A partire da ONTAP 9.4, è possibile ["Abilitare l'autenticazione a più fattori SSH"](#) Per utenti remoti LDAP e NIS.
- A partire da ONTAP 9.13.1, è possibile aggiungere facoltativamente la convalida del certificato al processo di autenticazione SSH per migliorare la sicurezza di accesso. A tal fine, ["Associare un certificato X.509 alla chiave pubblica"](#) utilizzato da un account. Se si accede utilizzando SSH sia con una chiave pubblica SSH che con un certificato X.509, ONTAP verifica la validità del certificato X.509 prima di autenticarsi con la chiave pubblica SSH. L'accesso SSH viene rifiutato se il certificato è scaduto o revocato e la chiave pubblica SSH viene disattivata automaticamente.
- A partire da ONTAP 9.14.1, è possibile aggiungere facoltativamente l'autenticazione a due fattori Cisco Duo al processo di autenticazione SSH per migliorare la sicurezza dell'accesso. Al primo accesso dopo aver attivato l'autenticazione Cisco Duo, gli utenti dovranno registrare un dispositivo per fungere da autenticatore per le sessioni SSH. Fare riferimento a. ["Configurare Cisco Duo 2FA per gli accessi SSH"](#) Per ulteriori informazioni sulla configurazione dell'autenticazione SSH Cisco Duo per ONTAP.

## Fasi

1. Da un host di amministrazione, immettere `ssh` comando in uno dei seguenti formati:

- `ssh username@hostname_or_IP [command]`
- `ssh -l username hostname_or_IP [command]`

Se si utilizza un account utente di dominio ad, è necessario specificare *username* nel formato di *domainname\AD\_accountname* (con barre rovesciate doppie dopo il nome di dominio) o. *"domainname\AD\_accountname"* (racchiuso tra virgolette doppie e con una barra rovesciata singola dopo il nome di dominio).

*hostname\_or\_IP* È il nome host o l'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi. Si consiglia di utilizzare la LIF di gestione del cluster. È possibile utilizzare un indirizzo IPv4 o IPv6.

*command* Non è richiesto per le sessioni interattive SSH.

## Esempi di richieste SSH

I seguenti esempi mostrano come l'account utente "joe" può emettere una richiesta SSH per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node           Health  Eligibility
-----
node1           true    true
node2           true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

I seguenti esempi mostrano come l'account utente "john" del dominio "DOMAIN1" può emettere una richiesta SSH per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

L'esempio seguente mostra come l'account utente "joe" può inviare una richiesta SSH MFA per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

## Informazioni correlate



## Sicurezza di accesso SSH

A partire da ONTAP 9.5, è possibile visualizzare le informazioni sugli accessi precedenti, i tentativi di accesso non riusciti e le modifiche ai privilegi dall'ultimo accesso riuscito.

Le informazioni relative alla sicurezza vengono visualizzate quando si effettua l'accesso come utente amministratore SSH. L'utente viene avvisato delle seguenti condizioni:

- L'ultima volta in cui è stato effettuato l'accesso al nome dell'account.
- Il numero di tentativi di accesso non riusciti dall'ultimo accesso riuscito.
- Se il ruolo è cambiato dall'ultimo accesso (ad esempio, se il ruolo dell'account admin è cambiato da "admin" a "backup").
- Se le funzionalità di aggiunta, modifica o eliminazione del ruolo sono state modificate dall'ultimo accesso.



Se una delle informazioni visualizzate è sospetta, contattare immediatamente il reparto di sicurezza.

Per ottenere queste informazioni al momento dell'accesso, devono essere soddisfatti i seguenti prerequisiti:

- Il provisioning dell'account utente SSH deve essere eseguito in ONTAP.
- È necessario creare l'accesso di sicurezza SSH.
- Il tentativo di accesso deve essere riuscito.

## Restrizioni e altre considerazioni per la sicurezza dell'accesso SSH

Le seguenti restrizioni e considerazioni si applicano alle informazioni di sicurezza per l'accesso SSH:

- Le informazioni sono disponibili solo per gli accessi basati su SSH.
- Per gli account admin basati su gruppo, come ad esempio gli account LDAP/NIS e ad, gli utenti possono visualizzare le informazioni di accesso SSH se il gruppo di cui fanno parte è configurato come account admin in ONTAP.

Tuttavia, gli avvisi relativi alle modifiche al ruolo dell'account utente non possono essere visualizzati per questi utenti. Inoltre, gli utenti appartenenti a un gruppo ad che è stato fornito come account admin in ONTAP non possono visualizzare il numero di tentativi di accesso non riusciti che si sono verificati dall'ultimo accesso.

- Le informazioni conservate per un utente vengono eliminate quando l'account utente viene cancellato da ONTAP.
- Le informazioni non vengono visualizzate per le connessioni ad applicazioni diverse da SSH.

## Esempi di informazioni di sicurezza per l'accesso SSH

I seguenti esempi mostrano il tipo di informazioni visualizzate dopo l'accesso.

- Questo messaggio viene visualizzato dopo ogni accesso riuscito:

```
Last Login : 7/19/2018 06:11:32
```

- Questi messaggi vengono visualizzati se si sono verificati tentativi di accesso non riusciti dall'ultimo accesso riuscito:

```
Last Login : 4/12/2018 08:21:26  
Unsuccessful login attempts since last login - 5
```

- Questi messaggi vengono visualizzati se si sono verificati tentativi di accesso non riusciti e i privilegi sono stati modificati dall'ultimo accesso riuscito:

```
Last Login : 8/22/2018 20:08:21  
Unsuccessful login attempts since last login - 3  
Your privileges have changed since last login
```

## Abilitare l'accesso Telnet o RSH al cluster

Come Best practice per la sicurezza, Telnet e RSH sono disattivati nella policy predefinita del firewall di gestione (mgmt). Per consentire al cluster di accettare richieste Telnet o RSH, è necessario creare un nuovo criterio firewall di gestione con Telnet o RSH attivato, quindi associare il nuovo criterio alla LIF di gestione del cluster.

### A proposito di questa attività

ONTAP impedisce di modificare le policy firewall predefinite, ma è possibile creare una nuova policy clonando quelle predefinite mgmt Policy del firewall di gestione, quindi abilitazione di Telnet o RSH in base alla nuova policy. Tuttavia, Telnet e RSH non sono protocolli sicuri, pertanto si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

Per abilitare l'accesso Telnet o RSH ai cluster, attenersi alla seguente procedura:

### Fasi

1. Accedere alla modalità avanzata dei privilegi:  
**set advanced**
2. Abilitare un protocollo di sicurezza (RSH o Telnet):  
**security protocol modify -application security\_protocol -enabled true**
3. Creare una nuova policy del firewall di gestione basata su mgmt policy del firewall di gestione:  
**system services firewall policy clone -policy mgmt -destination-policy policy-name**
4. Abilitare Telnet o RSH nella nuova policy del firewall di gestione:  
**system services firewall policy create -policy policy-name -service security\_protocol -action allow -ip-list ip\_address/netmask** Per consentire tutti gli indirizzi IP, specificare **-ip-list 0.0.0.0/0**
5. Associare la nuova policy alla LIF di gestione del cluster:  
**network interface modify -vserver cluster\_management\_LIF -lif cluster\_mgmt**

**-firewall-policy *policy-name***

## Accedere al cluster utilizzando Telnet

È possibile inviare richieste Telnet al cluster per eseguire attività amministrative. Telnet è disattivato per impostazione predefinita.

### Di cosa hai bisogno

Prima di poter utilizzare Telnet per accedere al cluster, è necessario soddisfare le seguenti condizioni:

- È necessario disporre di un account utente locale del cluster configurato per utilizzare Telnet come metodo di accesso.

Il `-application` del parametro `security login commands` specifica il metodo di accesso per un account utente. Per ulteriori informazioni, consultare `security login` pagine man.

- Telnet deve essere già attivato nel criterio del firewall di gestione utilizzato dalle LIF di gestione del cluster o dei nodi, in modo che le richieste Telnet possano passare attraverso il firewall.

Per impostazione predefinita, Telnet è disattivato. Il `system services firewall policy show` con il `-service telnet` Parametro indica se Telnet è stato attivato in un criterio firewall. Per ulteriori informazioni, consultare `system services firewall policy` pagine man.

- Se si utilizzano connessioni IPv6, IPv6 deve essere già configurato e abilitato sul cluster e i criteri firewall devono essere già configurati con gli indirizzi IPv6.

Il `network options ipv6 show` Il comando indica se IPv6 è attivato. Il `system services firewall policy show` visualizza i criteri del firewall.

### A proposito di questa attività

- Telnet non è un protocollo sicuro.

Si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

- ONTAP supporta un massimo di 50 sessioni Telnet simultanee per nodo.

Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

- Se si desidera accedere all'interfaccia utente di ONTAP da un host Windows, è possibile utilizzare un'utilità di terze parti, ad esempio putty.

### Fasi

1. Da un host di amministrazione, immettere il seguente comando:

```
telnet hostname_or_IP
```

*hostname\_or\_IP* È il nome host o l'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi. Si consiglia di utilizzare la LIF di gestione del cluster. È possibile utilizzare un indirizzo IPv4 o IPv6.

## Esempio di richiesta Telnet

L'esempio seguente mostra come l'utente "joe", configurato con accesso Telnet, può inviare una richiesta Telnet per accedere a un cluster la cui LIF di gestione del cluster è 10.72.137.28:

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

## Accedere al cluster utilizzando RSH

È possibile inviare richieste RSH al cluster per eseguire attività amministrative. RSH non è un protocollo sicuro ed è disattivato per impostazione predefinita.

### Di cosa hai bisogno

Prima di poter utilizzare RSH per accedere al cluster, è necessario soddisfare le seguenti condizioni:

- È necessario disporre di un account utente locale del cluster configurato per utilizzare RSH come metodo di accesso.

Il `-application` del parametro `security login commands` specifica il metodo di accesso per un account utente. Per ulteriori informazioni, consultare `security login` pagine man.

- RSH deve essere già abilitato nella policy del firewall di gestione utilizzata dalle LIF di gestione del cluster o dei nodi, in modo che le richieste RSH possano passare attraverso il firewall.

Per impostazione predefinita, RSH è disattivato. Il `system services firewall policy show` con il `-service rsh` Parametro indica se RSH è stato attivato in una policy firewall. Per ulteriori informazioni, consultare `system services firewall policy` pagine man.

- Se si utilizzano connessioni IPv6, IPv6 deve essere già configurato e abilitato sul cluster e i criteri firewall devono essere già configurati con gli indirizzi IPv6.

Il `network options ipv6 show` Il comando indica se IPv6 è attivato. Il `system services firewall policy show` visualizza i criteri del firewall.

### A proposito di questa attività

- RSH non è un protocollo sicuro.

Si consiglia di utilizzare SSH per accedere al cluster. SSH offre una shell remota sicura e una sessione di rete interattiva.

- ONTAP supporta un massimo di 50 sessioni RSH simultanee per nodo.

Se la LIF di gestione del cluster risiede nel nodo, condivide questo limite con la LIF di gestione del nodo.

Se la velocità delle connessioni in entrata è superiore a 10 al secondo, il servizio viene temporaneamente disattivato per 60 secondi.

## Fasi

1. Da un host di amministrazione, immettere il seguente comando:

```
rsh hostname_or_IP -l username:passwordcommand
```

*hostname\_or\_IP* È il nome host o l'indirizzo IP della LIF di gestione del cluster o di una LIF di gestione dei nodi. Si consiglia di utilizzare la LIF di gestione del cluster. È possibile utilizzare un indirizzo IPv4 o IPv6.

*command* È il comando che si desidera eseguire su RSH.

## Esempio di richiesta RSH

L'esempio seguente mostra come l'utente "joe", che è stato configurato con accesso RSH, può emettere una richiesta RSH per eseguire `cluster show` comando:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true

2 entries were displayed.

```
admin_host$
```

## Utilizzare l'interfaccia della riga di comando di ONTAP

### Utilizzando l'interfaccia della riga di comando di ONTAP

L'interfaccia a riga di comando (CLI) di ONTAP fornisce una vista basata su comandi dell'interfaccia di gestione. I comandi vengono immessi al prompt del sistema di storage e i risultati dei comandi vengono visualizzati in testo.

Il prompt dei comandi CLI è rappresentato come `cluster_name::>`.

Se si imposta il livello di privilegio (ovvero, l' `-privilege` del parametro `set` comando) a `advanced`, il prompt include un asterisco (\*), ad esempio:

```
cluster_name::*>
```

### Informazioni sulle diverse shell per i comandi CLI (solo amministratori del cluster)

Il cluster dispone di tre diverse shell per i comandi CLI, la *clustershell*, la *nodeshell* e la *systemshell*. Le shell hanno scopi diversi, ognuno dei quali ha un set di comandi diverso.

- La shell *clustershell* è la shell nativa che viene avviata automaticamente quando si accede al cluster.

Fornisce tutti i comandi necessari per configurare e gestire il cluster. La guida CLI della shell del

clustershell (attivata da ? al prompt di clustershell) visualizza i comandi disponibili di clustershell. Il `man command_name` il comando nella shell clustershell visualizza la pagina man del comando clustershell specificato.

- Il nodeshell è una shell speciale per i comandi che hanno effetto solo a livello di nodo.

Il nodeshell è accessibile attraverso `system node run` comando.

Il nodeshell CLI help (attivato da ? oppure `help` al prompt nodeshell) visualizza i comandi nodeshell disponibili. Il `man command_name` nel nodeshell viene visualizzata la pagina man del comando nodeshell specificato.

Molti comandi e opzioni nodeshell comunemente utilizzati sono tunneled o aliased nella clustershell e possono essere eseguiti anche dalla clustershell.

- Systemshell è una shell di basso livello che viene utilizzata solo per scopi di diagnostica e troubleshooting.

La shell di sistema e l'account associato "diag" sono destinati a scopi diagnostici di basso livello. Il loro accesso richiede il livello di privilegio diagnostico ed è riservato solo al supporto tecnico per eseguire le attività di risoluzione dei problemi.

### Accesso a comandi e opzioni nodeshell nella shell dei clustershell

I comandi e le opzioni di Nodeshell sono accessibili attraverso il nodeshell:

```
system node run -node nodename
```

Molti comandi e opzioni nodeshell comunemente utilizzati sono tunneled o aliased nella clustershell e possono essere eseguiti anche dalla clustershell.

È possibile accedere alle opzioni Nodeshell supportate nella shell clustershell utilizzando `vserver options clustershell` comando. Per visualizzare queste opzioni, è possibile effettuare una delle seguenti operazioni:

- Eseguire una query della CLI della shell del clustershell con `vserver options -vserver nodename_or_clustername -option-name ?`
- Accedere a `vserver options` Man page nella CLI della shell del clustershell con `man vserver options`

Se si immette un comando o un'opzione nodeshell o legacy nella clustershell e il comando o l'opzione ha un comando clustershell equivalente, ONTAP informa dell'utilizzo del comando clustershell.

Se si immette un comando o un'opzione legacy o nodeshell non supportato nella shell del clustershell, ONTAP indica lo stato "Not Supported" (non supportato) per il comando o l'opzione.

### Visualizza i comandi nodeshell disponibili

Puoi ottenere un elenco dei comandi nodeshell disponibili usando l'aiuto CLI del nodeshell.

#### Fasi

1. Per accedere al nodeshell, immettere il seguente comando al prompt di sistema della shell:

```
system node run -node {nodename|local}
```

local è il nodo utilizzato per accedere al cluster.



Il `system node run` il comando dispone di un comando alias, `run`.

2. Immettere il seguente comando nel nodeshell per visualizzare l'elenco dei comandi nodeshell disponibili:

**[*commandname*] help**

``_commandname_`` è il nome del comando di cui si desidera visualizzare la disponibilità. Se non si include ``_commandname_``, La CLI visualizza tutti i comandi nodeshell disponibili.

Viene immesso `exit` In alternativa, digitare `Ctrl-d` per tornare alla CLI della shell cluster.

### Esempio di visualizzazione dei comandi nodeshell disponibili

Nell'esempio seguente viene effettuato l'accesso al nodeshell di un nodo denominato `node2` e vengono visualizzate le informazioni relative al comando nodeshell `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

### Metodi per navigare nelle directory dei comandi CLI

I comandi nella CLI sono organizzati in una gerarchia in base alle directory dei comandi. È possibile eseguire i comandi nella gerarchia inserendo il percorso completo dei comandi o navigando nella struttura della directory.

Quando si utilizza l'interfaccia CLI, è possibile accedere alla directory dei comandi digitando il nome della directory al prompt e premendo Invio. Il nome della directory viene quindi incluso nel testo del prompt per indicare che si sta interagendo con la directory dei comandi appropriata. Per approfondire la gerarchia dei comandi, digitare il nome di una sottodirectory dei comandi, quindi premere Invio. Il nome della sottodirectory viene quindi incluso nel testo del prompt e il contesto viene spostato in tale sottodirectory.

È possibile navigare attraverso diverse directory di comandi immettendo l'intero comando. Ad esempio, è possibile visualizzare le informazioni relative ai dischi immettendo il `storage disk show` al prompt. È inoltre possibile eseguire il comando esplorando una directory di comandi alla volta, come illustrato nell'esempio seguente:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

È possibile abbreviare i comandi immettendo solo il numero minimo di lettere in un comando che rende il comando unico per la directory corrente. Ad esempio, per abbreviare il comando nell'esempio precedente, è possibile immettere `st d sh`. È inoltre possibile utilizzare il tasto Tab per espandere i comandi abbreviati e visualizzare i parametri di un comando, inclusi i valori dei parametri predefiniti.

È possibile utilizzare `top` per passare al livello superiore della gerarchia di comandi e `a. up` comando o `...` per salire di un livello nella gerarchia di comandi.



I comandi e le opzioni di comando preceduti da un asterisco (\*) nella CLI possono essere eseguiti solo a livello di privilegio avanzato o superiore.

## Regole per specificare i valori nella CLI

La maggior parte dei comandi include uno o più parametri obbligatori o opzionali. Molti parametri richiedono di specificare un valore per essi. Esistono alcune regole per specificare i valori nella CLI.

- Un valore può essere un numero, un identificatore booleano, una selezione da un elenco enumerato di valori predefiniti o una stringa di testo.

Alcuni parametri possono accettare un elenco separato da virgole di due o più valori. Gli elenchi di valori separati da virgole non devono essere tra virgolette (" "). Ogni volta che si specifica il testo, uno spazio o un carattere di query (quando non si intende una query o un testo che inizia con un simbolo minore o maggiore di), è necessario racchiudere l'entità tra virgolette.

- L'interfaccia CLI interpreta un punto interrogativo (" ? ") come comando per visualizzare le informazioni della guida per un determinato comando.
- Alcuni testi immessi nella CLI, come i nomi dei comandi, i parametri e alcuni valori, non fanno distinzione tra maiuscole e minuscole.

Ad esempio, quando si immettono i valori dei parametri per `vserver cifs` comandi, le maiuscole vengono ignorate. Tuttavia, la maggior parte dei valori dei parametri, come i nomi dei nodi, le macchine virtuali di storage (SVM), gli aggregati, i volumi e le interfacce logiche, è sensibile al maiuscolo/minuscolo.

- Se si desidera cancellare il valore di un parametro che prende una stringa o un elenco, specificare un set vuoto di virgolette (" ") o un trattino (" - ").
- Il simbolo cancelletto (" n. `"), noto anche come simbolo cancelletto, indica un commento per un input della riga di comando; se utilizzato, dovrebbe essere visualizzato dopo l'ultimo parametro in una riga di comando.

L'interfaccia CLI ignora il testo tra " n. `" e la fine della riga.

Nell'esempio seguente, viene creata una SVM con un commento di testo. La SVM viene quindi modificata per eliminare il commento:



```
cluster1::> vsserver create -vsserver vs0 -subtype default -rootvolume  
root_vs0  
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is-  
-repository false -ipSPACE ipSPACEA -comment "My SVM"  
cluster1::> vsserver modify -vsserver vs0 -comment ""
```

Nell'esempio seguente, un commento della riga di comando che utilizza il segno " n." indica la funzione del comando.

```
cluster1::> security login create -vsserver vs0 -user-or-group-name new-  
admin  
-application ssh -authmethod password #This command creates a new user  
account
```

### Metodi di visualizzazione della cronologia dei comandi e di reinvio dei comandi

Ogni sessione CLI conserva una cronologia di tutti i comandi in essa emessi. È possibile visualizzare la cronologia dei comandi della sessione corrente. È inoltre possibile emettere nuovamente i comandi.

Per visualizzare la cronologia dei comandi, è possibile utilizzare `history` comando.

Per rimettere un comando, è possibile utilizzare `redo` comando con uno dei seguenti argomenti:

- Stringa che corrisponde a parte di un comando precedente

Ad esempio, se solo `volume` il comando eseguito è `volume show`, è possibile utilizzare `redo volume` per eseguire nuovamente il comando.

- L'ID numerico di un comando precedente, come elencato dal `history` comando

Ad esempio, è possibile utilizzare `redo 4` comando per emettere nuovamente il quarto comando nell'elenco della cronologia.

- Offset negativo dalla fine dell'elenco della cronologia

Ad esempio, è possibile utilizzare `redo -2` comando per emettere nuovamente il comando eseguito due comandi fa.

Ad esempio, per ripetere il comando che è il terzo dalla fine della cronologia dei comandi, immettere il seguente comando:

```
cluster1::> redo -3
```

## Tasti di scelta rapida per la modifica dei comandi CLI

Il comando al prompt dei comandi corrente è il comando attivo. L'utilizzo dei tasti di scelta rapida consente di modificare rapidamente il comando attivo. Questi tasti di scelta rapida sono simili a quelli della shell UNIX `tcsh` e dell'editor `Emacs`.

La seguente tabella elenca i tasti di scelta rapida per la modifica dei comandi CLI. "Ctrl-" indica che si tiene premuto il tasto `Ctrl` mentre si digita il carattere specificato. "Esc-" indica che si preme e si rilascia il tasto `Esc`, quindi si digita il carattere specificato.

Se si desidera...	Utilizzare la seguente scelta rapida da tastiera...
Spostare il cursore indietro di un carattere	Ctrl-B.
Freccia indietro	Spostare il cursore in avanti di un carattere
Ctrl-F.	Freccia avanti
Spostare il cursore indietro di una parola	ESC-B.
Spostare il cursore in avanti di una parola	ESC-F.
Spostare il cursore all'inizio della riga	Ctrl-A.
Spostare il cursore alla fine della riga	Ctrl-E.
Rimuovere il contenuto della riga di comando dall'inizio della riga al cursore e salvarlo nel buffer di taglio. Il buffer cut agisce come una memoria temporanea, simile a quella che viene chiamata <i>clipboard</i> in alcuni programmi.	Ctrl-U
Rimuovere il contenuto della riga di comando dal cursore alla fine della riga e salvarlo nel buffer di taglio	Ctrl-K.
Rimuovere il contenuto della riga di comando dal cursore alla fine della parola seguente e salvarlo nel buffer di taglio	ESC-D
Rimuovere la parola prima del cursore e salvarla nel buffer di taglio	Ctrl-W.
Inserire il contenuto del buffer di taglio e inserirlo nella riga di comando del cursore	Ctrl-Y
Consente di eliminare il carattere che precede il cursore	Ctrl-H

Se si desidera...	Utilizzare la seguente scelta rapida da tastiera...
Backspace	Consente di eliminare il carattere in cui si trova il cursore
Ctrl-D	Eliminare la linea
Ctrl-C.	Cancellare lo schermo
Ctrl-L.	Sostituire il contenuto corrente della riga di comando con la voce precedente nell'elenco della cronologia.  Ad ogni ripetizione del tasto di scelta rapida, il cursore della cronologia passa alla voce precedente.
Ctrl-P.	ESC-P.
Freccia su	Sostituire il contenuto corrente della riga di comando con la voce successiva nell'elenco della cronologia. Ad ogni ripetizione del tasto di scelta rapida, il cursore della cronologia passa alla voce successiva.
Ctrl-N.	ESC-N.
Freccia giù	Espandere un comando o un elenco di input validi inseriti parzialmente dalla posizione di modifica corrente
Scheda	Ctrl-I.
Visualizza la guida sensibile al contesto	?
Escape the special mapping for the question mark (“?”) character. For instance, to enter a question mark into a command's argument, press Esc and then the “?” carattere.	ESC-?
Avviare l'output TTY	Ctrl-Q.
Interrompere l'output TTY	Ctrl-S.

### Utilizzo dei livelli di privilegio amministrativi

I comandi e i parametri ONTAP sono definiti a tre livelli di privilegio: *Admin*, *Advanced* e *Diagnostic*. I livelli di privilegio riflettono i livelli di competenza richiesti per l'esecuzione delle attività.

- **admin**

La maggior parte dei comandi e dei parametri è disponibile a questo livello. Vengono utilizzati per attività comuni o di routine.

- **avanzato**

I comandi e i parametri di questo livello vengono utilizzati raramente, richiedono conoscenze avanzate e possono causare problemi se utilizzati in modo non appropriato.

I comandi o i parametri avanzati vengono utilizzati solo con la consulenza del personale di supporto.

- **diagnostica**

I comandi e i parametri diagnostici possono causare interruzioni. Vengono utilizzati solo dal personale di supporto per diagnosticare e risolvere i problemi.

## **Impostare il livello di privilegio nella CLI**

È possibile impostare il livello di privilegio nella CLI utilizzando `set` comando. Le modifiche alle impostazioni del livello di privilegio si applicano solo alla sessione in corso. Non sono persistenti tra le sessioni.

### **Fasi**

1. Per impostare il livello di privilegio nella CLI, utilizzare `set` con il `-privilege` parametro.

### **Esempio di impostazione del livello di privilegio**

Nell'esempio seguente viene impostato il livello di privilegio su Advanced (avanzato) e quindi su admin (admin):

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

## **Impostare le preferenze di visualizzazione nella CLI**

È possibile impostare le preferenze di visualizzazione per una sessione CLI utilizzando `set` comando e `rows` comando. Le preferenze impostate si applicano solo alla sessione in cui ci si trova. Non sono persistenti tra le sessioni.

### **A proposito di questa attività**

È possibile impostare le seguenti preferenze di visualizzazione CLI:

- Il livello di privilegio della sessione di comando
- Se vengono emesse conferme per comandi potenzialmente disgregativi
- Se `show` i comandi visualizzano tutti i campi
- Il carattere o i caratteri da utilizzare come separatore di campo

- L'unità predefinita quando si riferiscono le dimensioni dei dati
- Il numero di righe visualizzate nella sessione CLI corrente prima che l'interfaccia sospende l'output

Se il numero preferito di righe non viene specificato, viene regolato automaticamente in base all'altezza effettiva del terminale. Se l'altezza effettiva non è definita, il numero predefinito di righe è 24.

- La SVM (Storage Virtual Machine) o il nodo predefinito
- Se un comando che continua deve arrestarsi in caso di errore

## Fasi

1. Per impostare le preferenze di visualizzazione CLI, utilizzare `set` comando.

Per impostare il numero di righe visualizzate nella sessione CLI corrente, è possibile utilizzare anche il `rows` comando.

Per ulteriori informazioni, consultare le pagine man del `set` comando e `rows` comando.

## Esempio di impostazione delle preferenze di visualizzazione nella CLI

Nell'esempio seguente viene impostata una virgola come separatore di campo, `set GB` come unità predefinita per la dimensione dei dati e imposta il numero di righe su 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

## Metodi di utilizzo degli operatori di query

L'interfaccia di gestione supporta query e modelli in stile UNIX e caratteri jolly per consentire la corrispondenza di più valori negli argomenti dei parametri di comando.

La seguente tabella descrive gli operatori di query supportati:

Operatore	Descrizione
*	Carattere jolly che corrisponde a tutte le voci.  Ad esempio, il comando <code>volume show -volume *tmp*</code> visualizza un elenco di tutti i volumi i cui nomi includono la stringa <code>tmp</code> .
!	NON operatore.  Indica un valore che non deve essere associato; ad esempio, <code>!vs0</code> indica di non corrispondere al valore <code>vs0</code> .

Operatore	Descrizione
O operatore .	vs2*` corrisponde a vs0 o vs2. È possibile specificare più istruzioni OR, ad esempio `a  Separa due valori da confrontare; ad esempio, `*vs0
b*	*c*` corrisponde alla voce a, qualsiasi voce che inizia con b`e qualsiasi voce che includa `c.
..	Operatore del raggio d'azione.  Ad esempio, 5 . .10 corrisponde a qualsiasi valore da 5 a. 10, incluso.
<	Meno dell'operatore.  Ad esempio, <20 corrisponde a qualsiasi valore inferiore a. 20.
>	Maggiore rispetto all'operatore.  Ad esempio, >5 corrisponde a qualsiasi valore maggiore di 5.
≤	Minore o uguale all'operatore.  Ad esempio, ≤5 corrisponde a qualsiasi valore minore o uguale a. 5.
≥	Maggiore o uguale all'operatore.  Ad esempio, ≥5 corrisponde a qualsiasi valore maggiore o uguale a. 5.
{query}	Query estesa.  Una query estesa deve essere specificata come primo argomento dopo il nome del comando, prima di qualsiasi altro parametro.  Ad esempio, il comando <code>volume modify {-volume *tmp*} -state offline</code> imposta offline tutti i volumi i cui nomi includono la stringa tmp.

Se si desidera analizzare i caratteri di query come valori letterali, è necessario racchiudere i caratteri tra virgolette doppie (ad esempio, "<10", "0 . .100", "\*abc\*", o "a|b") per restituire i risultati corretti.

È necessario racchiudere i nomi dei file raw tra virgolette doppie per impedire l'interpretazione di caratteri speciali. Questo vale anche per i caratteri speciali utilizzati dalla shell.

È possibile utilizzare più operatori di query in un'unica riga di comando. Ad esempio, il comando `volume show -size >1GB -percent-used <50 -vserver !vs1` Visualizza tutti i volumi con dimensioni superiori a 1 GB, meno del 50% utilizzati e non nella macchina virtuale di storage (SVM) denominata "vs1".

#### Informazioni correlate

["Tasti di scelta rapida per la modifica dei comandi CLI"](#)

#### Metodi di utilizzo delle query estese

È possibile utilizzare query estese per associare ed eseguire operazioni sugli oggetti che hanno valori specificati.

Le query estese vengono specificate racchiudendole tra parentesi graffe (`{}`). Una query estesa deve essere specificata come primo argomento dopo il nome del comando, prima di qualsiasi altro parametro. Ad esempio, per impostare offline tutti i volumi i cui nomi includono la stringa `tmp`, eseguire il comando nel seguente esempio:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Le query estese sono generalmente utili solo con `modify` e `delete` comandi. Non hanno alcun significato in `create` oppure `show` comandi.

La combinazione di query e operazioni di modifica è uno strumento utile. Tuttavia, se implementato in modo errato, potrebbe causare confusione ed errori. Ad esempio, utilizzando (privilegio avanzato) `system node image modify` il comando per impostare l'immagine software predefinita di un nodo imposta automaticamente l'altra immagine software in modo che non sia quella predefinita. Il comando nell'esempio seguente è effettivamente un'operazione nulla:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

Questo comando imposta l'immagine predefinita corrente come immagine non predefinita, quindi imposta la nuova immagine predefinita (l'immagine precedente non predefinita) sull'immagine non predefinita, mantenendo le impostazioni predefinite originali. Per eseguire correttamente l'operazione, utilizzare il comando riportato nell'esempio seguente:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

#### Metodi di personalizzazione dell'output del comando `show` utilizzando i campi

Quando si utilizza `-instance` parametro con `a. show` comando per visualizzare i dettagli, l'output può essere lungo e includere più informazioni di quante ne hai bisogno. Il `-fields` parametro di `a. show` il comando consente di visualizzare solo le informazioni specificate.

Ad esempio, in esecuzione `volume show -instance` è probabile che si traducono in diverse schermate di informazioni. È possibile utilizzare `volume show -fields fieldname[,fieldname...]` per personalizzare l'output in modo che includa solo il campo o i campi specificati (oltre ai campi predefiniti sempre visualizzati). È

possibile utilizzare `-fields` ? per visualizzare i campi validi per a. show comando.

L'esempio seguente mostra la differenza di output tra `-instance` e il `-fields` parametro:

```
cluster1::> volume show -instance

Vserver Name: cluster1-1
Volume Name: vol0
Aggregate Name: aggr0
Volume Size: 348.3GB
Volume Data Set ID: -
Volume Master Data Set ID: -
Volume State: online
Volume Type: RW
Volume Style: flex
...
Space Guarantee Style: volume
Space Guarantee in Effect: true
...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume  space-guarantee  space-guarantee-enabled
-----  -
cluster1-1 vol0    volume          true
cluster1-2 vol0    volume          true
vs1      root_vol
          volume          true
vs2      new_vol
          volume          true
vs2      root_vol
          volume          true
...
cluster1::>
```

### Informazioni sui parametri di posizione

È possibile sfruttare la funzionalità dei parametri di posizione della CLI ONTAP per aumentare l'efficienza nell'input dei comandi. È possibile eseguire una query su un comando per identificare i parametri posizionali per il comando.



## Che cos'è un parametro posizionale

- Un parametro posizionale è un parametro che non richiede di specificare il nome del parametro prima di specificare il valore del parametro.
- Un parametro posizionale può essere intervallato con parametri non posizionali nell'input del comando, purché osservi la sua sequenza relativa con altri parametri posizionali nello stesso comando, come indicato nella **command\_name ?** output.
- Un parametro posizionale può essere un parametro obbligatorio o facoltativo per un comando.
- Un parametro può essere posizionale per un comando ma non posizionale per un altro.



L'utilizzo della funzionalità dei parametri di posizione negli script non è consigliato, in particolare quando i parametri di posizione sono facoltativi per il comando o hanno parametri facoltativi elencati prima di essi.

## Identificare un parametro di posizione

È possibile identificare un parametro di posizione in **command\_name ?** output del comando. Un parametro di posizione ha parentesi quadre che circondano il nome del parametro, in uno dei seguenti formati:

- `[-parameter_name] parameter_value` mostra un parametro obbligatorio posizionale.
- `[.[-parameter_name] parameter_value]` mostra un parametro opzionale posizionale.

Ad esempio, se visualizzato come segue in **command\_name ?** output, il parametro è posizionale per il comando in cui viene visualizzato:

- `[-lif] <lif-name>`
- `[[-lif] <lif-name>]`

Tuttavia, quando viene visualizzato come segue, il parametro non è posizionale per il comando in cui viene visualizzato:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

## Esempi di utilizzo dei parametri di posizione

Nell'esempio seguente, il **volume create ?** l'output mostra che tre parametri sono posizionali per il comando: `-volume`, `-aggregate`, e. `-size`.

```

cluster1::> volume create ?
    -vserver <vserver name>           Vserver Name
    [-volume] <volume name>           Volume Name
    [-aggregate] <aggregate name>      Aggregate Name
    [[-size] {<integer>[KB|MB|GB|TB|PB]] Volume Size
    [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                           Volume State (default: online)
    [ -type {RW|DP|DC} ]               Volume Type (default: RW)
    [ -policy <text> ]                 Export Policy
    [ -user <user name> ]              User ID
    ...
    [ -space-guarantee|-s {none|volume} ] Space Guarantee Style (default:
volume)
    [ -percent-snapshot-space <percent> ] Space Reserved for Snapshot
Copies
    ...

```

Nell'esempio seguente, il `volume create` il comando viene specificato senza sfruttare la funzionalità del parametro di posizione:

```

cluster1::> volume create -vserver svml -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

Gli esempi seguenti utilizzano la funzionalità del parametro di posizione per aumentare l'efficienza dell'input del comando. I parametri di posizione sono intervallati da parametri non posizionali in `volume create` e i valori dei parametri di posizione vengono specificati senza i nomi dei parametri. I parametri di posizione vengono specificati nella stessa sequenza indicata da **volume create ?** output. Questo è il valore per `-volume` viene specificato prima di `-aggregate`, a sua volta specificata prima di quella di `-size`.

```

cluster1::> volume create vol2 aggr1 1g -vserver svml -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svml vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

## Metodi di accesso alle pagine man di ONTAP

Le pagine man (manual) di ONTAP spiegano come utilizzare i comandi CLI di ONTAP. Queste pagine sono disponibili nella riga di comando e sono pubblicate anche nei *riferimenti ai comandi* specifici della release.

Nella riga di comando ONTAP, utilizzare `man command_name` per visualizzare la pagina manuale del comando specificato. Se non si specifica un nome di comando, viene visualizzato l'indice della pagina manuale. È possibile utilizzare `man man` per visualizzare informazioni su `man` comando stesso. È possibile uscire da una pagina man immettendo `q`.

Fare riferimento a [Riferimento al comando per la versione di ONTAP 9 in uso](#) Per ulteriori informazioni sui comandi ONTAP a livello amministrativo e avanzato disponibili nella release.

## Gestire le sessioni CLI

È possibile registrare una sessione CLI in un file con un nome e una dimensione specificati, quindi caricare il file in una destinazione FTP o HTTP. È inoltre possibile visualizzare o eliminare i file in cui sono state precedentemente registrate le sessioni CLI.

### Registrare una sessione CLI

Il record di una sessione CLI termina quando si interrompe la registrazione o si termina la sessione CLI o quando il file raggiunge il limite di dimensione specificato. Il limite predefinito per le dimensioni del file è di 1 MB. La dimensione massima del file è di 2 GB.

La registrazione di una sessione CLI è utile, ad esempio, se si sta risolvendo un problema e si desidera salvare informazioni dettagliate o se si desidera creare una registrazione permanente dell'utilizzo dello spazio in un momento specifico.

#### Fasi

1. Avviare la registrazione della sessione CLI corrente in un file:

```
system script start
```

Per ulteriori informazioni sull'utilizzo di `system script start` vedere la pagina [man](#).

ONTAP avvia la registrazione della sessione CLI nel file specificato.

2. Procedere con la sessione CLI.
3. Al termine, interrompere la registrazione della sessione:

```
system script stop
```

Per ulteriori informazioni sull'utilizzo di `system script stop` vedere la pagina [man](#).

ONTAP interrompe la registrazione della sessione CLI.

### Comandi per la gestione dei record delle sessioni CLI

Si utilizza `system script` Comandi per gestire i record delle sessioni CLI.

Se si desidera...	Utilizzare questo comando...
Avviare la registrazione della sessione CLI corrente in un file specificato	<code>system script start</code>
Interrompere la registrazione della sessione CLI corrente	<code>system script stop</code>
Visualizza le informazioni sui record delle sessioni CLI	<code>system script show</code>

Se si desidera...	Utilizzare questo comando...
Caricare un record di una sessione CLI su una destinazione FTP o HTTP	<code>system script upload</code>
Eliminare un record di una sessione CLI	<code>system script delete</code>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

### Comandi per la gestione del periodo di timeout automatico delle sessioni CLI

Il valore di timeout specifica per quanto tempo una sessione CLI rimane inattiva prima di essere terminata automaticamente. Il valore di timeout CLI è esteso a tutto il cluster. Ovvero, ogni nodo di un cluster utilizza lo stesso valore di timeout CLI.

Per impostazione predefinita, il periodo di timeout automatico delle sessioni CLI è di 30 minuti.

Si utilizza `system timeout` Comandi per gestire il periodo di timeout automatico delle sessioni CLI.

Se si desidera...	Utilizzare questo comando...
Visualizza il periodo di timeout automatico per le sessioni CLI	<code>system timeout show</code>
Modificare il periodo di timeout automatico per le sessioni CLI	<code>system timeout modify</code>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

### Gestione cluster (solo amministratori cluster)

#### Visualizza le informazioni sui nodi di un cluster

È possibile visualizzare i nomi dei nodi, verificare che i nodi siano integri e se sono idonei a partecipare al cluster. A livello di privilegi avanzati, è anche possibile visualizzare se un nodo contiene epsilon.

#### Fasi

1. Per visualizzare informazioni sui nodi di un cluster, utilizzare `cluster show` comando.

Se si desidera che l'output mostri se un nodo contiene epsilon, eseguire il comando al livello di privilegio avanzato.

#### Esempi di visualizzazione dei nodi in un cluster

Nell'esempio seguente vengono visualizzate informazioni su tutti i nodi di un cluster a quattro nodi:

```
cluster1::> cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true
node3	true	true
node4	true	true

Nell'esempio seguente vengono visualizzate informazioni dettagliate sul nodo denominato "node1" a livello di privilegi avanzati:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

      Node: node1
Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
  Epsilon: false
Eligibility: true
    Health: true
```

## Visualizzare gli attributi del cluster

È possibile visualizzare l'identificatore univoco (UUID), il nome, il numero di serie, la posizione e le informazioni di contatto di un cluster.

### Fasi

1. Per visualizzare gli attributi di un cluster, utilizzare `cluster identity show` comando.

### Esempio di visualizzazione degli attributi del cluster

Nell'esempio seguente vengono visualizzati il nome, il numero di serie, la posizione e le informazioni di contatto di un cluster.

```
cluster1::> cluster identity show

      Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
      Cluster Name: cluster1
Cluster Serial Number: 1-80-123456
  Cluster Location: Sunnyvale
    Cluster Contact: jsmith@example.com
```

## Modificare gli attributi del cluster

È possibile modificare gli attributi di un cluster, ad esempio il nome del cluster, la posizione e le informazioni di contatto, in base alle necessità.

### A proposito di questa attività

Non è possibile modificare l'UUID di un cluster, impostato al momento della creazione del cluster.

### Fasi

1. Per modificare gli attributi del cluster, utilizzare `cluster identity modify` comando.

Il `-name` parametro specifica il nome del cluster. Il `cluster identity modify` la pagina man descrive le regole per specificare il nome del cluster.

Il `-location` parametro specifica la posizione del cluster.

Il `-contact` parametro specifica le informazioni di contatto, ad esempio un nome o un indirizzo e-mail.

### Esempio di ridenominazione di un cluster

Il seguente comando rinomina il cluster corrente ("cluster1") in "cluster2":

```
cluster1::> cluster identity modify -name cluster2
```

## Visualizza lo stato degli anelli di replica del cluster

È possibile visualizzare lo stato degli anelli di replica del cluster per diagnosticare i problemi a livello di cluster. In caso di problemi nel cluster, il personale di supporto potrebbe richiedere di eseguire questa attività per agevolare la risoluzione dei problemi.

### Fasi

1. Per visualizzare lo stato degli anelli di replica del cluster, utilizzare `cluster ring show` al livello di privilegio avanzato.

### Esempio di visualizzazione dello stato di replica del cluster

Nell'esempio seguente viene visualizzato lo stato dell'anello di replica VLDB su un nodo denominato node0:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
      Node: node0
    Unit Name: vldb
      Status: master
        Epoch: 5
Master Node: node0
  Local Node: node0
      DB Epoch: 5
DB Transaction: 56
  Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

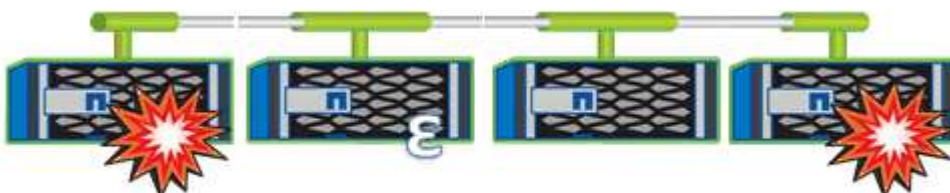
### Informazioni su quorum ed epsilon

Il quorum e l'epsilon sono misure importanti per lo stato e la funzione dei cluster che indicano insieme come i cluster affrontano le potenziali sfide di comunicazione e connettività.

*Quorum* è una condizione preliminare per un cluster completamente funzionante. Quando un cluster si trova in quorum, la maggior parte dei nodi è in buone condizioni e può comunicare tra loro. In caso di perdita del quorum, il cluster perde la capacità di eseguire le normali operazioni del cluster. Solo un insieme di nodi può avere il quorum alla volta, perché tutti i nodi condividono collettivamente una singola vista dei dati. Pertanto, se a due nodi non comunicanti è consentito modificare i dati in modo divergente, non è più possibile riconciliare i dati in una singola vista dati.

Ogni nodo del cluster partecipa a un protocollo di voting che elegge un nodo *master*; ogni nodo rimanente è un *secondario*. Il nodo master è responsabile della sincronizzazione delle informazioni nel cluster. Una volta formato, il quorum viene mantenuto con il voto continuo. Se il nodo master non è in linea e il cluster è ancora in quorum, viene selezionato un nuovo master dai nodi che rimangono in linea.

Poiché esiste la possibilità di un legame in un cluster con un numero pari di nodi, un nodo ha un peso di voto frazionario aggiuntivo chiamato *epsilon*. Se la connettività tra due parti uguali di un cluster di grandi dimensioni non riesce, il gruppo di nodi che contiene epsilon mantiene il quorum, presupponendo che tutti i nodi siano integri. Ad esempio, la seguente illustrazione mostra un cluster a quattro nodi in cui due dei nodi sono guasti. Tuttavia, poiché uno dei nodi sopravvissuti contiene epsilon, il cluster rimane in quorum anche se non esiste una semplice maggioranza di nodi sani.



Epsilon viene assegnato automaticamente al primo nodo al momento della creazione del cluster. Se il nodo che contiene epsilon diventa inintegro, assume il controllo del partner ad alta disponibilità o viene sostituito dal partner ad alta disponibilità, epsilon viene automaticamente riassegnato a un nodo integro in una coppia ha diversa.

L'utilizzo offline di un nodo può influire sulla capacità del cluster di rimanere in quorum. Pertanto, ONTAP emette un messaggio di avviso se si tenta di eseguire un'operazione che toglie il quorum al cluster o se si mette fuori servizio un'operazione per evitare la perdita del quorum. È possibile disattivare i messaggi di avviso del quorum utilizzando `cluster quorum-service options modify` al livello di privilegio avanzato.

In generale, supponendo una connettività affidabile tra i nodi del cluster, un cluster più grande è più stabile di un cluster più piccolo. Il requisito di quorum di una semplice maggioranza della metà dei nodi più epsilon è più semplice da gestire in un cluster di 24 nodi che in un cluster di due nodi.

Un cluster a due nodi presenta alcune sfide specifiche per il mantenimento del quorum. I cluster a due nodi utilizzano *cluster ha*, in cui nessuno dei due nodi contiene epsilon; invece, entrambi i nodi vengono continuamente interrogati per garantire che, in caso di guasto di un nodo, l'altro disponga dell'accesso completo in lettura/scrittura ai dati, nonché dell'accesso alle interfacce logiche e alle funzioni di gestione.

### **Quali sono i volumi di sistema**

I volumi di sistema sono volumi FlexVol che contengono metadati speciali, ad esempio metadati per i log di audit dei servizi file. Questi volumi sono visibili nel cluster in modo da poter tenere pienamente conto dell'utilizzo dello storage nel cluster.

I volumi di sistema sono di proprietà del server di gestione del cluster (chiamato anche SVM di amministrazione) e vengono creati automaticamente quando viene attivato il controllo dei file service.

È possibile visualizzare i volumi di sistema utilizzando `volume show` ma la maggior parte delle altre operazioni del volume non è consentita. Ad esempio, non è possibile modificare un volume di sistema utilizzando `volume modify` comando.

Questo esempio mostra quattro volumi di sistema sulla SVM amministrativa, che sono stati creati automaticamente quando è stato attivato il controllo dei servizi file per una SVM di dati nel cluster:



```
cluster1::> volume show -vserver cluster1
```

Vserver	Volume	Aggregate	State	Type	Size	Available
Used%						
-----	-----	-----	-----	-----	-----	-----
-----						
cluster1	MDV_aud_1d0131843d4811e296fc123478563412	aggr0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_8be27f813d7311e296fc123478563412	root_vs0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_9dc4ad503d7311e296fc123478563412	aggr1	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_a4b887ac3d7311e296fc123478563412	aggr2	online	RW	2GB	1.90GB
5%						

4 entries were displayed.

## Gestire i nodi

### Aggiungere nodi al cluster

Una volta creato un cluster, è possibile espanderlo aggiungendo nodi. È possibile aggiungere un solo nodo alla volta.

#### Di cosa hai bisogno

- Se si aggiungono nodi a un cluster a più nodi, tutti i nodi esistenti nel cluster devono essere integri (indicati da `cluster show`).
- Se stai aggiungendo nodi a un cluster senza switch a due nodi, devi convertire il cluster senza switch a due nodi in un cluster con switch usando uno switch cluster supportato da NetApp.

La funzionalità cluster senza switch è supportata solo in un cluster a due nodi.

- Se si aggiunge un secondo nodo a un cluster a nodo singolo, il secondo nodo deve essere stato installato e la rete del cluster deve essere stata configurata.
- Se nel cluster è attivata la configurazione automatica SP, la subnet specificata per il SP deve disporre di risorse disponibili per consentire al nodo di Unione di utilizzare la subnet specificata per configurare automaticamente il SP.
- Per la LIF di gestione dei nodi del nuovo nodo è necessario aver raccolto le seguenti informazioni:
  - Porta
  - Indirizzo IP
  - Netmask
  - Gateway predefinito

## A proposito di questa attività

I nodi devono essere in numeri pari in modo da poter formare coppie. Dopo aver iniziato ad aggiungere un nodo al cluster, è necessario completare il processo. Il nodo deve far parte del cluster prima di poter aggiungere un altro nodo.

### Fasi

1. Accendere il nodo che si desidera aggiungere al cluster.

Il nodo viene avviato e la procedura guidata Node Setup viene avviata sulla console.

```
Welcome to node setup.
```

```
You can enter the following commands at any time:
```

```
"help" or "?" - if you want to have a question clarified,
```

```
"back" - if you want to change previously answered questions, and
```

```
"exit" or "quit" - if you want to quit the setup wizard.
```

```
Any changes you made before quitting will be saved.
```

```
To accept a default or omit a question, do not enter a value.
```

```
Enter the node management interface port [e0M]:
```

2. Uscire dalla procedura guidata Node Setup (Configurazione nodo): `exit`

La procedura guidata Node Setup (Configurazione nodo) viene chiusa e viene visualizzato un prompt di accesso che avvisa che le attività di installazione non sono state completate.

3. Accedere all'account admin utilizzando `admin` nome utente.
4. Avviare l'installazione guidata del cluster:

```
cluster setup
```

```
::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".  
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing  
`https://<node_mgmt_or_e0M_IP_address>`

Otherwise, press Enter to complete cluster setup using the  
command line interface:



Per ulteriori informazioni sulla configurazione di un cluster mediante la GUI di installazione, consultare ["System Manager"](#) guida in linea.

5. Premere Invio per utilizzare l'interfaccia CLI per completare l'attività. Quando viene richiesto di creare un nuovo cluster o di unirsi a un cluster esistente, immettere **join**.

```
Do you want to create a new cluster or join an existing cluster?  
{create, join}:  
join
```

Se la versione di ONTAP eseguita sul nuovo nodo è diversa dalla versione in esecuzione sul cluster esistente, il sistema riporta un `System checks Error: Cluster join operation cannot be performed at this time` errore. Questo è il comportamento previsto. Per continuare, eseguire `add-node -allow-mixed-version-join new_node_name` comando a livello di privilegi avanzati da un nodo esistente nel cluster.

6. Seguire le istruzioni per configurare il nodo e unirsi al cluster:
  - Per accettare il valore predefinito di un prompt, premere Invio.
  - Per immettere un valore personalizzato per un prompt, immettere il valore, quindi premere Invio.
7. Ripetere i passaggi precedenti per ogni nodo aggiuntivo che si desidera aggiungere.

### Al termine

Dopo aver aggiunto nodi al cluster, è necessario attivare il failover dello storage per ogni coppia ha.

### Informazioni correlate

["Cluster ONTAP a versione mista"](#)

## Rimuovere i nodi dal cluster

È possibile rimuovere i nodi indesiderati da un cluster, un nodo alla volta. Dopo aver rimosso un nodo, è necessario rimuovere anche il partner di failover. Se si rimuove un nodo, i relativi dati diventano inaccessibili o cancellati.

### Prima di iniziare

Prima di rimuovere i nodi dal cluster, devono essere soddisfatte le seguenti condizioni:

- Più della metà dei nodi nel cluster deve essere integro.
- Tutti i dati sul nodo che si desidera rimuovere devono essere stati svuotati.
  - Ciò potrebbe includere ["eliminazione dei dati da un volume crittografato"](#).
- Tutti i volumi non root lo sono ["spostato"](#) da aggregati di proprietà del nodo.
- Tutti gli aggregati non root sono stati ["cancellato"](#) dal nodo.
- Se il nodo possiede dischi FIPS (Federal Information Processing Standards) o dischi con crittografia automatica (SED), ["la crittografia del disco è stata rimossa"](#) riportando i dischi in modalità non protetta.
  - Potrebbe anche essere utile ["Sanificare i dischi FIPS o i SED"](#).
- I dati LIF lo sono ["cancellato"](#) oppure ["trasferito"](#) dal nodo.
- Le LIF di gestione del cluster lo sono state ["trasferito"](#) dal nodo e le porte home sono cambiate.
- Tutte le LIF intercluster sono state ["rimosso"](#).
  - Quando si rimuovono le LIF di intercluster, viene visualizzato un avviso che può essere ignorato.
- Il failover dello storage è stato così ["disattivato"](#) per il nodo.
- Tutte le regole di failover LIF lo sono state ["modificato"](#) per rimuovere le porte sul nodo.
- Tutte le VLAN sul nodo sono state ["cancellato"](#).
- Se si dispone di LUN sul nodo da rimuovere, è necessario ["Modificare l'elenco dei nodi di reporting della mappa LUN selettiva \(SLM\)"](#) prima di rimuovere il nodo.

Se non si rimuove il nodo e il relativo partner ha dall'elenco dei nodi di reporting SLM, l'accesso alle LUN precedentemente presenti sul nodo può andare perso anche se i volumi contenenti le LUN sono stati spostati in un altro nodo.

Si consiglia di inviare un messaggio AutoSupport per informare il supporto tecnico NetApp che la rimozione del nodo è in corso.

**Nota:** non è necessario eseguire operazioni come `cluster remove-node`, `cluster unjoin`, e `node rename` Quando è in corso un aggiornamento automatico di ONTAP.

### A proposito di questa attività

- Se si esegue un cluster a versione mista, è possibile rimuovere l'ultimo nodo a versione bassa utilizzando uno dei comandi di privilegio avanzati che iniziano con ONTAP 9.3:
  - ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
  - ONTAP 9.4 e versioni successive: `cluster remove-node -skip-last-low-version-node-check`
- Se si disuniscono 2 nodi da un cluster a 4 nodi, il cluster ha viene attivato automaticamente sui due nodi rimanenti.



Tutti i dati del sistema e dell'utente, provenienti da tutti i dischi collegati al nodo, devono essere resi inaccessibili agli utenti prima di rimuovere un nodo dal cluster. Se un nodo non è stato collegato correttamente da un cluster, contattare il supporto NetApp per assistenza con le opzioni di ripristino.

## Fasi

1. Impostare il livello di privilegio su avanzato:

```
set -privilege advanced
```

2. Verificare se un nodo sul cluster contiene epsilon:

```
cluster show -epsilon true
```

3. Se un nodo nel cluster contiene epsilon e quel nodo verrà disaccoppiato, spostare epsilon in un nodo che non verrà disaccoppiato:

- a. Spostare epsilon dal nodo che si intende disunire

```
cluster modify -node <name_of_node_to_be_unjoined> -epsilon false
```

- b. Spostare epsilon in un nodo che non verrà disUnito:

```
cluster modify -node <node_name> -epsilon true
```

4. Identificare il nodo master corrente:

```
cluster ring show
```

Il nodo master è il nodo che contiene processi come "mgmt", "vldb", "vifmgr", "bcomd" e "crs".

5. Se il nodo che si desidera rimuovere è il nodo master corrente, abilitare l'elezione di un altro nodo nel cluster come nodo master:

- a. Rendere il nodo master corrente non idoneo a partecipare al cluster:

```
cluster modify - node <node_name> -eligibility false
```

Quando il nodo master non è idoneo, uno dei nodi rimanenti viene selezionato dal quorum del cluster come nuovo master.

- b. Rendere il nodo master precedente idoneo a partecipare nuovamente al cluster:

```
cluster modify - node <node_name> -eligibility true
```

6. Accedere alla LIF di gestione dei nodi remoti o alla LIF di gestione dei cluster su un nodo diverso da quello da rimuovere.
7. Rimuovere il nodo dal cluster:

Per questa versione di ONTAP...	Utilizzare questo comando...
ONTAP 9.3	<pre>cluster unjoin</pre>
ONTAP 9.4 e versioni successive	<pre>cluster remove-node*</pre>

Se si dispone di un cluster con versione mista e si sta rimuovendo l'ultimo nodo della versione inferiore, utilizzare `-skip-last-low-version-node-check` con questi comandi.

Il sistema informa l'utente di quanto segue:

- È inoltre necessario rimuovere il partner di failover del nodo dal cluster.
- Una volta rimosso il nodo e prima di poterlo riconnettere a un cluster, è necessario utilizzare l'opzione del menu di avvio (4) pulizia della configurazione e inizializzazione di tutti i dischi o l'opzione (9) Configurazione della partizione avanzata del disco per cancellare la configurazione del nodo e inizializzare tutti i dischi.

Viene generato un messaggio di errore se si verificano condizioni che è necessario risolvere prima di rimuovere il nodo. Ad esempio, il messaggio potrebbe indicare che il nodo dispone di risorse condivise che è necessario rimuovere o che si trova in una configurazione ha del cluster o in una configurazione di failover dello storage che è necessario disattivare.

Se il nodo è il master del quorum, il cluster perderà brevemente e tornerà al quorum. Questa perdita di quorum è temporanea e non influisce sulle operazioni dei dati.

8. Se un messaggio di errore indica condizioni di errore, risolvere tali condizioni ed eseguire nuovamente il `cluster remove-node` oppure `cluster unjoin` comando.

Il nodo viene riavviato automaticamente dopo che è stato rimosso dal cluster.

9. Se si sta ridisponendo il nodo, cancellare la configurazione del nodo e inizializzare tutti i dischi:
  - a. Durante il processo di avvio, premere Ctrl-C per visualizzare il menu di avvio quando richiesto.
  - b. Selezionare l'opzione del menu di avvio (4) pulizia della configurazione e inizializzazione di tutti i dischi.
10. Torna al livello di privilegio admin:

```
set -privilege admin
```

11. Ripetere i passaggi precedenti per rimuovere il partner di failover dal cluster.

## Accedere ai file di log, core dump e MIB di un nodo utilizzando un browser Web

L'infrastruttura del Service Processor (`spi`) È attivato per impostazione predefinita per consentire a un browser Web di accedere ai file log, core dump e MIB di un nodo del cluster. I file rimangono accessibili anche quando il nodo non è attivo, a condizione che il nodo venga sostituito dal partner.

### Di cosa hai bisogno

- La LIF di gestione del cluster deve essere attiva.

È possibile utilizzare la LIF di gestione del cluster o di un nodo per accedere a `spi` servizio web. Tuttavia, si consiglia di utilizzare la LIF di gestione del cluster.

Il `network interface show` Il comando visualizza lo stato di tutte le LIF nel cluster.

- Per accedere a, è necessario utilizzare un account utente locale `spi` servizio web, gli account utente di dominio non sono supportati.
- Se l'account utente non ha il ruolo "admin" (che ha accesso a `spi` servizio web per impostazione predefinita), al ruolo di controllo degli accessi deve essere concesso l'accesso a `spi` servizio web.

Il `vserver services web access show` il comando mostra i ruoli a cui viene concesso l'accesso a quali servizi web.

- Se non si utilizza l'account utente "admin" (che include `http access method` (metodo di accesso), l'account utente deve essere impostato con `http` metodo di accesso.

Il `security login show` il comando mostra i metodi di accesso e accesso degli account utente e i ruoli di controllo degli accessi.

- Se si desidera utilizzare HTTPS per un accesso Web sicuro, è necessario attivare SSL e installare un certificato digitale.

Il `system services web show` il comando visualizza la configurazione del motore del protocollo web a livello di cluster.

### A proposito di questa attività

Il `spi` il servizio web è attivato per impostazione predefinita ed è possibile disattivarlo manualmente (`vserver services web modify -vserver * -name spi -enabled false`).

Al ruolo "admin" viene concesso l'accesso a `spi` servizio web per impostazione predefinita e l'accesso può essere disattivato manualmente (`services web access delete -vserver cluster_name -name spi -role admin`).

### Fasi

1. Puntare il browser Web su `spi` URL del servizio web in uno dei seguenti formati:

- `http://cluster-mgmt-LIF/spi/`
- `https://cluster-mgmt-LIF/spi/`

`cluster-mgmt-LIF` È l'indirizzo IP della LIF di gestione del cluster.

2. Quando richiesto dal browser, inserire l'account utente e la password.

Una volta autenticato l'account, il browser visualizza i collegamenti a `/mroot/etc/log/`, `/mroot/etc/crash/`, e `/mroot/etc/mib/` directory di ciascun nodo del cluster.

### Accedere alla console di sistema di un nodo

Se un nodo si trova nel menu di boot o nel prompt dell'ambiente di boot, è possibile accedervi solo dalla console di sistema (chiamata anche *console seriale*). È possibile accedere alla console di sistema di un nodo da una connessione SSH all'SP del nodo o al cluster.

#### A proposito di questa attività

Sia SP che ONTAP offrono comandi che consentono di accedere alla console di sistema. Tuttavia, dal provider di servizi Internet, è possibile accedere solo alla console di sistema del proprio nodo. Dal cluster, è possibile accedere alla console di sistema di qualsiasi nodo del cluster.

#### Fasi

1. Accedere alla console di sistema di un nodo:

Se si è in...	Immettere questo comando...
CLI SP del nodo	<code>system console</code>
CLI ONTAP	<code>system node run-console</code>

2. Quando richiesto, accedere alla console di sistema.
3. Per uscire dalla console di sistema, premere Ctrl-D.

### Esempi di accesso alla console di sistema

Nell'esempio riportato di seguito viene illustrato il risultato dell'immissione di `system console` Al prompt "SP node2". La console di sistema indica che node2 è in sospenso al prompt dell'ambiente di boot. Il `boot_ontap` Il comando viene immesso nella console per avviare il nodo su ONTAP. Premere Ctrl-D per uscire dalla console e tornare all'SP.



```
SP node2> system console
Type Ctrl-D to exit.
```

```
LOADER>
LOADER> boot_ontap

...
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
...
```

Premere Ctrl-D per uscire dalla console di sistema.

```
Connection to 123.12.123.12 closed.
SP node2>
```

Nell'esempio riportato di seguito viene illustrato il risultato dell'immissione di `system node run-console` Comando da ONTAP per accedere alla console di sistema di node2, che si trova al prompt dell'ambiente di boot. Il `boot_ontap` Il comando viene immesso nella console per avviare node2 in ONTAP. Premere Ctrl-D per uscire dalla console e tornare a ONTAP.

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap

...
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
...
```

Premere Ctrl-D per uscire dalla console di sistema.

```
Connection to 123.12.123.12 closed.
cluster1::>
```

## Gestire i volumi root dei nodi e gli aggregati root

Il volume root di un nodo è un volume FlexVol installato in fabbrica o dal software di installazione. È riservato ai file di sistema, ai file di log e ai file principali. Il nome della directory è `/mroot`, accessibile solo attraverso la shell di sistema dal supporto tecnico. La dimensione minima del volume root di un nodo dipende dal modello di piattaforma.

### Panoramica delle regole che disciplinano i volumi root dei nodi e gli aggregati root

Il volume root di un nodo contiene directory e file speciali per quel nodo. L'aggregato root contiene il volume root. Alcune regole governano il volume root e l'aggregato root di un nodo.

- Le seguenti regole governano il volume root del nodo:
  - A meno che il supporto tecnico non lo richieda, non modificare la configurazione o il contenuto del volume root.
  - Non memorizzare i dati dell'utente nel volume root.

L'archiviazione dei dati dell'utente nel volume root aumenta il tempo di giveback dello storage tra i nodi di una coppia ha.

- È possibile spostare il volume root in un altro aggregato. Vedere [\[relocate-root\]](#).
- L'aggregato root è dedicato solo al volume root del nodo.

ONTAP impedisce la creazione di altri volumi nell'aggregato root.

## "NetApp Hardware Universe"

### Liberare spazio sul volume root di un nodo

Quando il volume root di un nodo è pieno o quasi pieno, viene visualizzato un messaggio di avviso. Il nodo non può funzionare correttamente quando il volume root è pieno. È possibile liberare spazio sul volume root di un nodo eliminando i file core dump, i file di traccia dei pacchetti e le copie Snapshot del volume root.

### Fasi

1. Visualizzare i file core dump del nodo e i relativi nomi:

```
system node coredump show
```

2. Eliminare i file core dump indesiderati dal nodo:

```
system node coredump delete
```

3. Accedi al nodeshell:

```
system node run -node nodename
```

*nodename* è il nome del nodo di cui si desidera liberare spazio nel volume root.

4. Passa al livello di privilegio avanzato più incondiscendente dal nodeshell:

```
priv set advanced
```

5. Visualizzare ed eliminare i file di traccia dei pacchetti del nodo attraverso il nodeshell:

a. Visualizza tutti i file nel volume root del nodo:

```
ls /etc
```

b. Se vi sono file di traccia dei pacchetti (\*.trc) si trovano nel volume root del nodo, eliminarli singolarmente:

```
rm /etc/log/packet_traces/file_name.trc
```

6. Identificare ed eliminare le copie Snapshot del volume root del nodo attraverso il nodeshell:

a. Identificare il nome del volume root:

```
vol status
```

Il volume root è indicato dalla parola “root” nella colonna “Options” di `vol status` output del comando.

Nell'esempio seguente, il volume root è `vol0`:

```
node1*> vol status
```

Volume	State	Status	Options
vol0	online	raid_dp, flex 64-bit	root, nvfail=on

a. Visualizza copie Snapshot del volume root:

```
snap list root_vol_name
```

b. Eliminare le copie Snapshot del volume root indesiderate:

```
snap delete root_vol_namesnapshot_name
```

7. Uscire dal nodeshell e tornare alla shell di clustershell:

```
exit
```

### **Spostare i volumi root in nuovi aggregati**

La procedura di sostituzione root migra l'aggregato root corrente in un altro set di dischi senza interruzioni.

#### **A proposito di questa attività**

Per spostare i volumi root, è necessario abilitare il failover dello storage. È possibile utilizzare `storage failover modify -node nodename -enable true` comando per abilitare il failover.

È possibile modificare la posizione del volume root in un nuovo aggregato nei seguenti scenari:

- Quando gli aggregati root non si trovano sul disco, si preferisce

- Quando si desidera riorganizzare i dischi collegati al nodo
- Quando si esegue una sostituzione degli shelf degli shelf di dischi EOS

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set privilege advanced
```

2. Spostare l'aggregato root:

```
system node migrate-root -node nodename -disklist disklist -raid-type raid-type
```

- **-nodo**

Specifica il nodo proprietario dell'aggregato root che si desidera migrare.

- **-disklist**

Specifica l'elenco dei dischi su cui verrà creato il nuovo aggregato root. Tutti i dischi devono essere spare e di proprietà dello stesso nodo. Il numero minimo di dischi richiesto dipende dal tipo di RAID.

- **-raid-type**

Specifica il tipo RAID dell'aggregato root. Il valore predefinito è `raid-dp`.

3. Monitorare l'avanzamento del lavoro:

```
job show -id jobid -instance
```

## Risultati

Se tutti i controlli preliminari hanno esito positivo, il comando avvia un processo di sostituzione del volume root ed esce. Attendere il riavvio del nodo.

## Consente di avviare o interrompere una panoramica dei nodi

Potrebbe essere necessario avviare o arrestare un nodo per motivi di manutenzione o risoluzione dei problemi. È possibile eseguire questa operazione dall'interfaccia utente di ONTAP, dal prompt dell'ambiente di avvio o dall'interfaccia utente di SP.

Utilizzando il comando SP CLI `system power off` oppure `system power cycle` Per spegnere o spegnere e riaccendere un nodo potrebbe causare un arresto non corretto del nodo (chiamato anche *shutdown anomalo*) e non sostituire un arresto corretto mediante ONTAP `system node halt` comando.

## Riavviare un nodo al prompt del sistema

È possibile riavviare un nodo in modalità normale dal prompt di sistema. Un nodo è configurato per l'avvio dal dispositivo di avvio, ad esempio una scheda PC CompactFlash.

## Fasi

1. Se il cluster contiene quattro o più nodi, verificare che il nodo da riavviare non contenga epsilon:

a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

b. Determinare quale nodo contiene epsilon:

```
cluster show
```

Il seguente esempio mostra che “node1” contiene epsilon:

```
cluster1::*> cluster show
Node           Health Eligibility Epsilon
-----
node1          true   true      true
node2          true   true      false
node3          true   true      false
node4          true   true      false
4 entries were displayed.
```

a. Se il nodo da riavviare contiene epsilon, rimuovere epsilon dal nodo:

```
cluster modify -node node_name -epsilon false
```

b. Assegnare epsilon a un nodo diverso che rimarrà attivo:

```
cluster modify -node node_name -epsilon true
```

c. Tornare al livello di privilegio admin:

```
set -privilege admin
```

2. Utilizzare `system node reboot` comando per riavviare il nodo.

Se non si specifica `-skip-lif-migration` Il comando tenta di migrare i dati e le LIF di gestione del cluster in modo sincrono su un altro nodo prima del riavvio. Se la migrazione LIF non riesce o si interrompe, il processo di riavvio viene interrotto e ONTAP visualizza un errore per indicare che la migrazione LIF non è riuscita.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

Il nodo avvia il processo di riavvio. Viene visualizzato il prompt di accesso di ONTAP, che indica che il processo di riavvio è stato completato.

### Boot ONTAP al prompt dell'ambiente di boot

È possibile avviare la release corrente o la release di backup di ONTAP quando si è al prompt dell'ambiente di boot di un nodo.

### Fasi

1. Accedere al prompt dell'ambiente di boot dal prompt del sistema di storage utilizzando `system node halt` comando.

La console del sistema di storage visualizza il prompt dell'ambiente di boot.

2. Al prompt dell'ambiente di boot, immettere uno dei seguenti comandi:

Per avviare...	Inserisci...
L'attuale release di ONTAP	<code>boot_ontap</code>
L'immagine principale di ONTAP dal dispositivo di avvio	<code>boot_primary</code>
Immagine di backup di ONTAP dal dispositivo di avvio	<code>boot_backup</code>

In caso di dubbi sull'immagine da utilizzare, è necessario utilizzarla `boot_ontap` in primo luogo.

### Chiudere un nodo

È possibile arrestare un nodo se non risponde o se il personale di supporto lo ha indicato come parte delle attività di risoluzione dei problemi.

### Fasi

1. Se il cluster contiene quattro o più nodi, verificare che il nodo da arrestare non contenga epsilon:
  - a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- b. Determinare quale nodo contiene epsilon:

```
cluster show
```

Il seguente esempio mostra che "node1" contiene epsilon:

```
cluster1::*> cluster show
Node           Health Eligibility Epsilon
-----
node1          true   true      true
node2          true   true      false
node3          true   true      false
node4          true   true      false
4 entries were displayed.
```

- a. Se il nodo da spegnere contiene epsilon, rimuovere epsilon dal nodo:

```
cluster modify -node node_name -epsilon false
```

b. Assegnare epsilon a un nodo diverso che rimarrà attivo:

```
cluster modify -node node_name -epsilon true
```

c. Tornare al livello di privilegio admin:

```
set -privilege admin
```

2. Utilizzare `system node halt` comando per arrestare il nodo.

Se non si specifica `-skip-lif-migration` Il comando tenta di migrare i dati e le LIF di gestione del cluster in modo sincrono su un altro nodo prima dello shutdown. Se la migrazione LIF non riesce o va in timeout, il processo di arresto viene interrotto e ONTAP visualizza un errore per indicare che la migrazione LIF non è riuscita.

È possibile attivare manualmente un core dump con lo shutdown utilizzando entrambi `-dump` parametro.

Nell'esempio seguente viene chiuso il nodo "node1" per la manutenzione dell'hardware:

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

### Gestire un nodo utilizzando il menu di boot

È possibile utilizzare il menu di avvio per correggere i problemi di configurazione su un nodo, reimpostare la password di amministratore, inizializzare i dischi, ripristinare la configurazione del nodo e ripristinare le informazioni di configurazione del nodo sul dispositivo di avvio.



Se è in uso una coppia ha ["Crittografia dei dischi SAS o NVMe \(SED, NSE, FIPS\)"](#), è necessario seguire le istruzioni riportate nell'argomento ["Ripristino di un'unità FIPS o SED in modalità non protetta"](#) Per tutti i dischi all'interno della coppia ha prima dell'inizializzazione del sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

### Fasi

1. Riavviare il nodo per accedere al menu di avvio utilizzando `system node reboot` al prompt del sistema.

Il nodo avvia il processo di riavvio.

2. Durante il processo di riavvio, premere Ctrl-C per visualizzare il menu di avvio quando richiesto.

Il nodo visualizza le seguenti opzioni per il menu di boot:

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```




Opzione del menu di boot (2) l'avvio senza /etc/rc è obsoleto e non ha alcun effetto sul sistema.

3. Selezionare una delle seguenti opzioni immettendo il numero corrispondente:

Per...	Selezionare...
Continuare ad avviare il nodo in modalità normale	1) Avvio normale
Modificare la password del nodo, che è anche la password dell'account "admin"	3) modificare la password



Per...	Selezionare...
Inizializzare i dischi del nodo e creare un volume root per il nodo	<p>4) pulire la configurazione e inizializzare tutti i dischi</p> <div>  <p>Questa opzione di menu cancella tutti i dati presenti sui dischi del nodo e ripristina la configurazione del nodo alle impostazioni predefinite.</p> </div> <p>Selezionare questa voce di menu solo dopo che il nodo è stato rimosso da un cluster (non Unito) e non è stato Unito a un altro cluster.</p> <p>Per un nodo con shelf di dischi interni o esterni, viene inizializzato il volume root sui dischi interni. Se non sono presenti shelf di dischi interni, viene inizializzato il volume root sui dischi esterni.</p> <p>Per un sistema che esegue la virtualizzazione FlexArray con shelf di dischi interni o esterni, le LUN degli array non vengono inizializzate. Tutti i dischi nativi sugli shelf interni o esterni vengono inizializzati.</p> <p>Per un sistema che esegue la virtualizzazione FlexArray con solo LUN di array e senza shelf di dischi interni o esterni, il volume root sulle LUN degli array di storage viene inizializzato, vedere <a href="#">"Installazione di FlexArray"</a>.</p> <p>Se il nodo che si desidera inizializzare dispone di dischi partizionati per la partizione dei dati root, i dischi devono essere dispartizionati prima che il nodo possa essere inizializzato, vedere <b>9) Configurazione della partizione avanzata dei dischi</b> e. <a href="#">"Gestione di dischi e aggregati"</a>.</p>
Eseguire operazioni di manutenzione di aggregati e dischi e ottenere informazioni dettagliate su aggregati e dischi.	<p>5) Avvio in modalità di manutenzione</p> <p>Per uscire dalla modalità di manutenzione, utilizzare <code>halt</code> comando.</p>
Ripristinare le informazioni di configurazione dal volume root del nodo al dispositivo di avvio, ad esempio una scheda PC CompactFlash	<p>6) aggiornare la flash dalla configurazione di backup</p> <p>ONTAP memorizza alcune informazioni di configurazione del nodo sul dispositivo di avvio. Quando il nodo viene riavviato, viene eseguito automaticamente il backup delle informazioni sul dispositivo di avvio sul volume root del nodo. Se il dispositivo di boot risulta corrotto o deve essere sostituito, utilizzare questa opzione di menu per ripristinare le informazioni di configurazione dal volume root del nodo al dispositivo di boot.</p>

Per...	Selezionare...
Installare il nuovo software sul nodo	<p>7) installare prima il nuovo software</p> <p>Se il software ONTAP sul dispositivo di boot non include il supporto per lo storage array che si desidera utilizzare per il volume root, è possibile utilizzare questa opzione di menu per ottenere una versione del software che supporti lo storage array e installarla sul nodo.</p> <p>Questa opzione di menu consente di installare una versione più recente del software ONTAP su un nodo che non dispone di un volume root installato. Non utilizzare questa opzione di menu per aggiornare ONTAP.</p>
Riavviare il nodo	8) riavviare il nodo
Dispartizionare tutti i dischi e rimuovere le informazioni di proprietà o pulire la configurazione e inizializzare il sistema con dischi interi o partizionati	<p>9) configurare la partizione avanzata dei dischi</p> <p>A partire da ONTAP 9.2, l'opzione di partizione avanzata dei dischi offre funzionalità di gestione aggiuntive per i dischi configurati per la partizione root-data o root-data-data. Le seguenti opzioni sono disponibili dall'opzione di avvio 9:</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>(9a) Unpartition all disks and remove their ownership information.</p> <p>(9b) Clean configuration and initialize system with partitioned disks.</p> <p>(9c) Clean configuration and initialize system with whole disks.</p> <p>(9d) Reboot the node.</p> <p>(9e) Return to main boot menu.</p> </div>

## Visualizza gli attributi del nodo

È possibile visualizzare gli attributi di uno o più nodi nel cluster, ad esempio il nome, il proprietario, la posizione, numero di modello, numero di serie, durata dell'esecuzione del nodo, stato di salute e idoneità a partecipare a un cluster.

### Fasi

1. Per visualizzare gli attributi di un nodo specifico o di tutti i nodi di un cluster, utilizzare `system node show` comando.

### Esempio di visualizzazione di informazioni su un nodo

Nell'esempio seguente vengono visualizzate informazioni dettagliate sul nodo 1:

```
cluster1::> system node show -node node1
Node: node1
Owner: Eng IT
Location: Lab 5
Model: model_number
Serial Number: 12345678
Asset Tag: -
Uptime: 23 days 04:42
NVRAM System ID: 118051205
System ID: 0118051205
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: true
Capacity Optimized: false
QLC Optimized: false
All-Flash Select Optimized: false
SAS2/SAS3 Mixed Stack Support: none
```

## Modificare gli attributi del nodo

È possibile modificare gli attributi di un nodo in base alle esigenze. Gli attributi che è possibile modificare includono le informazioni sul proprietario del nodo, le informazioni sulla posizione, il tag delle risorse e l'idoneità a partecipare al cluster.

### A proposito di questa attività

L'idoneità di un nodo a partecipare al cluster può essere modificata a livello di privilegio avanzato utilizzando `-eligibility` del parametro `system node modify` oppure `cluster modify` comando. Se si imposta l'idoneità di un nodo su `false`, il nodo diventa inattivo nel cluster.



Non è possibile modificare localmente l'idoneità del nodo. Deve essere modificato da un nodo diverso. L'eleggibilità del nodo non può essere modificata anche con una configurazione cluster ha.



Evitare di impostare l'idoneità di un nodo su `false`, ad eccezione di situazioni come il ripristino della configurazione del nodo o la manutenzione prolungata del nodo. L'accesso AI dati SAN e NAS al nodo potrebbe essere compromesso quando il nodo non è idoneo.

## Fasi

1. Utilizzare `system node modify` per modificare gli attributi di un nodo.

### Esempio di modifica degli attributi del nodo

Il seguente comando modifica gli attributi del nodo "node1". Il proprietario del nodo è impostato su "Joe Smith" e il relativo tag asset è impostato su "js1234":

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag js1234
```

## Rinominare un nodo

È possibile modificare il nome di un nodo in base alle esigenze.

### Fasi

1. Per rinominare un nodo, utilizzare `system node rename` comando.

Il `-newname` parametro specifica il nuovo nome del nodo. Il `system node rename` la pagina man descrive le regole per specificare il nome del nodo.

Se si desidera rinominare più nodi nel cluster, è necessario eseguire il comando per ciascun nodo singolarmente.



Il nome del nodo non può essere "all" perché "all" è un nome riservato al sistema.

### Esempio di ridenominazione di un nodo

Il seguente comando rinomina il nodo "node1" in "node1a":

```
cluster1::> system node rename -node node1 -newname node1a
```

## Gestisci cluster a nodo singolo

Un cluster a nodo singolo è un'implementazione speciale di un cluster in esecuzione su un nodo standalone. I cluster a nodo singolo non sono consigliati, in quanto non forniscono ridondanza. Se il nodo si guasta, l'accesso ai dati viene perso.



Per la tolleranza agli errori e le operazioni senza interruzioni, è consigliabile configurare il cluster con ["Alta disponibilità \(coppie ha\)"](#).

Se scegli di configurare o eseguire l'upgrade di un cluster a nodo singolo, devi conoscere i seguenti aspetti:

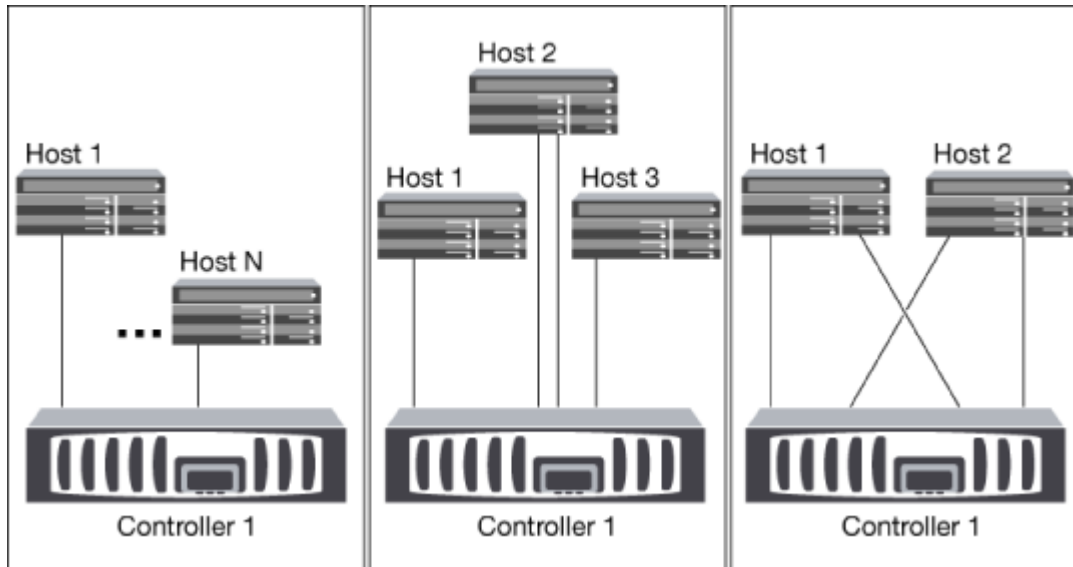
- La crittografia del volume root non è supportata su cluster a nodo singolo.
- Se si rimuovono i nodi per avere un cluster a nodo singolo, è necessario modificare le porte del cluster per erogare traffico dati modificando le porte del cluster in modo che siano porte dati e creando quindi LIF dati sulle porte per dati.
- Per i cluster a nodo singolo, puoi specificare la destinazione di backup della configurazione durante la configurazione del software. Dopo l'installazione, è possibile modificare tali impostazioni utilizzando i comandi ONTAP.
- Se al nodo sono connessi più host, è possibile configurare ciascun host con un sistema operativo diverso, ad esempio Windows o Linux. Se sono presenti più percorsi dall'host al controller, ALUA deve essere abilitato sull'host.

### Modi per configurare host SAN iSCSI con nodi singoli

È possibile configurare gli host SAN iSCSI in modo che si connettano direttamente a un singolo nodo o tramite uno o più switch IP. Il nodo può avere più connessioni iSCSI allo switch.

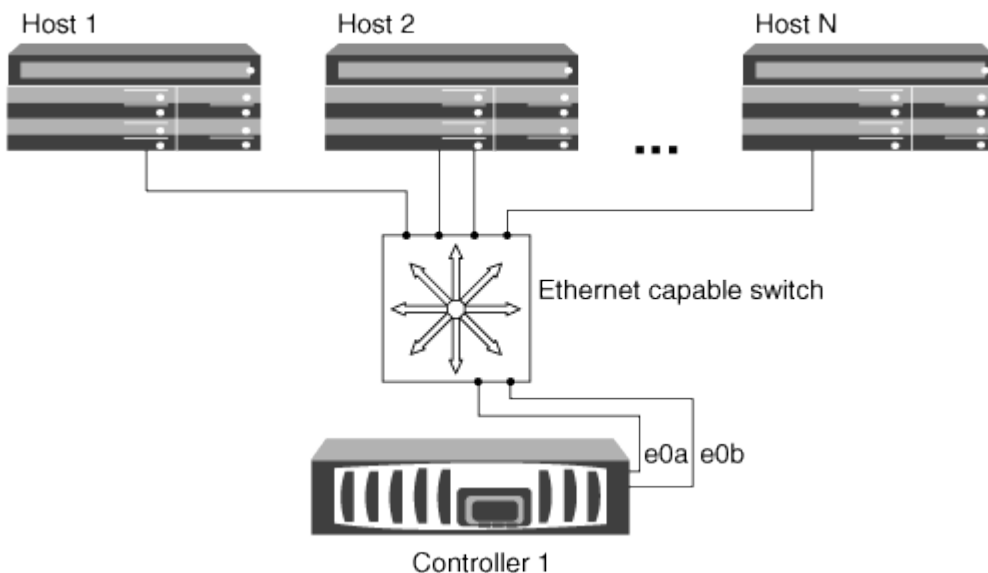
#### Configurazioni a nodo singolo direct-attached

Nelle configurazioni a nodo singolo direct-attached, uno o più host sono connessi direttamente al nodo.



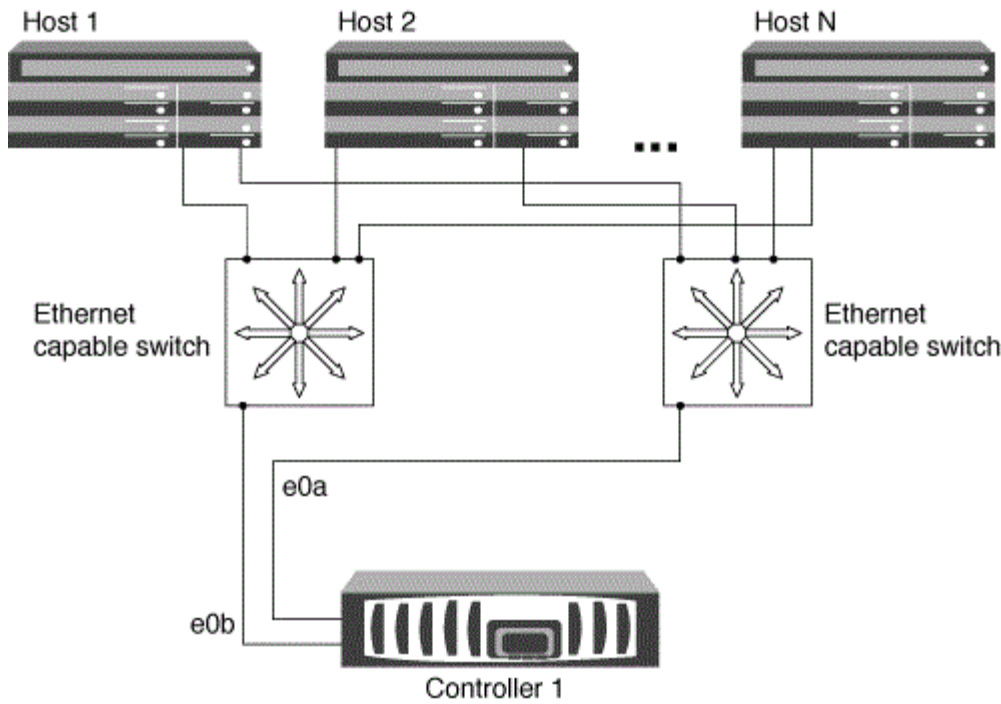
#### Configurazioni a nodo singolo di rete

Nelle configurazioni a nodo singolo di rete, uno switch connette un singolo nodo a uno o più host. Poiché esiste un singolo switch, questa configurazione non è completamente ridondante.



#### Configurazioni multi-rete a nodo singolo

Nelle configurazioni multi-network a nodo singolo, due o più switch collegano un singolo nodo a uno o più host. Poiché esistono più switch, questa configurazione è completamente ridondante.



#### Modi per configurare host FC e SAN FC-NVMe con nodi singoli

È possibile configurare host FC e SAN FC-NVMe con nodi singoli attraverso uno o più fabric. N-Port ID Virtualization (NPIV) è necessario e deve essere attivato su tutti gli switch FC del fabric. Non è possibile collegare direttamente host SAN FC o FC-NVMe a nodi singoli senza utilizzare uno switch FC.

#### Configurazioni single-fabric a nodo singolo

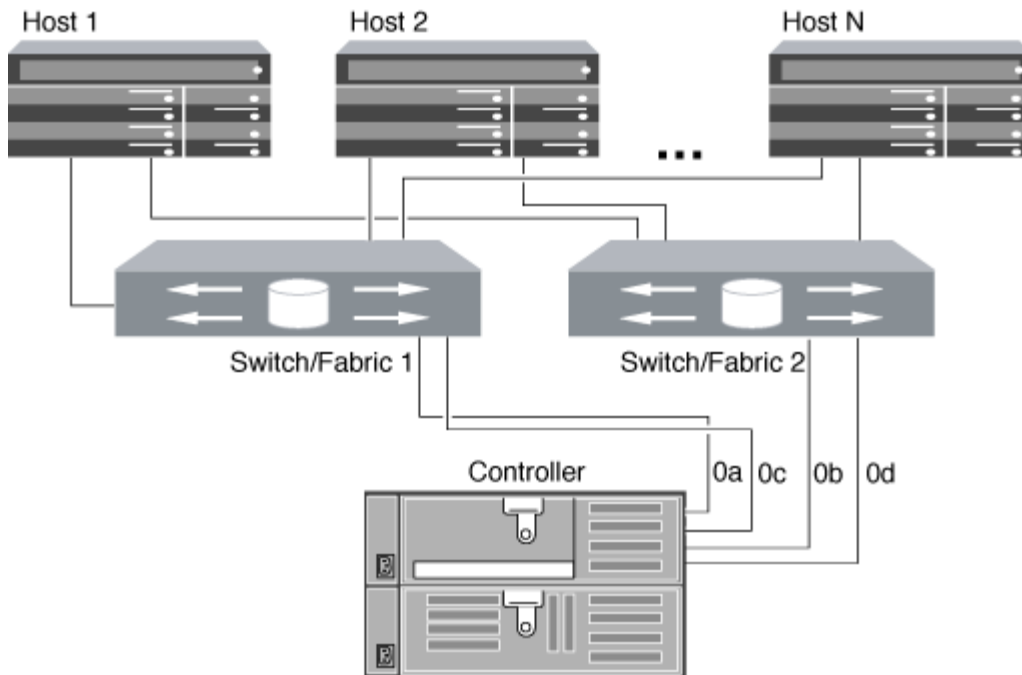
Nelle configurazioni a nodo singolo con fabric singolo, è disponibile uno switch che collega un singolo nodo a uno o più host. Poiché esiste un singolo switch, questa configurazione non è completamente ridondante.

Nelle configurazioni a nodo singolo con fabric singolo, il software di multipathing non è necessario se si dispone di un solo percorso dall'host al nodo.

#### Configurazioni multi-nodo singolo

Nelle configurazioni multi-nodo singolo, sono presenti due o più switch che collegano un singolo nodo a uno o più host. Per semplicità, la figura seguente mostra una configurazione multi-nodo singolo con solo due fabric, ma è possibile avere due o più fabric in qualsiasi configurazione multifabrica. In questa figura, lo storage controller è montato nello chassis superiore e quello inferiore può essere vuoto o può avere un modulo IOMX, come in questo esempio.

Le porte di destinazione FC (0a, 0c, 0b, 0d) nelle figure sono esempi. I numeri di porta effettivi variano a seconda del modello del nodo di storage e dell'utilizzo di adattatori di espansione.



### Informazioni correlate

["Report tecnico NetApp 4684: Implementazione e configurazione di SAN moderne con NVMe-of"](#)

### Upgrade ONTAP per cluster a nodo singolo

A partire da ONTAP 9,2, puoi utilizzare l'interfaccia a riga di comando di ONTAP per eseguire un update automatico di un cluster a nodo singolo. Poiché i cluster a nodo singolo non hanno ridondanza, gli aggiornamenti sono sempre di tipo disgregativo. Non è possibile eseguire upgrade con interruzioni usando System Manager.

### Prima di iniziare

È necessario completare l'aggiornamento ["preparazione"](#) fasi.

### Fasi

1. Eliminare il pacchetto software ONTAP precedente:

```
cluster image package delete -version previous_package_version
```

2. Scarica il pacchetto software ONTAP di destinazione:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz
```

```
Package download completed.
Package processing completed.
```

3. Verificare che il pacchetto software sia disponibile nel repository dei pacchetti del cluster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.7              M/DD/YYYY 10:32:15
```

4. Verificare che il cluster sia pronto per l'aggiornamento:

```
cluster image validate -version package_version_number
```

```
cluster1::> cluster image validate -version 9.7
```

```
WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. Monitorare l'avanzamento della convalida:

```
cluster image show-update-progress
```

6. Completare tutte le azioni richieste identificate dalla convalida.

7. Facoltativamente, generare una stima dell'aggiornamento del software:

```
cluster image update -version package_version_number -estimate-only
```

La stima dell'aggiornamento software visualizza i dettagli relativi a ciascun componente da aggiornare e la durata stimata dell'aggiornamento.

8. Eseguire l'aggiornamento del software:

```
cluster image update -version package_version_number
```



Se si verifica un problema, l'aggiornamento viene messo in pausa e richiede di intraprendere un'azione correttiva. È possibile utilizzare il comando `show-update-progress` dell'immagine del cluster per visualizzare i dettagli relativi a eventuali problemi e allo stato di avanzamento dell'aggiornamento. Dopo aver corretto il problema, è possibile riprendere l'aggiornamento utilizzando il comando `resume-update` dell'immagine del cluster.



9. Visualizzare l'avanzamento dell'aggiornamento del cluster:

```
cluster image show-update-progress
```

Il nodo viene riavviato come parte dell'aggiornamento e non è possibile accedervi durante il riavvio.

10. Attivare una notifica:

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

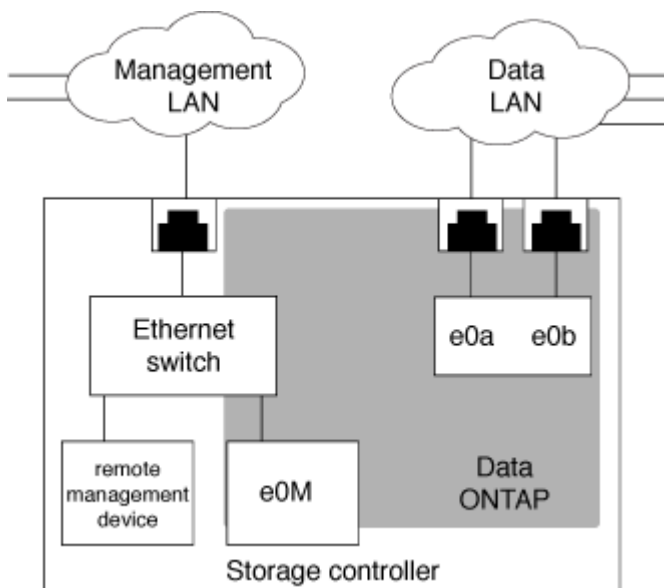
Se il cluster non è configurato per l'invio di messaggi, una copia della notifica viene salvata localmente.

## Configurare la rete SP/BMC

### Isolare il traffico di rete di gestione

Si consiglia di configurare SP/BMC e l'interfaccia di gestione e0M su una subnet dedicata al traffico di gestione. L'esecuzione del traffico dati sulla rete di gestione può causare il peggioramento delle performance e problemi di routing.

La porta Ethernet di gestione della maggior parte dei controller di storage (indicata dall'icona di una chiave a tubo sul retro dello chassis) è collegata a uno switch Ethernet interno. Lo switch interno fornisce la connettività a SP/BMC e all'interfaccia di gestione e0M, che è possibile utilizzare per accedere al sistema di storage tramite protocolli TCP/IP come Telnet, SSH e SNMP.



Se si intende utilizzare sia il dispositivo di gestione remota che e0M, è necessario configurarli sulla stessa subnet IP. Poiché si tratta di interfacce a bassa larghezza di banda, la procedura migliore consiste nel configurare SP/BMC ed e0M su una subnet dedicata al traffico di gestione.

Se non è possibile isolare il traffico di gestione o se la rete di gestione dedicata è insolitamente grande, si consiglia di mantenere il volume di traffico di rete il più basso possibile. Un traffico broadcast o multicast in entrata eccessivo può compromettere le prestazioni di SP/BMC.



Alcuni storage controller, come AFF A800, dispongono di due porte esterne, una per BMC e l'altra per e0M. Per questi controller, non è necessario configurare BMC ed e0M sulla stessa subnet IP.

## Considerazioni per la configurazione di rete SP/BMC

È possibile attivare la configurazione di rete automatica a livello di cluster per l'SP (consigliato). È inoltre possibile lasciare disattivata la configurazione di rete automatica SP (impostazione predefinita) e gestire la configurazione di rete SP manualmente a livello di nodo. Esistono alcune considerazioni per ciascun caso.



Questo argomento si applica sia all'SP che al BMC.

La configurazione automatica della rete SP consente all'SP di utilizzare le risorse di indirizzo (inclusi l'indirizzo IP, la subnet mask e l'indirizzo del gateway) della subnet specificata per configurare automaticamente la rete. Con la configurazione automatica della rete SP, non è necessario assegnare manualmente gli indirizzi IP per l'SP di ciascun nodo. Per impostazione predefinita, la configurazione di rete automatica SP è disattivata, poiché l'abilitazione della configurazione richiede che la subnet venga utilizzata per la configurazione sia definita nel cluster.

Se si attiva la configurazione di rete automatica SP, si applicano le seguenti considerazioni e scenari:

- Se l'SP non è mai stato configurato, la rete SP viene configurata automaticamente in base alla subnet specificata per la configurazione automatica della rete SP.
- Se l'SP è stato precedentemente configurato manualmente o se la configurazione di rete SP esistente si basa su una subnet diversa, la rete SP di tutti i nodi del cluster viene riconfigurata in base alla subnet specificata nella configurazione di rete automatica dell'SP.

La riconfigurazione potrebbe comportare l'assegnazione di un indirizzo diverso al SP, che potrebbe avere un impatto sulla configurazione DNS e sulla capacità di risolvere i nomi host SP. Di conseguenza, potrebbe essere necessario aggiornare la configurazione DNS.

- Un nodo che si unisce al cluster utilizza la subnet specificata per configurare automaticamente la propria rete SP.
- Il `system service-processor network modify` Il comando non consente di modificare l'indirizzo IP SP.

Quando la configurazione di rete automatica SP è attivata, il comando consente solo di attivare o disattivare l'interfaccia di rete SP.

- Se la configurazione di rete automatica SP era precedentemente abilitata, disattivando l'interfaccia di rete SP la risorsa di indirizzo assegnata viene rilasciata e restituita alla subnet.
- Se si disattiva e si riattiva l'interfaccia di rete SP, quest'ultima potrebbe essere riconfigurata con un indirizzo diverso.

Se la configurazione di rete automatica SP è disattivata (impostazione predefinita), si applicano le seguenti situazioni e considerazioni:

- Se l'SP non è mai stato configurato, per impostazione predefinita la configurazione di rete IPv4 SP utilizza DHCP IPv4 e IPv6 è disattivato.

Un nodo che si unisce al cluster utilizza anche IPv4 DHCP per la configurazione di rete SP per impostazione predefinita.

- Il `system service-processor network modify` Il comando consente di configurare l'indirizzo IP SP di un nodo.

Quando si tenta di configurare manualmente la rete SP con gli indirizzi assegnati a una subnet, viene visualizzato un messaggio di avviso. Ignorare l'avviso e procedere con l'assegnazione manuale dell'indirizzo potrebbe comportare uno scenario con indirizzi duplicati.

Se la configurazione di rete automatica SP viene disattivata dopo essere stata attivata in precedenza, si applicano le seguenti situazioni e considerazioni:

- Se la configurazione di rete automatica SP ha la famiglia di indirizzi IPv4 disattivata, la rete SP IPv4 utilizza per impostazione predefinita DHCP e il `system service-processor network modify` Il comando consente di modificare la configurazione SP IPv4 per i singoli nodi.
- Se la configurazione di rete automatica SP ha la famiglia di indirizzi IPv6 disattivata, anche la rete IPv6 SP viene disattivata e il `system service-processor network modify` Il comando consente di attivare e modificare la configurazione di IPv6 SP per i singoli nodi.

### Attivare la configurazione automatica di rete SP/BMC

È preferibile abilitare l'SP per l'utilizzo della configurazione di rete automatica rispetto alla configurazione manuale della rete SP. Poiché la configurazione automatica della rete SP è estesa a tutto il cluster, non è necessario gestire manualmente la rete SP per i singoli nodi.



Questa attività si applica sia all'SP che al BMC.

- La subnet che si desidera utilizzare per la configurazione automatica della rete SP deve essere già definita nel cluster e non deve presentare conflitti di risorse con l'interfaccia di rete SP.

Il `network subnet show` il comando visualizza le informazioni sulla subnet del cluster.

Il parametro che forza l'associazione della subnet (il `-force-update-lif-associations` del parametro `network subnet` ) è supportato solo su LIF di rete e non sull'interfaccia di rete SP.

- Se si desidera utilizzare le connessioni IPv6 per l'SP, IPv6 deve essere già configurato e abilitato per ONTAP.

Il `network options ipv6 show` Il comando visualizza lo stato corrente delle impostazioni IPv6 per ONTAP.

### Fasi

1. Specificare la famiglia di indirizzi IPv4 o IPv6 e il nome della subnet che si desidera utilizzare con l'SP `system service-processor network auto-configuration enable` comando.
2. Visualizzare la configurazione di rete automatica SP utilizzando `system service-processor network auto-configuration show` comando.
3. Se in seguito si desidera disattivare o riabilitare l'interfaccia di rete SP IPv4 o IPv6 per tutti i nodi che si trovano in quorum, utilizzare `system service-processor network modify` con il `-address`

`-family [IPv4|IPv6] e. -enable [true|false].`

Quando la configurazione di rete automatica SP è attivata, non è possibile modificare l'indirizzo IP SP per un nodo che si trova in quorum. È possibile attivare o disattivare solo l'interfaccia di rete SP IPv4 o IPv6.

Se un nodo non ha raggiunto il quorum, è possibile modificare la configurazione di rete SP del nodo, incluso l'indirizzo IP SP, eseguendo `system service-processor network modify` Dal nodo e confermando che si desidera eseguire l'override della configurazione di rete automatica SP per il nodo. Tuttavia, quando il nodo si unisce al quorum, viene eseguita la riconfigurazione automatica dell'SP per il nodo in base alla subnet specificata.

## Configurare la rete SP/BMC manualmente

Se non si dispone della configurazione di rete automatica impostata per l'SP, è necessario configurare manualmente la rete SP di un nodo affinché l'SP sia accessibile utilizzando un indirizzo IP.

### Di cosa hai bisogno

Se si desidera utilizzare le connessioni IPv6 per l'SP, IPv6 deve essere già configurato e abilitato per ONTAP. Il `network options ipv6` I comandi gestiscono le impostazioni IPv6 per ONTAP.



Questa attività si applica sia all'SP che al BMC.

È possibile configurare l'SP in modo che utilizzi IPv4, IPv6 o entrambi. La configurazione SP IPv4 supporta l'indirizzamento statico e DHCP, mentre la configurazione SP IPv6 supporta solo l'indirizzamento statico.

Se è stata impostata la configurazione di rete automatica SP, non è necessario configurare manualmente la rete SP per i singoli nodi e il `system service-processor network modify` Il comando consente di attivare o disattivare solo l'interfaccia di rete SP.

### Fasi

1. Configurare la rete SP per un nodo utilizzando `system service-processor network modify` comando.

- Il `-address-family` Parametro specifica se modificare la configurazione IPv4 o IPv6 dell'SP.
- Il `-enable` Il parametro attiva l'interfaccia di rete della famiglia di indirizzi IP specificata.
- Il `-dhcp` Parametro specifica se utilizzare la configurazione di rete dal server DHCP o dall'indirizzo di rete fornito.

È possibile attivare DHCP (tramite l'impostazione `-dhcp a. v4`) Solo se si utilizza IPv4. Non è possibile attivare DHCP per le configurazioni IPv6.

- Il `-ip-address` Parametro specifica l'indirizzo IP pubblico per l'SP.

Quando si tenta di configurare manualmente la rete SP con gli indirizzi assegnati a una subnet, viene visualizzato un messaggio di avviso. Ignorare l'avviso e procedere con l'assegnazione manuale dell'indirizzo potrebbe causare un'assegnazione duplicata dell'indirizzo.

- Il `-netmask` Parametro specifica la netmask per l'SP (se si utilizza IPv4).
- Il `-prefix-length` Parametro specifica la lunghezza del prefisso di rete della subnet mask per l'SP (se si utilizza IPv6).

- Il `-gateway` Parametro specifica l'indirizzo IP del gateway per l'SP.
2. Configurare la rete SP per i nodi rimanenti nel cluster ripetendo il passaggio 1.
  3. Visualizzare la configurazione di rete SP e verificare lo stato di configurazione SP utilizzando `system service-processor network show` con il `-instance` oppure `-field setup-status` parametri.

Lo stato di setup SP per un nodo può essere uno dei seguenti:

- `not-setup` — non configurato
- `succeeded` — Configurazione riuscita
- `in-progress` — Configurazione in corso
- `failed` — Configurazione non riuscita

### **Esempio di configurazione della rete SP**

Nell'esempio seguente viene configurato l'SP di un nodo per l'utilizzo di IPv4, viene attivato l'SP e viene visualizzata la configurazione di rete SP per verificare le impostazioni:

```

cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

Node: node1
Address Type: IPv4
Interface Enabled: true
Type of Device: SP
Status: online
Link Status: up
DHCP Status: none
IP Address: 192.168.123.98
MAC Address: ab:cd:ef:fe:ed:02
Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: 192.168.123.1
Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
Subnet Name: -
Enable IPv6 Router Assigned Address: -
SP Network Setup Status: succeeded
SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>

```

## Modificare la configurazione del servizio API SP

L'API SP è un'API di rete sicura che consente a ONTAP di comunicare con l'SP sulla rete. È possibile modificare la porta utilizzata dal servizio API SP, rinnovare i certificati utilizzati dal servizio per la comunicazione interna o disattivare completamente il servizio. È necessario modificare la configurazione solo in situazioni rare.

### A proposito di questa attività

- Il servizio API SP utilizza la porta 50000 per impostazione predefinita.

È possibile modificare il valore della porta se, ad esempio, ci si trova in un'impostazione di rete dove porta 50000 Viene utilizzato per la comunicazione da parte di un'altra applicazione di rete oppure si desidera differenziare tra il traffico proveniente da altre applicazioni e il traffico generato dal servizio API SP.

- I certificati SSL e SSH utilizzati dal servizio API SP sono interni al cluster e non distribuiti esternamente.

Nell'improbabile eventualità che i certificati vengano compromessi, è possibile rinnovarli.

- Il servizio API SP è attivato per impostazione predefinita.

È necessario disattivare il servizio API SP solo in situazioni rare, ad esempio in una LAN privata in cui l'SP non è configurato o utilizzato e si desidera disattivare il servizio.

Se il servizio API SP è disattivato, l'API non accetta connessioni in entrata. Inoltre, funzionalità come gli aggiornamenti del firmware SP basati sulla rete e la raccolta di log SP "dOwn System" basata sulla rete non sono più disponibili. Il sistema passa all'utilizzo dell'interfaccia seriale.

## Fasi

1. Passare al livello di privilegio avanzato utilizzando `set -privilege advanced` comando.
2. Modificare la configurazione del servizio API SP:

Se si desidera...	Utilizzare il seguente comando...
Modificare la porta utilizzata dal servizio API SP	<code>system service-processor api-service modify con -port {49152..65535} parametro</code>
Rinnovare i certificati SSL e SSH utilizzati dal servizio API SP per la comunicazione interna	<ul style="list-style-type: none"><li>• Per ONTAP 9.5 o versioni successive <code>system service-processor api-service renew-internal-certificate</code></li><li>• Per ONTAP 9.4 e versioni precedenti</li><li>• <code>system service-processor api-service renew-certificates</code></li></ul> <p>Se non viene specificato alcun parametro, vengono rinnovati solo i certificati host (inclusi i certificati client e server).</p> <p>Se il <code>-renew-all true</code> Viene specificato il parametro, i certificati host e il certificato CA principale vengono rinnovati.</p>
com	
Disattivare o riabilitare il servizio API SP	<code>system service-processor api-service modify con -is-enabled {true</code>

3. Visualizzare la configurazione del servizio API SP utilizzando `system service-processor api-service show` comando.

## Gestire i nodi in remoto utilizzando SP/BMC

### Gestire un nodo in remoto utilizzando la panoramica SP/BMC

È possibile gestire un nodo in remoto utilizzando un controller integrato, denominato

Service Processor (SP) o Baseboard Management Controller (BMC). Questo controller di gestione remota è incluso in tutti gli attuali modelli di piattaforma. Il controller rimane operativo indipendentemente dallo stato operativo del nodo.

Le seguenti piattaforme supportano BMC anziché SP:

- FAS 8700
- FAS 8300
- FAS27x0
- AFF A800
- AFF A700
- AFF A400
- AFF A320
- AFF A220
- AFF C190

### A proposito di SP

Service Processor (SP) è un dispositivo di gestione remota che consente di accedere, monitorare e risolvere i problemi di un nodo in remoto.

Le funzionalità principali del SP includono:

- L'SP consente di accedere a un nodo in remoto per diagnosticare, spegnere, spegnere e riaccendere o riavviare il nodo, indipendentemente dallo stato del controller del nodo.

L'SP è alimentato da una tensione di standby, disponibile a condizione che il nodo abbia alimentazione in ingresso da almeno uno dei suoi alimentatori.

È possibile accedere al SP utilizzando un'applicazione client Secure Shell da un host di amministrazione. È quindi possibile utilizzare l'interfaccia CLI SP per monitorare e risolvere i problemi del nodo in remoto. Inoltre, è possibile utilizzare l'SP per accedere alla console seriale ed eseguire i comandi ONTAP in remoto.

È possibile accedere all'SP dalla console seriale o dalla console seriale dall'SP. SP consente di aprire contemporaneamente una sessione CLI SP e una sessione console separata.

Ad esempio, quando un sensore di temperatura diventa estremamente alto o basso, ONTAP attiva l'SP per spegnere la scheda madre in modo corretto. La console seriale non risponde, ma è comunque possibile premere Ctrl-G sulla console per accedere alla CLI SP. È quindi possibile utilizzare `system power on` oppure `system power cycle` Comando dall'SP per accendere o spegnere e riaccendere il nodo.

- L'SP monitora i sensori ambientali e registra gli eventi per aiutarti a intraprendere azioni di servizio tempestive ed efficaci.

L'SP monitora i sensori ambientali, ad esempio le temperature del nodo, le tensioni, le correnti e la velocità della ventola. Quando un sensore ambientale ha raggiunto una condizione anomala, l'SP registra le letture anomale, notifica il problema a ONTAP e invia avvisi e notifiche "sistema proprio `d`" secondo necessità attraverso un messaggio AutoSupport, indipendentemente dal fatto che il nodo possa inviare messaggi AutoSupport.



L'SP registra anche eventi come l'avanzamento dell'avvio, le modifiche delle FRU (Field Replaceable Unit), gli eventi generati da ONTAP e la cronologia dei comandi SP. È possibile richiamare manualmente un messaggio AutoSupport per includere i file di log SP raccolti da un nodo specifico.

Oltre a generare questi messaggi per conto di un nodo inattivo e allegare informazioni diagnostiche aggiuntive ai messaggi AutoSupport, il SP non ha alcun effetto sulla funzionalità AutoSupport. Le impostazioni di configurazione di AutoSupport e il comportamento del contenuto dei messaggi sono ereditati da ONTAP.



L'SP non si basa su `-transport` impostazione dei parametri di `system node autosupport modify` comando per inviare notifiche. L'SP utilizza solo il protocollo SMTP (Simple Mail Transport Protocol) e richiede la configurazione AutoSupport dell'host per includere le informazioni sull'host di posta.

Se SNMP è attivato, l'SP genera trap SNMP per gli host trap configurati per tutti gli eventi “dproprio sistema”.

- L'SP dispone di un buffer di memoria non volatile che memorizza fino a 4,000 eventi in un registro eventi di sistema (SEL) per facilitare la diagnosi dei problemi.

Il SEL memorizza ogni voce del registro di controllo come evento di audit. Viene memorizzato nella memoria flash integrata dell'SP. L'elenco degli eventi del SEL viene inviato automaticamente dall'SP a destinatari specificati tramite un messaggio AutoSupport.

Il SEL contiene le seguenti informazioni:

- Eventi hardware rilevati dall'SP, ad esempio lo stato del sensore relativo a alimentatori, tensione o altri componenti
  - Errori rilevati dall'SP, ad esempio un errore di comunicazione, un guasto alla ventola o un errore della memoria o della CPU
  - Eventi software critici inviati al SP dal nodo, ad esempio un panico, un errore di comunicazione, un errore di avvio o un “dsistema proprio” attivato dall'utente come risultato dell'emissione del SP `system reset` oppure `system power cycle` comando
- SP monitora la console seriale indipendentemente dal fatto che gli amministratori siano connessi o connessi alla console.

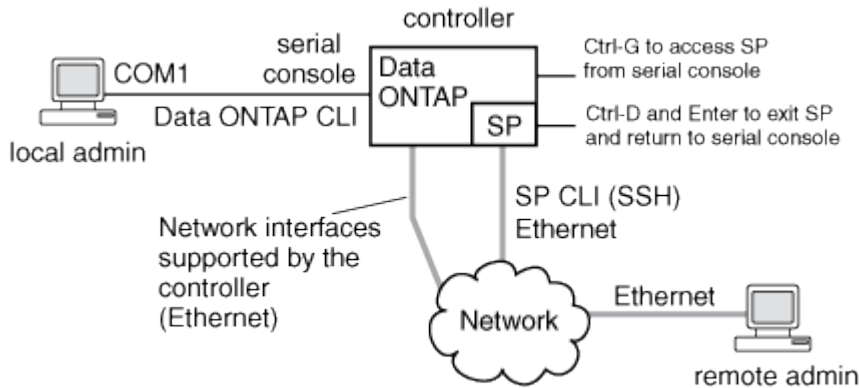
Quando i messaggi vengono inviati alla console, il SP li memorizza nel log della console. Il registro della console rimane attivo fino a quando l'SP è alimentato da uno degli alimentatori del nodo. Poiché l'SP funziona con l'alimentazione in standby, rimane disponibile anche quando il nodo viene spento e riacceso o spento.

- Il Takeover assistito dall'hardware è disponibile se il SP è configurato.
- Il servizio API SP consente a ONTAP di comunicare con il provider di servizi di rete.

Il servizio migliora la gestione ONTAP dell'SP supportando funzionalità basate sulla rete, ad esempio l'utilizzo dell'interfaccia di rete per l'aggiornamento del firmware SP, consentendo a un nodo di accedere alla funzionalità SP di un altro nodo o alla console di sistema e caricando il registro SP da un altro nodo.

È possibile modificare la configurazione del servizio API SP modificando la porta utilizzata dal servizio, rinnovando i certificati SSL e SSH utilizzati dal servizio per la comunicazione interna o disattivando completamente il servizio.

Il seguente diagramma illustra l'accesso a ONTAP e all'SP di un nodo. L'accesso all'interfaccia SP avviene tramite la porta Ethernet (indicata dall'icona di una chiave a tubo sul retro dello chassis):



### Funzionalità di Baseboard Management Controller

A partire da ONTAP 9.1, su alcune piattaforme hardware, il software viene personalizzato per supportare un nuovo controller integrato denominato Baseboard Management Controller (BMC). BMC dispone di comandi CLI (Command-Line Interface) che è possibile utilizzare per gestire il dispositivo in remoto.

Il BMC funziona in modo simile al Service Processor (SP) e utilizza molti degli stessi comandi. BMC consente di effettuare le seguenti operazioni:

- Configurare le impostazioni di rete BMC.
- Accedere a un nodo in remoto ed eseguire attività di gestione dei nodi come diagnosticare, spegnere, spegnere e riaccendere o riavviare il nodo.

Esistono alcune differenze tra SP e BMC:

- Il BMC controlla completamente il monitoraggio ambientale di elementi di alimentazione, elementi di raffreddamento, sensori di temperatura, sensori di tensione e sensori di corrente. Il BMC riporta le informazioni del sensore a ONTAP tramite IPMI.
- Alcuni comandi di alta disponibilità (ha) e storage sono diversi.
- BMC non invia messaggi AutoSupport.

Gli aggiornamenti automatici del firmware sono disponibili anche quando si esegue ONTAP 9.2 GA o versioni successive con i seguenti requisiti:

- È necessario installare la revisione del firmware BMC 1.15 o successiva.



È necessario un aggiornamento manuale per aggiornare il firmware BMC dalla versione 1.12 alla 1.15 o successiva.

- BMC si riavvia automaticamente al termine di un aggiornamento del firmware.



Le operazioni del nodo non vengono influenzate durante il riavvio di BMC.

## Metodi di gestione degli aggiornamenti del firmware SP/BMC

ONTAP include un'immagine del firmware SP denominata *immagine di riferimento*. Se successivamente diventa disponibile una nuova versione del firmware SP, è possibile scaricarla e aggiornarla alla versione scaricata senza aggiornare la versione di ONTAP.



Questo argomento si applica sia all'SP che al BMC.

ONTAP offre i seguenti metodi per la gestione degli aggiornamenti del firmware SP:

- La funzionalità di aggiornamento automatico SP è attivata per impostazione predefinita, consentendo l'aggiornamento automatico del firmware SP nei seguenti scenari:
  - Quando si esegue l'aggiornamento a una nuova versione di ONTAP

Il processo di aggiornamento di ONTAP include automaticamente l'aggiornamento del firmware SP, a condizione che la versione del firmware SP fornita con ONTAP sia più recente della versione SP in esecuzione sul nodo.



ONTAP rileva un aggiornamento automatico SP guasto e attiva un'azione correttiva per riprovare l'aggiornamento automatico SP fino a tre volte. Se tutti e tre i tentativi falliscono, consultare l'articolo della Knowledge base: [Health Monitor SPAutoUpgrade FailedMajorAlert SP upgrade fails - AutoSupport message](#).

- Quando si scarica una versione del firmware SP dal NetApp Support Site e la versione scaricata è più recente di quella attualmente in esecuzione sul SP
- Quando si esegue il downgrade o si torna a una versione precedente di ONTAP

Il firmware SP viene aggiornato automaticamente alla versione più recente compatibile supportata dalla versione di ONTAP a cui si è eseguito il ripristino o il downgrade. Non è richiesto un aggiornamento manuale del firmware SP.

È possibile disattivare la funzionalità di aggiornamento automatico SP utilizzando `system service-processor image modify` comando. Tuttavia, si consiglia di lasciare attivata la funzionalità. La disattivazione della funzionalità può causare combinazioni non ottimali o non qualificate tra l'immagine ONTAP e l'immagine del firmware SP.

- ONTAP consente di attivare manualmente un aggiornamento SP e di specificare la modalità di esecuzione dell'aggiornamento utilizzando `system service-processor image update` comando.

È possibile specificare le seguenti opzioni:

- Il pacchetto firmware SP da utilizzare (`-package`)

È possibile aggiornare il firmware SP a un pacchetto scaricato specificando il nome del file del pacchetto. Il progresso `system image package show` Comando Visualizza tutti i file di pacchetto (inclusi i file per il pacchetto firmware SP) disponibili su un nodo.

- Se utilizzare il pacchetto firmware SP di base per l'aggiornamento SP (`-baseline`)

È possibile aggiornare il firmware SP alla versione di base fornita con la versione attualmente in esecuzione di ONTAP.



Se si utilizzano alcune opzioni o parametri di aggiornamento più avanzati, le impostazioni di configurazione del BMC potrebbero essere temporaneamente cancellate. Dopo il riavvio, ONTAP può impiegare fino a 10 minuti per ripristinare la configurazione BMC.

- ONTAP consente di visualizzare lo stato dell'ultimo aggiornamento del firmware SP attivato da ONTAP utilizzando `system service-processor image update-progress show` comando.

Qualsiasi connessione esistente all'SP viene interrotta quando il firmware dell'SP viene aggiornato. Questo è il caso se l'aggiornamento del firmware SP viene attivato automaticamente o manualmente.

#### Informazioni correlate

["Download NetApp: Firmware di sistema e diagnostica"](#)

#### Quando SP/BMC utilizza l'interfaccia di rete per gli aggiornamenti del firmware

Un aggiornamento del firmware SP attivato da ONTAP con SP con versione 1.5, 2.5, 3.1 o successiva supporta l'utilizzo di un meccanismo di trasferimento file basato su IP sull'interfaccia di rete SP.



Questo argomento si applica sia all'SP che al BMC.

Un aggiornamento del firmware SP tramite l'interfaccia di rete è più veloce di un aggiornamento tramite l'interfaccia seriale. Riduce la finestra di manutenzione durante la quale viene aggiornato il firmware SP e non comporta interruzioni per il funzionamento di ONTAP. Le versioni SP che supportano questa funzionalità sono incluse in ONTAP. Sono inoltre disponibili sul sito di supporto NetApp e possono essere installati su controller che eseguono una versione compatibile di ONTAP.

Se si utilizza SP versione 1.5, 2.5, 3.1 o successiva, si applicano le seguenti procedure di aggiornamento del firmware:

- Un aggiornamento del firmware SP che viene *automaticamente* attivato da ONTAP utilizza per impostazione predefinita l'interfaccia di rete per l'aggiornamento; tuttavia, l'aggiornamento automatico SP passa all'utilizzo dell'interfaccia seriale per l'aggiornamento del firmware se si verifica una delle seguenti condizioni:
  - L'interfaccia di rete SP non è configurata o non è disponibile.
  - Il trasferimento dei file basato su IP non riesce.
  - Il servizio API SP è disattivato.

Indipendentemente dalla versione SP in esecuzione, un aggiornamento del firmware SP attivato dall'interfaccia di rete SP utilizza sempre l'interfaccia di rete SP per l'aggiornamento.

#### Informazioni correlate

["Download NetApp: Firmware di sistema e diagnostica"](#)

#### Account che possono accedere al SP

Quando si tenta di accedere al SP, viene richiesto di immettere le credenziali. Account utente del cluster creati con `service-processor` Il tipo di applicazione ha accesso alla CLI SP su qualsiasi nodo del cluster. Gli account utente SP sono gestiti da ONTAP e autenticati mediante password. A partire da ONTAP 9.9.1, gli account utente SP devono

disporre di `admin` ruolo.

Gli account utente per l'accesso al SP vengono gestiti da ONTAP invece che dall'interfaccia utente di servizio (CLI) SP. Un account utente del cluster può accedere al SP se creato con `-application` del parametro `security login create` comando impostato su `service-processor` e a. `-authmethod` parametro impostato su `password`. L'SP supporta solo l'autenticazione tramite `password`.

Specificare `-role` Parametro durante la creazione di un account utente SP.

- In ONTAP 9.9.1 e versioni successive, è necessario specificare `admin` per `-role` e qualsiasi modifica apportata a un account richiede `admin` ruolo. Altri ruoli non sono più consentiti per motivi di sicurezza.
  - Se si esegue l'aggiornamento a ONTAP 9.9.1 o versioni successive, vedere ["Modifica degli account utente che possono accedere al Service Processor"](#).
  - Se si torna a ONTAP 9.8 o versioni precedenti, vedere ["Verificare gli account utente che possono accedere al Service Processor"](#).
- In ONTAP 9.8 e versioni precedenti, qualsiasi ruolo può accedere al SP, ma `admin` è consigliato.

Per impostazione predefinita, l'account utente del cluster "admin" include `service-processor` Tipo di applicazione e ha accesso al SP.

ONTAP impedisce di creare account utente con nomi riservati al sistema (ad esempio "root" e "naroot"). Non è possibile utilizzare un nome riservato al sistema per accedere al cluster o al SP.

È possibile visualizzare gli account utente SP correnti utilizzando `-application service-processor` del parametro `security login show` comando.

### Accedere a SP/BMC da un host di amministrazione

È possibile accedere all'SP di un nodo da un host di amministrazione per eseguire attività di gestione dei nodi in remoto.

#### Di cosa hai bisogno

Devono essere soddisfatte le seguenti condizioni:

- L'host di amministrazione utilizzato per accedere al SP deve supportare SSHv2.
- L'account utente deve essere già configurato per accedere al SP.

Per accedere al SP, l'account utente deve essere stato creato con `-application` del parametro `security login create` comando impostato su `service-processor` e a. `-authmethod` parametro impostato su `password`.



Questa attività si applica sia all'SP che al BMC.

Se l'SP è configurato per utilizzare un indirizzo IPv4 o IPv6 e se cinque tentativi di accesso SSH da un host falliscono consecutivamente entro 10 minuti, l'SP rifiuta le richieste di accesso SSH e sospende la comunicazione con l'indirizzo IP dell'host per 15 minuti. La comunicazione riprende dopo 15 minuti ed è possibile tentare di nuovo di accedere all'SP.

ONTAP impedisce di creare o utilizzare nomi riservati al sistema (come "root" e "naroot") per accedere al cluster o al SP.

## Fasi

1. Dall'host di amministrazione, accedere all'SP:

```
ssh username@SP_IP_address
```

2. Quando richiesto, immettere la password per `username`.

Viene visualizzato il prompt SP, che indica che si dispone dell'accesso alla CLI SP.

## Esempi di accesso SP da un host di amministrazione

Nell'esempio seguente viene illustrato come accedere al SP con un account utente `joe`, che è stato configurato per accedere al SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

Gli esempi seguenti mostrano come utilizzare l'indirizzo globale IPv6 o l'indirizzo pubblicizzato dal router IPv6 per accedere all'SP su un nodo con SSH impostato per IPv6 e l'SP configurato per IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

## Accedere a SP/BMC dalla console di sistema

È possibile accedere all'SP dalla console di sistema (chiamata anche *console seriale*) per eseguire attività di monitoraggio o risoluzione dei problemi.

### A proposito di questa attività

Questa attività si applica sia all'SP che al BMC.

## Fasi

1. Accedere alla CLI SP dalla console di sistema premendo Ctrl-G al prompt.
2. Accedere all'interfaccia CLI SP quando richiesto.

Viene visualizzato il prompt SP, che indica che si dispone dell'accesso alla CLI SP.

3. Uscire dalla CLI SP e tornare alla console di sistema premendo Ctrl-D, quindi premere Invio.

## Esempio di accesso alla CLI SP dalla console di sistema

L'esempio seguente mostra il risultato della pressione di Ctrl-G dalla console di sistema per accedere alla CLI SP. Il `help system power` Al prompt SP viene immesso il comando, quindi premere Ctrl-D e Invio per tornare alla console di sistema.

```
cluster1::>
```

Premere Ctrl-G per accedere alla CLI SP.

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

Premere Ctrl-D e Invio per tornare alla console di sistema.

```
cluster1::>
```

### Relazione tra le sessioni di SP CLI, console SP e console di sistema

È possibile aprire una sessione SP CLI per gestire un nodo in remoto e aprire una sessione separata della console SP per accedere alla console del nodo. La sessione della console SP esegue il mirroring dell'output visualizzato in una sessione della console di sistema simultanea. SP e la console di sistema dispongono di ambienti shell indipendenti con autenticazione di accesso indipendente.

Comprendere come sono correlate le sessioni di SP CLI, console SP e console di sistema aiuta a gestire un nodo in remoto. Di seguito viene descritta la relazione tra le sessioni:

- Solo un amministratore può accedere alla sessione SP CLI alla volta; tuttavia, il SP consente di aprire contemporaneamente una sessione SP CLI e una sessione SP console separata.

La CLI SP viene indicata con il prompt SP (`SP>`). Da una sessione CLI SP, è possibile utilizzare l'`SP system console` Per avviare una sessione della console SP. Allo stesso tempo, è possibile avviare una sessione CLI SP separata tramite SSH. Se si preme Ctrl-D per uscire dalla sessione della console SP, si torna automaticamente alla sessione della CLI SP. Se esiste già una sessione CLI SP, viene visualizzato un messaggio che chiede se terminare la sessione CLI SP esistente. Se si immette "y", la sessione CLI SP esistente viene terminata, consentendo di tornare dalla console SP alla CLI SP. Questa azione viene registrata nel registro eventi SP.

In una sessione CLI ONTAP connessa tramite SSH, è possibile passare alla console di sistema di un nodo

eseguendo `ONTAP system node run-console` comando da un altro nodo.

- Per motivi di sicurezza, la sessione CLI SP e la sessione della console di sistema dispongono di un'autenticazione di accesso indipendente.

Quando si avvia una sessione della console SP dalla CLI SP (utilizzando l'`SP system console` comando), viene richiesta la credenziale della console di sistema. Quando si accede alla CLI SP da una sessione della console di sistema (premendo Ctrl-G), viene richiesta la credenziale CLI SP.

- La sessione della console SP e la sessione della console di sistema hanno ambienti shell indipendenti.

La sessione della console SP esegue il mirroring dell'output visualizzato in una sessione della console di sistema simultanea. Tuttavia, la sessione della console di sistema simultanea non esegue il mirroring della sessione della console SP.

La sessione della console SP non esegue il mirroring dell'output delle sessioni SSH simultanee.

## Gestire gli indirizzi IP che possono accedere al SP

Per impostazione predefinita, l'SP accetta richieste di connessione SSH da host di amministrazione di qualsiasi indirizzo IP. È possibile configurare l'SP in modo che accetti le richieste di connessione SSH solo dagli host di amministrazione che hanno gli indirizzi IP specificati. Le modifiche apportate si applicano all'accesso SSH all'SP di qualsiasi nodo del cluster.

### Fasi

1. Concedere l'accesso SP solo agli indirizzi IP specificati utilizzando `system service-processor ssh add-allowed-addresses` con il `-allowed-addresses` parametro.
  - Il valore di `-allowed-addresses` il parametro deve essere specificato nel formato di `address/netmask` e multipli `address/netmask` le coppie devono essere separate da virgole, ad esempio `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.
  - Impostazione di `-allowed-addresses` parametro a `0.0.0.0/0, ::/0` Consente a tutti gli indirizzi IP di accedere all'SP (impostazione predefinita).
  - Quando si modifica l'impostazione predefinita limitando l'accesso SP solo agli indirizzi IP specificati, ONTAP richiede di confermare che si desidera che gli indirizzi IP specificati sostituiscano l'impostazione predefinita "Allow All" (`0.0.0.0/0, ::/0`).
  - Il `system service-processor ssh show` Il comando visualizza gli indirizzi IP che possono accedere al SP.
2. Se si desidera impedire a un indirizzo IP specificato di accedere all'SP, utilizzare `system service-processor ssh remove-allowed-addresses` con il `-allowed-addresses` parametro.

Se si impedisce a tutti gli indirizzi IP di accedere al SP, il SP diventa inaccessibile da qualsiasi host di amministrazione.

## Esempi di gestione degli indirizzi IP che possono accedere al SP

I seguenti esempi mostrano l'impostazione predefinita per l'accesso SSH all'SP, modificano l'impostazione predefinita limitando l'accesso SP solo agli indirizzi IP specificati, rimuovono gli indirizzi IP specificati dall'elenco di accesso e ripristinano l'accesso SP per tutti gli indirizzi IP:



```

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
      with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
      addresses will be denied access. To restore the "allow all"
default,
      use the "system service-processor ssh add-allowed-addresses
      -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
      {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

```

## Utilizzare la guida in linea di SP/BMC CLI

La guida in linea visualizza i comandi e le opzioni della CLI SP/BMC.

### A proposito di questa attività

Questa attività si applica sia all'SP che al BMC.

### Fasi

1. Per visualizzare le informazioni della guida per i comandi SP/BMC, immettere quanto segue:

Per accedere alla guida SP...	Per accedere alla guida BMC...
Tipo <code>help</code> Al prompt SP.	Tipo <code>system</code> Al prompt di BMC.

L'esempio seguente mostra la guida in linea di SP CLI.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

L'esempio seguente mostra la guida in linea di BMC CLI.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. Per visualizzare le informazioni della guida relative all'opzione di un comando SP/BMC, immettere `help` Prima o dopo il comando SP/BMC.

L'esempio seguente mostra la guida in linea di SP CLI per `SP events` comando.

```

SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events

```

Nell'esempio seguente viene illustrata la guida in linea di BMC CLI per BMC system power comando.

```

BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>

```

### Comandi per la gestione remota di un nodo


È possibile gestire un nodo in remoto accedendo al relativo SP ed eseguendo comandi SP CLI per eseguire attività di gestione dei nodi. Per diverse attività di gestione remota dei nodi eseguite di frequente, è possibile utilizzare i comandi ONTAP da un altro nodo del cluster. Alcuni comandi SP sono specifici della piattaforma e potrebbero non essere disponibili sulla piattaforma.


Se si desidera...	Utilizza questo comando SP...	Utilizza questo comando BMC...	Oppure questo comando ONTAP ...
Visualizza i comandi SP disponibili o i sottocomandi di un comando SP specificato	help [command]		
Visualizza il livello di privilegio corrente per la CLI SP	priv show		
Impostare il livello di privilegio per accedere alla modalità specificata per la CLI SP	priv set {admin	advanced	diag}
		Visualizzare la data e l'ora del sistema	date

Se si desidera...	Utilizza questo comando SP...	Utilizza questo comando BMC...	Oppure questo comando ONTAP ...
	date	Visualizza gli eventi registrati dall'SP	events {all
info	newest number	oldest number	search keyword}
		Visualizzazione dello stato SP e delle informazioni di configurazione della rete	sp status [-v
-d]  Il -v L'opzione visualizza le statistiche SP in forma dettagliata. Il -d L'opzione aggiunge il registro di debug SP al display.	bmc status [-v	-d]  Il -v L'opzione visualizza le statistiche SP in forma dettagliata. Il -d L'opzione aggiunge il registro di debug SP al display.	system service-processor show
Visualizza il periodo di tempo in cui il SP è rimasto attivo e il numero medio di lavori nella coda di esecuzione negli ultimi 1, 5 e 15 minuti	sp uptime	bmc uptime	
Visualizzare i log della console di sistema	system log		
Visualizzare gli archivi del registro SP o i file in un archivio	sp log history show [-archive {latest	{all	archive-name}} [-dump {all
file-name}}	bmc log history show [-archive {latest	{all	archive-name}} [-dump {all
file-name}}		Visualizza lo stato di alimentazione del controller di un nodo	system power status
	system node power show	Visualizza le informazioni sulla batteria	system battery show
		Visualizza le informazioni ACP o lo stato dei sensori di espansione	system acp [show

Se si desidera...	Utilizza questo comando SP...	Utilizza questo comando BMC...	Oppure questo comando ONTAP ...
sensors show]			Elencare tutte le FRU del sistema e i relativi ID
system fru list			Visualizzare le informazioni sul prodotto per la FRU specificata
system fru show fru_id			Visualizzare il registro della cronologia dei dati FRU
system fru log show (livello di privilegio avanzato)			Visualizzare lo stato dei sensori ambientali, inclusi i relativi stati e valori correnti
system sensors oppure system sensors show		system node environment sensors show	Visualizza lo stato e i dettagli del sensore specificato
system sensors get sensor_name  È possibile ottenere sensor_name utilizzando system sensors o il system sensors show comando.			Visualizza le informazioni sulla versione del firmware SP
version		system service-processor image show	Visualizza la cronologia dei comandi SP
sp log audit (livello di privilegio avanzato)	bmc log audit		Visualizza le informazioni di debug SP
sp log debug (livello di privilegio avanzato)	bmc log debug (livello di privilegio avanzato)		Visualizza il file dei messaggi SP

Se si desidera...	Utilizza questo comando SP...	Utilizza questo comando BMC...	Oppure questo comando ONTAP ...
sp log messages (livello di privilegio avanzato)	bmc log messages (livello di privilegio avanzato)		Consente di visualizzare le impostazioni per la raccolta di dati forensi del sistema in un evento di ripristino del watchdog, visualizzare le informazioni forensi del sistema raccolte durante un evento di ripristino del watchdog o cancellare le informazioni forensi del sistema raccolte
system forensics [show	log dump	log clear]	
	Accedere alla console di sistema	system console	
system node run-console	Premere Ctrl-D per uscire dalla sessione della console di sistema.	Accendere o spegnere il nodo oppure eseguire un ciclo di alimentazione (spegnendo e riaccendendo l'alimentazione)	system power on
	system node power on (livello di privilegio avanzato)	system power off	
	system power cycle		

Se si desidera...	Utilizza questo comando SP...	Utilizza questo comando BMC...	Oppure questo comando ONTAP ...
<p>L'alimentazione in standby rimane attiva per mantenere l'SP in funzione senza interruzioni. Durante il ciclo di alimentazione, si verifica una breve pausa prima di riaccendere il prodotto.</p> <div>  <p>L'utilizzo di questi comandi per spegnere o spegnere e riaccendere il nodo potrebbe causare un arresto non corretto del nodo (chiamato anche <i>shutdown anomalo</i>) e non può sostituire un arresto corretto mediante ONTAP <code>system node halt</code> comando.</p> </div>	<p>Creare un core dump e ripristinare il nodo</p>	<p><code>system core [-f]</code></p> <p>Il <code>-f</code> l'opzione forza la creazione di un core dump e il ripristino del nodo.</p>	

Se si desidera...	Utilizza questo comando SP...	Utilizza questo comando BMC...	Oppure questo comando ONTAP ...
<code>system node coredump trigger</code>  (livello di privilegio avanzato)	Questi comandi hanno lo stesso effetto della pressione del pulsante NMI (non-maskable Interrupt) su un nodo, causando un arresto anomalo del nodo e forzando un dump dei file core quando si arresta il nodo. Questi comandi sono utili quando ONTAP sul nodo è bloccato o non risponde a comandi come <code>system node shutdown</code> . I file core dump generati vengono visualizzati nell'output di <code>system node coredump show</code> comando. L'SP rimane operativo fino a quando l'alimentazione in ingresso al nodo non viene interrotta.	Riavviare il nodo con un'immagine del firmware del BIOS (primaria, di backup o corrente) opzionale per eseguire il ripristino in caso di problemi come un'immagine danneggiata del dispositivo di avvio del nodo	<code>system reset {primary</code>
<code>backup</code>	<code>current}</code>		<code>system node reset con -firmware {primary</code>
<code>backup</code>	<code>current} parameter(livello di privilegio avanzato)</code>  <code>system node reset</code>	<div>  <p>Questa operazione causa un arresto anomalo del nodo.</p> </div> <p>Se non viene specificata alcuna immagine del firmware del BIOS, l'immagine corrente viene utilizzata per il riavvio. L'SP rimane operativo fino a quando l'alimentazione in ingresso al nodo non viene interrotta.</p>	Consente di visualizzare lo stato dell'aggiornamento automatico del firmware della batteria oppure di attivare o disattivare l'aggiornamento automatico del firmware della batteria al successivo avvio SP



Se si desidera...	Utilizza questo comando SP...	Utilizza questo comando BMC...	Oppure questo comando ONTAP ...
system battery auto_update [status	enable	disable]  (livello di privilegio avanzato)	
	Confrontare l'immagine del firmware corrente della batteria con un'immagine del firmware specificata	system battery verify [image_URL]  (livello di privilegio avanzato)  Se image_URL non specificato, viene utilizzata l'immagine del firmware della batteria predefinita per il confronto.	
	Aggiornare il firmware della batteria dall'immagine nella posizione specificata	system battery flash image_URL  (livello di privilegio avanzato)  Utilizzare questo comando se il processo di aggiornamento automatico del firmware della batteria non è riuscito per qualche motivo.	
	Aggiornare il firmware SP utilizzando l'immagine nella posizione specificata	sp update image_URL image_URL non deve superare i 200 caratteri.	bmc update image_URL image_URL non deve superare i 200 caratteri.
system service-processor image update	Riavviare il SP	sp reboot	
system service-processor reboot-sp	Cancellare il contenuto della memoria flash NVRAM	system nvram flash clear (livello di privilegio avanzato)  Questo comando non può essere avviato quando il controller è spento (system power off).	

Se si desidera...	Utilizza questo comando SP...	Utilizza questo comando BMC...	Oppure questo comando ONTAP ...
	Uscire dalla CLI SP	<code>exit</code>	

### Informazioni sulle letture del sensore SP basate sulla soglia e sui valori di stato dell'output del comando dei sensori di sistema

I sensori basati su soglie rilevano periodicamente una vasta gamma di componenti del sistema. SP confronta la lettura di un sensore basato su soglia con i suoi limiti di soglia prefissati che definiscono le condizioni operative accettabili di un componente.

In base alla lettura del sensore, l'SP visualizza lo stato del sensore per consentire il monitoraggio delle condizioni del componente.

Esempi di sensori basati su soglia includono sensori per temperature, tensioni, correnti e velocità delle ventole del sistema. L'elenco specifico dei sensori basati su soglia dipende dalla piattaforma.

I sensori basati su soglia presentano le seguenti soglie, visualizzate nell'output dell'SP `system sensors` comando:

- LCR (Lower Critical)
- LNC (Lower non-critical)
- Uncritical superiore (UNC)
- Superiore critico (UCR)

Un valore del sensore tra LNC e LCR o tra UNC e UCR indica che il componente mostra segni di un problema e che potrebbe verificarsi un guasto al sistema. Pertanto, è consigliabile pianificare presto il servizio di componenti.

Un valore del sensore inferiore a LCR o superiore a UCR indica che il componente non funziona correttamente e che si sta per verificare un guasto al sistema. Pertanto, il componente richiede un'attenzione immediata.

Il seguente diagramma illustra gli intervalli di severità specificati dalle soglie:



La lettura di un sensore basato su soglia si trova sotto `Current` nella colonna `system sensors output` del comando. Il `system sensors get sensor_name` il comando visualizza ulteriori dettagli per il sensore specificato. Quando la lettura di un sensore basato su soglia supera gli intervalli di soglia non critici e critici, il sensore segnala un problema di gravità crescente. Quando il valore supera un limite di soglia, lo stato del sensore in `system sensors` l'output del comando cambia da `ok` a `nc` (non critico) o `cr` (Critico) a seconda del superamento della soglia e della registrazione di un messaggio di evento nel registro eventi SEL.

Alcuni sensori basati su soglia non hanno tutti e quattro i livelli di soglia. Per questi sensori, vengono visualizzate le soglie mancanti `na` come i loro limiti in `system sensors` Output del comando, che indica che il sensore specifico non presenta alcun problema di limite o gravità per la soglia data e che l'SP non monitora il

sensore per tale soglia.

**Esempio di output del comando dei sensori di sistema**

Nell'esempio riportato di seguito vengono illustrate alcune informazioni visualizzate da `system sensors`  
 Nell'interfaccia CLI SP:

```

SP node1> system sensors

Sensor Name      | Current      | Unit         | Status| LCR          | LNC
| UNC          | UCR
-----+-----+-----+-----+-----+
-----+-----+-----+-----+
CPU0_Temp_Margin | -55.000     | degrees C   | ok    | na          | na
| -5.000       | 0.000
CPU1_Temp_Margin | -56.000     | degrees C   | ok    | na          | na
| -5.000       | 0.000
In_Flow_Temp     | 32.000      | degrees C   | ok    | 0.000       | 10.000
| 42.000       | 52.000
Out_Flow_Temp    | 38.000      | degrees C   | ok    | 0.000       | 10.000
| 59.000       | 68.000
CPU1_Error       | 0x0         | discrete    | 0x0180| na          | na
| na           | na
CPU1_Therm_Trip  | 0x0         | discrete    | 0x0180| na          | na
| na           | na
CPU1_Hot         | 0x0         | discrete    | 0x0180| na          | na
| na           | na
IO_Mid1_Temp     | 30.000      | degrees C   | ok    | 0.000       | 10.000
| 55.000       | 64.000
IO_Mid2_Temp     | 30.000      | degrees C   | ok    | 0.000       | 10.000
| 55.000       | 64.000
CPU_VTT          | 1.106       | Volts       | ok    | 1.028       | 1.048
| 1.154        | 1.174
CPU0_VCC         | 1.154       | Volts       | ok    | 0.834       | 0.844
| 1.348        | 1.368
3.3V             | 3.323       | Volts       | ok    | 3.053       | 3.116
| 3.466        | 3.546
5V               | 5.002       | Volts       | ok    | 4.368       | 4.465
| 5.490        | 5.636
STBY_1.8V        | 1.794       | Volts       | ok    | 1.678       | 1.707
| 1.892        | 1.911
...
    
```

**Esempio di output del comando `SENSOR_NAME` dei sensori di sistema per un sensore basato su soglia**

L'esempio seguente mostra il risultato dell'immissione `system sensors get sensor_name` Nella CLI SP  
 per il sensore basato su soglia 5V:

```

SP node1> system sensors get 5V

Locating sensor record...
Sensor ID           : 5V (0x13)
Entity ID           : 7.97
Sensor Type (Analog) : Voltage
Sensor Reading       : 5.002 (+/- 0) Volts
Status               : ok
Lower Non-Recoverable : na
Lower Critical        : 4.246
Lower Non-Critical    : 4.490
Upper Non-Critical    : 5.490
Upper Critical        : 5.758
Upper Non-Recoverable : na
Assertion Events      :
Assertions Enabled    : lnc- lcr- ucr+
Deassertions Enabled  : lnc- lcr- ucr+

```

### Informazioni sui valori di stato del sensore SP discreto dell'output del comando dei sensori di sistema

I sensori discreti non hanno soglie. I relativi valori, visualizzati sotto `Current` Nella colonna `SP CLI system sensors Output` del comando, non portano significati effettivi e quindi vengono ignorati dal SP. Il `Status` nella colonna `system sensors` l'output del comando visualizza i valori di stato dei sensori discreti in formato esadecimale.

Esempi di sensori discreti includono sensori per la ventola, guasti all'alimentatore e guasti al sistema. L'elenco specifico di sensori discreti dipende dalla piattaforma.

È possibile utilizzare la CLI `SP system sensors get sensor_name` comando per l'interpretazione dei valori di stato per la maggior parte dei sensori discreti. I seguenti esempi mostrano i risultati dell'immissione `system sensors get sensor_name` Per i sensori discreti `CPU0_Error` e `io_Slot1_Present`:

```

SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID           : CPU0_Error (0x67)
Entity ID           : 7.97
Sensor Type (Discrete): Temperature
States Asserted      : Digital State
                     [State Deasserted]

```

```

SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID           : IO_Slot1_Present (0x74)
Entity ID          : 11.97
Sensor Type (Discrete): Add-in Card
States Asserted    : Availability State
                    [Device Present]

```

Anche se il `system sensors get sensor_name` Command visualizza le informazioni di stato per la maggior parte dei sensori discreti, non fornisce informazioni di stato per i sensori discreti `System_FW_Status`, `System_Watchdog`, `PSU1_Input_Type` e `PSU2_Input_Type`. È possibile utilizzare le seguenti informazioni per interpretare i valori di stato di questi sensori.

### System\_FW\_Status

La condizione del sensore `System_FW_Status` viene visualizzata sotto forma di `0xAABB`. È possibile combinare le informazioni di `AA` e `BB` per determinare le condizioni del sensore.

`AA` può avere uno dei seguenti valori:

Valori	Condizione del sensore
01	Errore del firmware di sistema
02	Il firmware di sistema si blocca
04	Avanzamento del firmware di sistema

`BB` può avere uno dei seguenti valori:

Valori	Condizione del sensore
00	Il software di sistema si è arrestato correttamente
01	Inizializzazione della memoria in corso
02	Inizializzazione NVMEM in corso (quando è presente NVMEM)
04	Ripristino dei valori MCH (Memory Controller Hub) (quando è presente NVMEM)
05	L'utente ha inserito il programma di installazione
13	Avviare il sistema operativo o IL CARICATORE

Valori	Condizione del sensore
1F	BIOS in fase di avvio
20	IL CARICATORE è in esecuzione
21	IL CARICATORE sta programmando il firmware principale del BIOS. Non spegnere il sistema.
22	IL CARICATORE sta programmando il firmware alternativo del BIOS. Non spegnere il sistema.
2F	ONTAP è in esecuzione
60	SP ha spento il sistema
61	SP ha acceso il sistema
62	SP ha ripristinato il sistema
63	Spegnere e riaccendere il watchdog SP
64	Ripristino a freddo del watchdog SP

Ad esempio, lo stato del sensore System\_FW\_Status 0x042F indica "System firmware Progress (04), ONTAP is running (2F)" (avanzamento del firmware di sistema ()).

#### System\_Watchdog

Il sensore System\_Watchdog può avere una delle seguenti condizioni:

- **0x0080**

Lo stato di questo sensore non è cambiato

Valori	Condizione del sensore
0x0081	Interruzione del timer
0x0180	Timer scaduto
0x0280	Reimpostazione a freddo
0x0480	Spegnere
0x0880	Spegnere e riaccendere

Ad esempio, lo stato del sensore System\_Watchdog 0x0880 indica che si verifica un timeout di watchdog e provoca un ciclo di alimentazione del sistema.

#### PSU1\_Input\_Type e PSU2\_Input\_Type

Per gli alimentatori a corrente continua (CC), i sensori PSU1\_Input\_Type e PSU2\_Input\_Type non sono applicabili. Per gli alimentatori a corrente alternata (CA), lo stato dei sensori può avere uno dei seguenti valori:

Valori	Condizione del sensore
0x01 xx	Tipo di PSU da 220 V.
0x02 xx	Tipo di PSU da 110 V.

Ad esempio, lo stato del sensore PSU1\_Input\_Type 0x0280 indica che il sensore segnala che il tipo di PSU è 110 V.

#### Comandi per la gestione dell'SP da ONTAP

ONTAP fornisce comandi per la gestione dell'SP, tra cui la configurazione della rete SP, l'immagine del firmware SP, l'accesso SSH all'SP e l'amministrazione generale dell'SP.

#### Comandi per la gestione della configurazione di rete SP

Se si desidera...	Eseguire questo comando ONTAP...
Abilitare la configurazione di rete automatica SP per l'SP per utilizzare la famiglia di indirizzi IPv4 o IPv6 della subnet specificata	<code>system service-processor network auto-configuration enable</code>
Disattiva la configurazione di rete automatica SP per la famiglia di indirizzi IPv4 o IPv6 della subnet specificata per l'SP	<code>system service-processor network auto-configuration disable</code>
Visualizza la configurazione di rete automatica SP	<code>system service-processor network auto-configuration show</code>


Se si desidera...	Eeguire questo comando ONTAP...
<p>Configurare manualmente la rete SP per un nodo, tra cui:</p> <ul style="list-style-type: none"> <li>• La famiglia di indirizzi IP (IPv4 o IPv6)</li> <li>• Se attivare l'interfaccia di rete della famiglia di indirizzi IP specificata</li> <li>• Se si utilizza IPv4, specificare se utilizzare la configurazione di rete dal server DHCP o l'indirizzo di rete specificato</li> <li>• L'indirizzo IP pubblico per l'SP</li> <li>• La netmask per l'SP (se si utilizza IPv4)</li> <li>• La lunghezza del prefisso di rete della subnet mask per l'SP (se si utilizza IPv6)</li> <li>• L'indirizzo IP del gateway per l'SP</li> </ul>	<p><code>system service-processor network modify</code></p>
<p>Visualizzare la configurazione di rete SP, tra cui:</p> <ul style="list-style-type: none"> <li>• La famiglia di indirizzi configurata (IPv4 o IPv6) e se è attivata</li> <li>• Il tipo di dispositivo di gestione remota</li> <li>• Lo stato SP corrente e lo stato del collegamento</li> <li>• Configurazione di rete, ad esempio indirizzo IP, indirizzo MAC, netmask, lunghezza prefisso della subnet mask, indirizzo IP assegnato dal router, indirizzo IP locale di collegamento e indirizzo IP del gateway</li> <li>• L'ora dell'ultimo aggiornamento del SP</li> <li>• Il nome della subnet utilizzata per la configurazione automatica SP</li> <li>• Se l'indirizzo IP assegnato dal router IPv6 è attivato</li> <li>• Stato di setup della rete SP</li> <li>• Motivo dell'errore di configurazione della rete SP</li> </ul>	<p><code>system service-processor network show</code></p> <p>La visualizzazione dei dettagli completi della rete SP richiede <code>-instance</code> parametro.</p>
<p>Modificare la configurazione del servizio API SP, includendo quanto segue:</p> <ul style="list-style-type: none"> <li>• Modifica della porta utilizzata dal servizio API SP</li> <li>• Attivazione o disattivazione del servizio API SP</li> </ul>	<p><code>system service-processor api-service modify</code></p> <p>(livello di privilegio avanzato)</p>



Se si desidera...	Eseguire questo comando ONTAP...
Visualizzare la configurazione del servizio API SP	<pre>system service-processor api-service show</pre> <p>(livello di privilegio avanzato)</p>
Rinnovare i certificati SSL e SSH utilizzati dal servizio API SP per la comunicazione interna	<ul style="list-style-type: none"> <li>• Per ONTAP 9.5 o versioni successive: <pre>system service-processor api-service renew-internal-certificates</pre></li> <li>• Per ONTAP 9.4 o versioni precedenti: <pre>system service-processor api-service renew-certificates</pre></li> </ul> <p>(livello di privilegio avanzato)</p>

#### Comandi per la gestione dell'immagine del firmware SP

Se si desidera...	Eseguire questo comando ONTAP...
<p>Visualizza i dettagli dell'immagine del firmware SP attualmente installata, tra cui:</p> <ul style="list-style-type: none"> <li>• Il tipo di dispositivo di gestione remota</li> <li>• L'immagine (principale o di backup) da cui viene avviato il SP, il suo stato e la versione del firmware</li> <li>• Se l'aggiornamento automatico del firmware è attivato e lo stato dell'ultimo aggiornamento</li> </ul>	<pre>system service-processor image show</pre> <p>Il <code>-is-current</code> Parametro indica l'immagine (primaria o di backup) da cui è attualmente avviato il SP, non se la versione del firmware installata è più recente.</p>
Attiva o disattiva l'aggiornamento automatico del firmware SP	<pre>system service-processor image modify</pre> <p>Per impostazione predefinita, il firmware SP viene aggiornato automaticamente con l'aggiornamento di ONTAP o quando viene scaricata manualmente una nuova versione del firmware SP. La disattivazione dell'aggiornamento automatico non è consigliata, in quanto può causare combinazioni non ottimali o non qualificate tra l'immagine ONTAP e l'immagine del firmware SP.</p>

Se si desidera...	Eeguire questo comando ONTAP...
Scaricare manualmente un'immagine del firmware SP su un nodo	<pre>system node image get</pre> <div>  <p>Prima di eseguire <code>system node image</code> è necessario impostare il livello di privilegio su <code>advanced</code> (avanzato) (<code>set -privilege advanced</code>), immettendo <b>y</b> quando viene richiesto di continuare.</p> </div> <p>L'immagine del firmware SP viene fornita con ONTAP. Non è necessario scaricare manualmente il firmware SP, a meno che non si desideri utilizzare una versione del firmware SP diversa da quella fornita con ONTAP.</p>
Visualizza lo stato dell'ultimo aggiornamento del firmware SP attivato da ONTAP, incluse le seguenti informazioni: <ul style="list-style-type: none"> <li>• L'ora di inizio e di fine dell'ultimo aggiornamento del firmware SP</li> <li>• Se è in corso un aggiornamento e la percentuale di completamento</li> </ul>	<pre>system service-processor image update-progress show</pre>

#### Comandi per la gestione dell'accesso SSH al SP

Se si desidera...	Eeguire questo comando ONTAP...
Concedere l'accesso SP solo agli indirizzi IP specificati	<pre>system service-processor ssh add-allowed-addresses</pre>
Impedisce agli indirizzi IP specificati di accedere al SP	<pre>system service-processor ssh remove-allowed-addresses</pre>
Visualizza gli indirizzi IP che possono accedere all'SP	<pre>system service-processor ssh show</pre>

#### Comandi per l'amministrazione SP generale

Se si desidera...	Eeguire questo comando ONTAP...
Visualizza informazioni generali sull'SP, tra cui: <ul style="list-style-type: none"> <li>• Il tipo di dispositivo di gestione remota</li> <li>• Lo stato SP corrente</li> <li>• Se la rete SP è configurata</li> <li>• Informazioni di rete, ad esempio l'indirizzo IP pubblico e l'indirizzo MAC</li> <li>• La versione del firmware SP e la versione dell'interfaccia di gestione della piattaforma intelligente (IPMI)</li> <li>• Se l'aggiornamento automatico del firmware SP è attivato</li> </ul>	<code>system service-processor show</code> La visualizzazione delle informazioni SP complete richiede <code>-instance</code> parametro.
Riavviare il SP su un nodo	<code>system service-processor reboot-sp</code>
Generare e inviare un messaggio AutoSupport che includa i file di log SP raccolti da un nodo specificato	<code>system node autosupport invoke-splog</code>
Visualizzare la mappa di allocazione dei file di log SP raccolti nel cluster, inclusi i numeri di sequenza dei file di log SP che risiedono in ciascun nodo di raccolta	<code>system service-processor log show-allocations</code>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

#### Comandi ONTAP per la gestione BMC

Questi comandi ONTAP sono supportati dal Baseboard Management Controller (BMC).

Il BMC utilizza alcuni degli stessi comandi del Service Processor (SP). I seguenti comandi SP sono supportati su BMC.

Se si desidera...	Utilizzare questo comando
Visualizzare le informazioni BMC	<code>system service-processor show</code>
Visualizzare/modificare la configurazione di rete BMC	<code>system service-processor network show/modify</code>
Ripristinare il BMC	<code>system service-processor reboot-sp</code>
Consente di visualizzare/modificare i dettagli dell'immagine del firmware BMC attualmente installata	<code>system service-processor image show/modify</code>

Se si desidera...	Utilizzare questo comando
Aggiornare il firmware BMC	<code>system service-processor image update</code>
Visualizza lo stato dell'ultimo aggiornamento del firmware BMC	<code>system service-processor image update-progress show</code>
Abilitare la configurazione di rete automatica per il BMC per l'utilizzo di un indirizzo IPv4 o IPv6 nella subnet specificata	<code>system service-processor network auto-configuration enable</code>
Disattivare la configurazione di rete automatica per un indirizzo IPv4 o IPv6 nella subnet specificata per BMC	<code>system service-processor network auto-configuration disable</code>
Visualizza la configurazione automatica di rete BMC	<code>system service-processor network auto-configuration show</code>

Per i comandi non supportati dal firmware BMC, viene visualizzato il seguente messaggio di errore.

```
::> Error: Command not supported on this platform.
```

## Comandi BMC CLI

È possibile accedere al BMC utilizzando SSH. I seguenti comandi sono supportati dalla riga di comando BMC.

Comando	Funzione
sistema	Visualizza un elenco di tutti i comandi.
console di sistema	Connettersi alla console del sistema. Utilizzare Ctrl+D per uscire dalla sessione.
core di sistema	Eseguire il dump del core di sistema e ripristinarlo.
spegnere e riaccendere il sistema	Spegnere e riaccendere il sistema.
spegnimento del sistema	Spegnere il sistema.
accensione del sistema	Accendere il sistema.
stato di alimentazione del sistema	Stampare lo stato di alimentazione del sistema.
ripristino del sistema	Ripristinare il sistema.

Comando	Funzione
log di sistema	Stampare i registri della console del sistema
fru di sistema mostra [id]	Scarica tutte le informazioni FRU (Field Replaceable Unit) selezionate.

## Gestire il tempo del cluster (solo amministratori del cluster)

I problemi possono verificarsi quando il tempo del cluster non è preciso. Sebbene ONTAP consenta di impostare manualmente fuso orario, data e ora sul cluster, è necessario configurare i server NTP (Network Time Protocol) per sincronizzare l'ora del cluster.

A partire da ONTAP 9.5, è possibile configurare il server NTP con autenticazione simmetrica.

NTP è sempre attivato. Tuttavia, la configurazione è ancora necessaria per la sincronizzazione del cluster con un'origine temporale esterna. ONTAP consente di gestire la configurazione NTP del cluster nei seguenti modi:

- È possibile associare al cluster un massimo di 10 server NTP esterni (`cluster time-service ntp server create`).
  - Per garantire la ridondanza e la qualità del servizio nel tempo, è necessario associare almeno tre server NTP esterni al cluster.
  - È possibile specificare un server NTP utilizzando il relativo indirizzo IPv4 o IPv6 o il nome host completo.
  - È possibile specificare manualmente la versione NTP (v3 o v4) da utilizzare.

Per impostazione predefinita, ONTAP seleziona automaticamente la versione di NTP supportata per un determinato server NTP esterno.

Se la versione NTP specificata non è supportata per il server NTP, non è possibile eseguire lo scambio di ore.

- A livello di privilegi avanzati, è possibile specificare un server NTP esterno associato al cluster come origine temporale principale per la correzione e la regolazione dell'ora del cluster.
- È possibile visualizzare i server NTP associati al cluster (`cluster time-service ntp server show`).
- È possibile modificare la configurazione NTP del cluster (`cluster time-service ntp server modify`).
- È possibile disassociare il cluster da un server NTP esterno (`cluster time-service ntp server delete`).
- A livello di privilegi avanzati, è possibile ripristinare la configurazione annullando l'associazione di tutti i server NTP esterni al cluster (`cluster time-service ntp server reset`).


Un nodo che si unisce a un cluster adotta automaticamente la configurazione NTP del cluster.

Oltre a utilizzare NTP, ONTAP consente anche di gestire manualmente il tempo del cluster. Questa funzionalità è utile quando è necessario correggere un tempo errato (ad esempio, l'ora di un nodo è diventata significativamente errata dopo un riavvio). In tal caso, è possibile specificare un periodo di tempo

approssimativo per il cluster fino a quando NTP non può essere sincronizzato con un server di riferimento orario esterno. Il tempo impostato manualmente ha effetto su tutti i nodi del cluster.

È possibile gestire manualmente l'ora del cluster nei seguenti modi:

- È possibile impostare o modificare il fuso orario, la data e l'ora sul cluster (`cluster date modify`).
- È possibile visualizzare le impostazioni correnti di fuso orario, data e ora del cluster (`cluster date show`).




Le pianificazioni dei processi non si adattano alle modifiche manuali di data e ora del cluster. Questi processi vengono pianificati per essere eseguiti in base all'ora corrente del cluster in cui è stato creato il processo o quando è stato eseguito più di recente. Pertanto, se si modifica manualmente la data o l'ora del cluster, è necessario utilizzare `job show` e `job history show` comandi per verificare che tutti i processi pianificati siano messi in coda e completati in base alle proprie esigenze.



Comandi per la gestione del tempo del cluster

Si utilizza `cluster time-service ntp server` Comandi per gestire i server NTP per il cluster. Si utilizza `cluster date` comandi per gestire manualmente l'ora del cluster.

A partire da ONTAP 9.5, è possibile configurare il server NTP con autenticazione simmetrica.

I seguenti comandi consentono di gestire i server NTP per il cluster:

Se si desidera...	Utilizzare questo comando...
Associare il cluster a un server NTP esterno senza autenticazione simmetrica	<code>cluster time-service ntp server create -server server_name</code>
Associare il cluster a un server NTP esterno con autenticazione simmetrica disponibile in ONTAP 9.5 o versione successiva	<div><div></div><div>Il <code>key_id</code> deve fare riferimento a una chiave condivisa esistente configurata con <code>'chiave ntp cluster time-service'</code>.</div></div> <code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Abilitare l'autenticazione simmetrica per un server NTP esistente. È possibile modificare il server NTP esistente per abilitare l'autenticazione aggiungendo l'ID chiave richiesto.  Disponibile in ONTAP 9.5 o versione successiva	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
Disattiva autenticazione simmetrica	<code>cluster time-service ntp server modify -server server_name -is-authentication-enabled false</code>

Se si desidera...	Utilizzare questo comando...
Configurare una chiave NTP condivisa	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>Le chiavi condivise sono indicate da un ID. L'ID, il tipo e il valore devono essere identici sia sul nodo che sul server NTP</p> </div>
Visualizza le informazioni sui server NTP associati al cluster	<pre>cluster time-service ntp server show</pre>
Modificare la configurazione di un server NTP esterno associato al cluster	<pre>cluster time-service ntp server modify</pre>
Dissocare un server NTP dal cluster	<pre>cluster time-service ntp server delete</pre>
Ripristinare la configurazione annullando l'associazione di tutti i server NTP esterni al cluster	<pre>cluster time-service ntp server reset</pre> <div>  <p>Questo comando richiede il livello di privilegio avanzato.</p> </div>

I seguenti comandi consentono di gestire manualmente l'ora del cluster:

Se si desidera...	Utilizzare questo comando...
Impostare o modificare il fuso orario, la data e l'ora	<pre>cluster date modify</pre>
Visualizza le impostazioni relative a fuso orario, data e ora del cluster	<pre>cluster date show</pre>

## Informazioni correlate

["Comandi di ONTAP 9"](#)

## Gestire il banner e MOTD

### Gestire il banner e la panoramica MOTD

ONTAP consente di configurare un banner di accesso o un messaggio del giorno (MOTD) per comunicare le informazioni amministrative agli utenti CLI del cluster o della macchina virtuale di storage (SVM).

Un banner viene visualizzato in una sessione della console (solo per l'accesso al cluster) o in una sessione SSH (per l'accesso al cluster o alla SVM) prima che venga richiesto all'utente di eseguire l'autenticazione, ad esempio una password. Ad esempio, è possibile utilizzare il banner per visualizzare un messaggio di avviso come il seguente a qualcuno che tenta di accedere al sistema:

```
$ ssh admin@cluster1-01
```

```
This system is for authorized users only. Your IP Address has been logged.
```

```
Password:
```

Un MOTD viene visualizzato in una sessione della console (solo per l'accesso al cluster) o in una sessione SSH (per l'accesso al cluster o a SVM) dopo l'autenticazione di un utente, ma prima della visualizzazione del prompt della shell del cluster. Ad esempio, è possibile utilizzare MOTD per visualizzare un messaggio di benvenuto o informativo, ad esempio:

```
$ ssh admin@cluster1-01
```

```
Password:
```

```
Greetings. This system is running ONTAP 9.0.
```

```
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015  
from 10.72.137.28.
```

È possibile creare o modificare il contenuto del banner o di MOTD utilizzando `security login banner modify` oppure `security login motd modify` di comando, rispettivamente, nei seguenti modi:

- È possibile utilizzare la CLI in modo interattivo o non interattivo per specificare il testo da utilizzare per il banner o MOTD.

La modalità interattiva, avviata quando si utilizza il comando senza `-message` oppure `-uri` parametro, consente di utilizzare newline (note anche come fine delle righe) nel messaggio.

La modalità non interattiva, che utilizza `-message` parametro per specificare la stringa del messaggio, non supporta newlines.

- È possibile caricare il contenuto da una posizione FTP o HTTP da utilizzare per il banner o MOTD.
- È possibile configurare il MOTD per visualizzare il contenuto dinamico.

Di seguito sono riportati alcuni esempi di elementi che è possibile configurare per la visualizzazione dinamica di MOTD:

- Nome del cluster, nome del nodo o nome SVM
- Data e ora del cluster
- Nome dell'utente che effettua l'accesso
- Ultimo accesso per l'utente su qualsiasi nodo del cluster
- Nome o indirizzo IP del dispositivo di accesso
- Nome del sistema operativo
- Versione del software
- Stringa della versione effettiva del cluster `security login motd modify` La pagina man descrive



le sequenze di escape che è possibile utilizzare per consentire a MOTD di visualizzare il contenuto generato dinamicamente.

Il banner non supporta il contenuto dinamico.

È possibile gestire il banner e il MOTD a livello di cluster o SVM:

- I seguenti fatti si applicano al banner:
  - Il banner configurato per il cluster viene utilizzato anche per tutte le SVM che non hanno un messaggio banner definito.
  - È possibile configurare un banner a livello di SVM per ogni SVM.

Se è stato configurato un banner a livello di cluster, questo viene ignorato dal banner a livello di SVM per la SVM indicata.

- I seguenti fatti si applicano al MOTD:
  - Per impostazione predefinita, il MOTD configurato per il cluster è abilitato anche per tutte le SVM.
  - Inoltre, è possibile configurare un MOTD a livello di SVM per ogni SVM.

In questo caso, gli utenti che accedono a SVM vedranno due MOTD, uno definito a livello di cluster e l'altro a livello di SVM.

- Il MOTD a livello di cluster può essere attivato o disattivato per SVM dall'amministratore del cluster.

Se l'amministratore del cluster disattiva il MOTD a livello di cluster per una SVM, un utente che accede a SVM non vedrà il MOTD a livello di cluster.

## Creare un banner

È possibile creare un banner per visualizzare un messaggio a qualcuno che tenta di accedere al cluster o alla SVM. Il banner viene visualizzato in una sessione della console (solo per l'accesso al cluster) o in una sessione SSH (per l'accesso al cluster o alla SVM) prima che venga richiesta l'autenticazione a un utente.

### Fasi

1. Utilizzare `security login banner modify` Comando per creare un banner per il cluster o SVM:

Se si desidera...	Quindi...
Specificare un messaggio che sia una singola riga	Utilizzare <code>-message "text"</code> per specificare il testo.
Includere le newline (note anche come fine delle righe) nel messaggio	Utilizzare il comando senza <code>-message</code> oppure <code>-uri</code> parametro per avviare la modalità interattiva per la modifica del banner.
Carica il contenuto da una posizione da utilizzare per il banner	Utilizzare <code>-uri</code> Parametro per specificare la posizione FTP o HTTP del contenuto.

La dimensione massima di un banner è di 2,048 byte, incluse le newline.

Banner creato utilizzando `-uri` il parametro è statico. Non viene aggiornato automaticamente per riflettere le modifiche successive del contenuto di origine.

Il banner creato per il cluster viene visualizzato anche per tutte le SVM che non dispongono di un banner esistente. Qualsiasi banner creato successivamente per una SVM sovrascrive il banner a livello di cluster per tale SVM. Specifica di `-message` parametro con un trattino tra virgolette doppie ("`-`") Per SVM ripristina la SVM per l'utilizzo del banner a livello di cluster.

2. Verificare che il banner sia stato creato visualizzandolo con `security login banner show` comando.

Specifica di `-message` parametro con una stringa vuota ("`"`") visualizza i banner che non hanno contenuto.

Specifica di `-message` parametro con "`-`" Visualizza tutte le SVM (admin o data) che non hanno un banner configurato.

### Esempi di creazione di banner

Nell'esempio seguente viene utilizzata la modalità non interattiva per creare un banner per il cluster "cluster1":

```
cluster1::> security login banner modify -message "Authorized users only!"  
  
cluster1::>
```

Nell'esempio seguente viene utilizzata la modalità interattiva per creare un banner per "svm1" SVM:

```
cluster1::> security login banner modify -vserver svm1  
  
Enter the message of the day for Vserver "svm1".  
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to  
abort.  
0          1          2          3          4          5          6          7  
8  
1234567890123456789012345678901234567890123456789012345678901234  
567890  
The svm1 SVM is reserved for authorized users only!  
  
cluster1::>
```

Nell'esempio seguente vengono visualizzati i banner creati:

```

cluster1::> security login banner show
Vserver: cluster1
Message
-----
---
Authorized users only!

Vserver: svm1
Message
-----
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>

```

## Informazioni correlate

[Gestione del banner](#)

## Gestione del banner

È possibile gestire il banner a livello di cluster o SVM. Il banner configurato per il cluster viene utilizzato anche per tutte le SVM che non hanno un messaggio banner definito. Un banner creato successivamente per una SVM sovrascrive il banner del cluster per tale SVM.

## Scelte

- Gestire il banner a livello di cluster:

Se si desidera...	Quindi...
Creare un banner da visualizzare per tutte le sessioni di accesso CLI	Impostare un banner a livello di cluster:  `*security login banner modify -vserver <i>cluster_name</i> { [-message "text"]
<code>[-uri ftp_or_http_addr] }*</code>	Rimuovere il banner per tutti gli accessi (cluster e SVM)
Impostare il banner su una stringa vuota (""):  <b>security login banner modify -vserver * -message ""</b>	Eseguire l'override di un banner creato da un amministratore SVM

Se si desidera...	Quindi...
Modificare il messaggio banner SVM:  `*security login banner modify -vserver <i>svm_name</i> { [-message " <i>text</i> "]	[-uri <i>ftp_or_http_addr</i> ] }*

- Gestire il banner a livello di SVM:

Specificare `-vserver svm_name` Non è richiesto nel contesto SVM.

Se si desidera...	Quindi...
Eseguire l'override del banner fornito dall'amministratore del cluster con un banner diverso per SVM	Creare un banner per SVM:  `*security login banner modify -vserver <i>svm_name</i> { [-message " <i>text</i> "]
[-uri <i>ftp_or_http_addr</i> ] }*	Eliminare il banner fornito dall'amministratore del cluster in modo che non venga visualizzato alcun banner per SVM
Impostare il banner SVM su una stringa vuota per SVM:  <b>security login banner modify -vserver <i>svm_name</i> -message ""</b>	Utilizzare il banner a livello di cluster quando SVM utilizza attualmente un banner a livello di SVM

## Creare un MOTD

È possibile creare un messaggio del giorno (MOTD) per comunicare informazioni agli utenti CLI autenticati. Il MOTD viene visualizzato in una sessione della console (solo per l'accesso al cluster) o in una sessione SSH (per l'accesso al cluster o alla SVM) dopo l'autenticazione di un utente, ma prima della visualizzazione del prompt della shell del cluster.

### Fasi

1. Utilizzare `security login motd modify` Comando per creare un MOTD per il cluster o SVM:

Se si desidera...	Quindi...
Specificare un messaggio che sia una singola riga	Utilizzare <code>-message "<i>text</i>"</code> per specificare il testo.
Includi newline (nota anche come fine delle righe)	Utilizzare il comando senza <code>-message</code> oppure <code>-uri</code> Parametro per avviare la modalità interattiva per la modifica del MOTD.

Se si desidera...	Quindi...
Caricare il contenuto da una posizione da utilizzare per il MOTD	Utilizzare <code>-uri</code> Parametro per specificare la posizione FTP o HTTP del contenuto.

La dimensione massima di un MOTD è di 2,048 byte, incluse le newline.

Il `security login motd modify` La pagina man descrive le sequenze di escape che è possibile utilizzare per consentire a MOTD di visualizzare il contenuto generato dinamicamente.

Un MOTD creato utilizzando `-uri` il parametro è statico. Non viene aggiornato automaticamente per riflettere le modifiche successive del contenuto di origine.

Un MOTD creato per il cluster viene visualizzato anche per tutti gli accessi SVM per impostazione predefinita, insieme a un MOTD a livello di SVM che è possibile creare separatamente per un determinato SVM. Impostazione di `-is-cluster-message-enabled` parametro a `false` Per una SVM impedisce la visualizzazione del MOTD a livello di cluster per tale SVM.

2. Verificare che il MOTD sia stato creato visualizzandolo con il `security login motd show` comando.

Specifica di `-message` parametro con una stringa vuota (`""`) Visualizza i MOTD non configurati o privi di contenuto.

Vedere "[modifica del motd di accesso di sicurezza](#)" Pagina man Command per un elenco di parametri da utilizzare per consentire a MOTD di visualizzare il contenuto generato dinamicamente. Controllare la pagina man specifica della versione di ONTAP.

## Esempi di creazione di MOTD

Nell'esempio seguente viene utilizzata la modalità non interattiva per creare un MOTD per il cluster "cluster1":

```
cluster1::> security login motd modify -message "Greetings!"
```

Nell'esempio seguente viene utilizzata la modalità interattiva per creare un MOTD per la SVM "svm1" che utilizza sequenze di escape per visualizzare il contenuto generato dinamicamente:

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0          1          2          3          4          5          6          7
8
1234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

Nell'esempio seguente vengono visualizzati i MOTD creati:

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-----
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-----
---
Welcome to the \n SVM.  Your user ID is '\N'.  Your last successful login
was \L.

2 entries were displayed.
```

**Gestire il MOTD**

È possibile gestire il messaggio del giorno (MOTD) a livello di cluster o SVM. Per impostazione predefinita, il MOTD configurato per il cluster è abilitato anche per tutte le SVM. Inoltre, è possibile configurare un MOTD a livello di SVM per ogni SVM. Il MOTD a livello di cluster può essere attivato o disattivato per ogni SVM dall'amministratore del cluster.

Per un elenco delle sequenze di escape che possono essere utilizzate per generare dinamicamente il contenuto per il MOTD, vedere ["riferimento al comando"](#).

**Scelte**

- Gestire il MOTD a livello di cluster:

Se si desidera...	Quindi...
Creare un MOTD per tutti gli accessi quando non esiste un MOTD	Impostare un MOTD a livello di cluster:  `*security login motd modify -vserver <i>cluster_name</i> { [-message " <i>text</i> "]
[-uri <i>ftp_or_http_addr</i> ] }*	Modificare il MOTD per tutti gli accessi quando non sono configurati MOTD a livello di SVM

Se si desidera...	Quindi...
<p>Modificare il MOTD a livello di cluster:</p> <pre>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"] }</pre>	<pre>[-uri ftp_or_http_addr] }*</pre>
<p>Rimuovere il MOTD per tutti gli accessi quando non sono configurati MOTD a livello di SVM</p>	<p>Impostare MOTD a livello di cluster su una stringa vuota (""):</p> <pre><b>security login motd modify -vserver <i>cluster_name</i> -message ""</b></pre>
<p>Ogni SVM deve visualizzare il MOTD a livello di cluster invece di utilizzare il MOTD a livello di SVM</p>	<p>Impostare un MOTD a livello di cluster, quindi impostare tutti i MOTD a livello di SVM su una stringa vuota con il MOTD a livello di cluster abilitato:</p> <p>a. <pre>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</pre></p>
<pre>[-uri <i>ftp_or_http_addr</i>] }* .. <b>security login motd modify { -vserver !"<i>cluster_name</i>" } -message "" -is -cluster-message-enabled true</b></pre>	<p>Visualizzare un MOTD solo per le SVM selezionate e non utilizzare alcun MOTD a livello di cluster</p>
<p>Impostare MOTD a livello di cluster su una stringa vuota, quindi impostare MOTD a livello di SVM per le SVM selezionate:</p> <p>a. <pre><b>security login motd modify -vserver <i>cluster_name</i> -message ""</b></pre></p> <p>b. <pre>`*security login motd modify -vserver <i>svm_name</i> { [-message "<i>text</i>"]</pre></p>	<pre>[-uri ftp_or_http_addr] }* + È possibile ripetere questo passaggio per ogni SVM in base alle necessità.</pre>
<p>Utilizzare lo stesso MOTD a livello di SVM per tutte le SVM (dati e amministratore)</p>	<p>Impostare il cluster e tutte le SVM in modo che utilizzino lo stesso MOTD:</p> <pre>`*security login motd modify -vserver * { [-message "<i>text</i>"]</pre>
<pre>[-uri ftp_or_http_addr] }*  [NOTE] ==== Se si utilizza la modalità interattiva, l'interfaccia CLI richiede di immettere il MOTD singolarmente per il cluster e per ciascuna SVM. È possibile incollare lo stesso MOTD in ogni istanza quando richiesto.  ====</pre>	<p>Disporre di un MOTD a livello di cluster disponibile come opzione per tutte le SVM, ma non si desidera che il MOTD venga visualizzato per gli accessi al cluster</p>

Se si desidera...	Quindi...
<p>Impostare un MOTD a livello di cluster, ma disattivarne la visualizzazione per il cluster:</p> <pre>`*security login motd modify -vserver <i>cluster_name</i> { [-message "<i>text</i>"]</pre>	<pre>[-uri <i>ftp_or_http_addr</i>] } -is-cluster-message-enabled false*</pre>
<p>Rimuovere tutti i MOTD a livello di cluster e SVM quando solo alcune SVM dispongono di MOTD a livello di cluster e SVM</p>	<p>Impostare il cluster e tutte le SVM in modo che utilizzino una stringa vuota per il MOTD:</p> <pre><b>security login motd modify -vserver * -message ""</b></pre>
<p>Modificare il MOTD solo per le SVM che hanno una stringa non vuota, quando altre SVM utilizzano una stringa vuota e quando viene utilizzato un MOTD diverso a livello di cluster</p>	<p>Utilizzare le query estese per modificare il MOTD in modo selettivo:</p> <pre>`*security login motd modify { -vserver !"<i>cluster_name</i>" -message !"" } { [-message "<i>text</i>"]</pre>
<pre>[-uri <i>ftp_or_http_addr</i>] }*</pre>	<p>Visualizza tutti i MOTD che contengono testo specifico (ad esempio “gennaio” seguito da “2015”) in qualsiasi punto di un messaggio singolo o multilinea, anche se il testo è diviso su righe diverse</p>
<p>Utilizzare una query per visualizzare i MOTD:</p> <pre><b>security login motd show -message *"January"*"2015"*</b></pre>	<p>Creare in modo interattivo un MOTD che includa più newline consecutive (noto anche come fine delle righe, o EOLS)</p>

- Gestire il MOTD a livello di SVM:

Specificare `-vserver svm_name` Non è richiesto nel contesto SVM.

Se si desidera...	Quindi...
<p>Utilizzare un MOTD a livello di SVM diverso, quando SVM dispone già di un MOTD a livello di SVM</p>	<p>Modificare il MOTD a livello di SVM:</p> <pre>`*security login motd modify -vserver <i>svm_name</i> { [- message "<i>text</i>"]</pre>
<pre>[-uri <i>ftp_or_http_addr</i>] }*</pre>	<p>Utilizzare solo il MOTD a livello di cluster per SVM, quando SVM dispone già di un MOTD a livello di SVM</p>



Se si desidera...	Quindi...
<p>Impostare MOTD a livello di SVM su una stringa vuota, quindi chiedere all'amministratore del cluster di attivare MOTD a livello di cluster per SVM:</p> <p>a. <b><code>security login motd modify -vserver svm_name -message ""</code></b></p> <p>b. (Per l'amministratore del cluster) <b><code>security login motd modify -vserver svm_name -is-cluster-message-enabled true</code></b></p>	<p>Non visualizzare alcun MOTD sul display SVM, quando per SVM sono attualmente visualizzati sia i MOTD a livello di cluster che quelli a livello di SVM</p>

## Gestire i lavori e pianificare

I lavori vengono inseriti in una coda di lavoro ed eseguiti in background quando le risorse sono disponibili. Se un lavoro consuma troppe risorse del cluster, è possibile interromperlo o metterlo in pausa fino a quando non si verifica una minore domanda sul cluster. È inoltre possibile monitorare e riavviare i lavori.

### Categorie di lavoro

È possibile gestire tre categorie di lavori: Affiliati a server, affiliati a cluster e privati.

Un lavoro può essere in una delle seguenti categorie:

- **Lavori affiliati al server**

Questi job vengono messi in coda dal framework di gestione a un nodo specifico da eseguire.

- **Lavori affiliati a cluster**

Questi processi vengono messi in coda dal framework di gestione a qualsiasi nodo del cluster da eseguire.

- **Lavori privati**

Questi lavori sono specifici di un nodo e non utilizzano il database replicato (RDB) o altri meccanismi del cluster. I comandi che gestiscono i processi privati richiedono un livello di privilegio avanzato o superiore.

### Comandi per la gestione dei lavori

Quando si immette un comando che richiama un processo, in genere, il comando informa che il processo è stato messo in coda e ritorna al prompt dei comandi CLI. Tuttavia, alcuni comandi riportano invece l'avanzamento del processo e non ritornano al prompt dei comandi CLI fino al completamento del processo. In questi casi, è possibile premere Ctrl-C per spostare il job in background.

Se si desidera...	Utilizzare questo comando...
Visualizza informazioni su tutti i lavori	<code>job show</code>
Visualizza le informazioni sui job in base al nodo	<code>job show bynode</code>

Se si desidera...	Utilizzare questo comando...
Visualizzare le informazioni sui job affiliati al cluster	<code>job show-cluster</code>
Visualizza le informazioni sui lavori completati	<code>job show-completed</code>
Visualizza le informazioni sulla cronologia dei lavori	<code>job history show</code>  Per ciascun nodo del cluster vengono memorizzati fino a 25,000 record di processi. Di conseguenza, il tentativo di visualizzare l'intera cronologia dei lavori potrebbe richiedere molto tempo. Per evitare tempi di attesa potenzialmente lunghi, è necessario visualizzare i lavori per nodo, SVM (Storage Virtual Machine) o ID record.
Visualizzare l'elenco dei processi privati	<code>job private show</code> (livello di privilegio avanzato)
Visualizza le informazioni sui processi privati completati	<code>job private show-completed</code> (livello di privilegio avanzato)
Visualizza le informazioni sullo stato di inizializzazione per i job manager	<code>job initstate show</code> (livello di privilegio avanzato)
Monitorare l'avanzamento di un lavoro	<code>job watch-progress</code>
Monitorare l'avanzamento di un processo privato	<code>job private watch-progress</code> (livello di privilegio avanzato)
Mettere in pausa un lavoro	<code>job pause</code>
Mettere in pausa un processo privato	<code>job private pause</code> (livello di privilegio avanzato)
Riprendere un processo in pausa	<code>job resume</code>
Riprendere un processo privato in pausa	<code>job private resume</code> (livello di privilegio avanzato)
Interrompere un lavoro	<code>job stop</code>
Interruzione di un processo privato	<code>job private stop</code> (livello di privilegio avanzato)
Eliminare un lavoro	<code>job delete</code>
Eliminare un processo privato	<code>job private delete</code> (livello di privilegio avanzato)

Se si desidera...	Utilizzare questo comando...
Disassociare un lavoro affiliato al cluster a un nodo non disponibile che lo possiede, in modo che un altro nodo possa assumere la proprietà di tale lavoro	<code>job unclaim</code> (livello di privilegio avanzato)



È possibile utilizzare `event log show` per determinare il risultato di un lavoro completato.

## Informazioni correlate

["Comandi di ONTAP 9"](#)

## Comandi per la gestione delle pianificazioni dei processi

Molte attività, ad esempio le copie Snapshot dei volumi, possono essere configurate per l'esecuzione su pianificazioni specificate. Le pianificazioni eseguite in orari specifici sono denominate *cron* schedules (simili a UNIX *cron* pianificazioni). Le pianificazioni eseguite a intervalli sono denominate *interval* schedules. Si utilizza `job schedule` comandi per gestire le pianificazioni dei processi.

Le pianificazioni dei processi non vengono regolate in base alle modifiche manuali della data e dell'ora del cluster. Questi processi vengono pianificati per essere eseguiti in base all'ora corrente del cluster in cui è stato creato il processo o quando è stato eseguito più di recente. Pertanto, se si modifica manualmente la data o l'ora del cluster, utilizzare `job show` e `job history show` comandi per verificare che tutti i processi pianificati siano messi in coda e completati in base alle proprie esigenze.

Se il cluster fa parte di una configurazione MetroCluster, le pianificazioni dei processi su entrambi i cluster devono essere identiche. Pertanto, se si crea, modifica o elimina una pianificazione del processo, è necessario eseguire la stessa operazione sul cluster remoto.

Se si desidera...	Utilizzare questo comando...
Visualizza le informazioni su tutti i programmi	<code>job schedule show</code>
Visualizza l'elenco dei lavori in base alla pianificazione	<code>job schedule show-jobs</code>
Visualizza le informazioni sulle pianificazioni cron	<code>job schedule cron show</code>
Visualizza le informazioni sulle pianificazioni degli intervalli	<code>job schedule interval show</code>
Creare un calendario di cron	<code>job schedule cron create</code>  A partire da ONTAP 9.10.1, puoi includere la SVM per la pianificazione del lavoro.
Creare una pianificazione a intervalli	<code>job schedule interval create</code>  Specificare almeno uno dei seguenti parametri: -days, -hours, -minutes, 0. -seconds.

Se si desidera...	Utilizzare questo comando...
Modificare una pianificazione cron	<code>job schedule cron modify</code>
Modificare una pianificazione di intervalli	<code>job schedule interval modify</code>
Eliminare un programma	<code>job schedule delete</code>
Eliminare una pianificazione cron	<code>job schedule cron delete</code>
Eliminare una pianificazione di intervalli	<code>job schedule interval delete</code>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

## Backup e ripristino delle configurazioni del cluster (solo amministratori del cluster)

### Quali sono i file di backup della configurazione

I file di backup della configurazione sono file di archivio (.7z) che contengono informazioni per tutte le opzioni configurabili necessarie per il corretto funzionamento del cluster e dei nodi al suo interno.

Questi file memorizzano la configurazione locale di ciascun nodo, oltre alla configurazione replicata a livello di cluster. I file di backup della configurazione vengono utilizzati per eseguire il backup e il ripristino della configurazione del cluster.

Esistono due tipi di file di backup della configurazione:

- **File di backup della configurazione del nodo**

Ogni nodo integro nel cluster include un file di backup della configurazione del nodo, che contiene tutte le informazioni di configurazione e i metadati necessari per il funzionamento corretto del nodo nel cluster.

- **File di backup della configurazione del cluster**

Questi file includono un archivio di tutti i file di backup della configurazione del nodo nel cluster, oltre alle informazioni di configurazione del cluster replicate (il database replicato o il file RDB). I file di backup della configurazione del cluster consentono di ripristinare la configurazione dell'intero cluster o di qualsiasi nodo del cluster. I programmi di backup della configurazione del cluster creano automaticamente questi file e li memorizzano su diversi nodi del cluster.



I file di backup della configurazione contengono solo informazioni di configurazione. Non includono dati dell'utente. Per informazioni sul ripristino dei dati utente, vedere ["Protezione dei dati"](#).

### Modalità di backup automatico delle configurazioni del nodo e del cluster

Tre pianificazioni separate creano automaticamente i file di backup della configurazione

del cluster e del nodo e li replicano tra i nodi del cluster.

I file di backup della configurazione vengono creati automaticamente in base alle seguenti pianificazioni:



- Ogni 8 ore
- Ogni giorno
- Settimanale

In ciascuna di queste situazioni, viene creato un file di backup della configurazione del nodo su ciascun nodo integro del cluster. Tutti questi file di backup della configurazione del nodo vengono quindi raccolti in un singolo file di backup della configurazione del cluster insieme alla configurazione del cluster replicata e salvati su uno o più nodi del cluster.

### Comandi per la gestione delle pianificazioni di backup della configurazione

È possibile utilizzare `system configuration backup settings` comandi per gestire le pianificazioni di backup della configurazione.


Questi comandi sono disponibili a livello di privilegio avanzato.


Se si desidera...	Utilizzare questo comando...
<p>Modificare le impostazioni per una pianificazione di backup della configurazione:</p> <ul style="list-style-type: none"><li>• Specificare un URL remoto (HTTP, HTTPS, FTP, FTPS o TFTP ) in cui verranno caricati i file di backup della configurazione oltre alle posizioni predefinite nel cluster</li><li>• Specificare un nome utente da utilizzare per accedere all'URL remoto</li><li>• Impostare il numero di backup da conservare per ogni pianificazione di backup della configurazione</li></ul>	<p><code>system configuration backup settings modify</code></p> <p>Quando si utilizza HTTPS nell'URL remoto, utilizzare <code>-validate-certification</code> opzione per attivare o disattivare la convalida digitale del certificato. La convalida del certificato è disattivata per impostazione predefinita.</p> <div><p>Il server Web su cui si sta caricando il file di backup della configurazione deve avere ATTIVATO le operazioni HTTP e POST per HTTPS. Per ulteriori informazioni, consultare la documentazione del server Web.</p></div>
<p>Impostare la password da utilizzare per accedere all'URL remoto</p>	<p><code>system configuration backup settings set-password</code></p>
<p>Visualizzare le impostazioni per la pianificazione del backup della configurazione</p>	<p><code>system configuration backup settings show</code></p> <div><p>Impostare <code>-instance</code> parametro per visualizzare il nome utente e il numero di backup da conservare per ciascuna pianificazione.</p></div>

## Comandi per la gestione dei file di backup della configurazione

Si utilizza `system configuration backup` comandi per gestire i file di backup della configurazione del cluster e del nodo.

Questi comandi sono disponibili a livello di privilegio avanzato.

Se si desidera...	Utilizzare questo comando...
Creare un nuovo file di backup della configurazione del nodo o del cluster	<code>system configuration backup create</code>
Copiare un file di backup della configurazione da un nodo a un altro nel cluster	<code>system configuration backup copy</code>
Caricare un file di backup della configurazione da un nodo del cluster a un URL remoto (FTP, HTTP, HTTPS, TFTP o FTPS)	<div><code>system configuration backup upload</code>  Quando si utilizza HTTPS nell'URL remoto, utilizzare <code>-validate-certification</code> opzione per attivare o disattivare la convalida digitale del certificato. La convalida del certificato è disattivata per impostazione predefinita.  <div> Il server Web su cui si sta caricando il file di backup della configurazione deve avere ATTIVATO le operazioni HTTP e POST per HTTPS. Alcuni server Web potrebbero richiedere l'installazione di un modulo aggiuntivo. Per ulteriori informazioni, consultare la documentazione del server Web. I formati URL supportati variano in base alla versione di ONTAP. Consultare la guida della riga di comando per la versione di ONTAP in uso.</div></div>
Scaricare un file di backup della configurazione da un URL remoto a un nodo del cluster e, se specificato, validare il certificato digitale	<div><code>system configuration backup download</code>  Quando si utilizza HTTPS nell'URL remoto, utilizzare <code>-validate-certification</code> opzione per attivare o disattivare la convalida digitale del certificato. La convalida del certificato è disattivata per impostazione predefinita.</div>
Rinominare un file di backup della configurazione su un nodo del cluster	<code>system configuration backup rename</code>
Visualizzare i file di backup della configurazione del nodo e del cluster per uno o più nodi nel cluster	<code>system configuration backup show</code>

Se si desidera...	Utilizzare questo comando...
Eliminare un file di backup della configurazione su un nodo	<pre>system configuration backup delete</pre> <div>  <p>Questo comando elimina il file di backup della configurazione solo sul nodo specificato. Se il file di backup della configurazione esiste anche su altri nodi del cluster, rimane su questi nodi.</p> </div>

### Trovare un file di backup della configurazione da utilizzare per il ripristino di un nodo

Per ripristinare la configurazione di un nodo, si utilizza un file di backup della configurazione situato in un URL remoto o su un nodo del cluster.

#### A proposito di questa attività

È possibile utilizzare un file di backup della configurazione del cluster o del nodo per ripristinare la configurazione di un nodo.

#### Fase

1. Rendere disponibile il file di backup della configurazione nel nodo per il quale si desidera ripristinare la configurazione.

Se si trova il file di backup della configurazione...	Quindi...
A un URL remoto	Utilizzare <code>system configuration backup download</code> al livello di privilegio avanzato per scaricarlo nel nodo di ripristino.
Su un nodo del cluster	<ol style="list-style-type: none"> <li>a. Utilizzare <code>system configuration backup show</code> al livello di privilegio avanzato per visualizzare l'elenco dei file di backup della configurazione disponibili nel cluster che contiene la configurazione del nodo di ripristino.</li> <li>b. Se il file di backup della configurazione identificato non esiste nel nodo di ripristino, utilizzare <code>system configuration backup copy</code> comando per copiarlo nel nodo di ripristino.</li> </ol>

Se in precedenza è stato ricreato il cluster, è necessario scegliere un file di backup della configurazione creato dopo la ricreazione del cluster. Se è necessario utilizzare un file di backup della configurazione creato prima della ricostruzione del cluster, dopo il ripristino del nodo, è necessario ricreare il cluster.

### Ripristinare la configurazione del nodo utilizzando un file di backup della configurazione

La configurazione del nodo viene ripristinata utilizzando il file di backup della

configurazione identificato e reso disponibile al nodo di ripristino.

### A proposito di questa attività

Eseguire questa attività solo per eseguire il ripristino da un disastro che ha causato la perdita dei file di configurazione locale del nodo.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Se il nodo è integro, utilizzare il livello di privilegio avanzato di un nodo diverso `cluster modify` con il `-node` e `-eligibility` parametri per contrassegnarlo come non idoneo e isolarlo dal cluster.

Se il nodo non è integro, saltare questo passaggio.

Questo esempio modifica il `node2` in modo che non sia idoneo a partecipare al cluster in modo che la sua configurazione possa essere ripristinata:

```
cluster1::*> cluster modify -node node2 -eligibility false
```

3. Utilizzare `system configuration recovery node restore` al livello di privilegio avanzato per ripristinare la configurazione del nodo da un file di backup della configurazione.

Se il nodo perde la propria identità, compreso il nome, utilizzare il `-nodename-in-backup` parametro per specificare il nome del nodo nel file di backup della configurazione.

Questo esempio ripristina la configurazione del nodo utilizzando uno dei file di backup della configurazione memorizzati nel nodo:

```
cluster1::*> system configuration recovery node restore -backup  
cluster1.8hour.2011-02-22.18_15_00.7z
```

```
Warning: This command overwrites local configuration files with  
files contained in the specified backup file. Use this  
command only to recover from a disaster that resulted  
in the loss of the local configuration files.  
The node will reboot after restoring the local configuration.  
Do you want to continue? {y|n}: y
```

La configurazione viene ripristinata e il nodo viene riavviato.

4. Se il nodo è stato contrassegnato come non idoneo, utilizzare `system configuration recovery cluster sync` per contrassegnare il nodo come idoneo e sincronizzarlo con il cluster.
5. Se si utilizza un ambiente SAN, utilizzare `system node reboot` Comando per riavviare il nodo e ristabilire il quorum SAN.

### Al termine



Se in precedenza è stato ricreato il cluster e si sta ripristinando la configurazione del nodo utilizzando un file di backup della configurazione creato prima della creazione del cluster, è necessario ricrearlo di nuovo.

## Trovare una configurazione da utilizzare per il ripristino di un cluster

La configurazione viene utilizzata da un nodo del cluster o da un file di backup della configurazione del cluster per ripristinare un cluster.

### Fasi

#### 1. Scegliere un tipo di configurazione per ripristinare il cluster.

- Un nodo nel cluster

Se il cluster è costituito da più di un nodo e uno di essi ha una configurazione del cluster da quando il cluster si trovava nella configurazione desiderata, è possibile ripristinare il cluster utilizzando la configurazione memorizzata su tale nodo.

Nella maggior parte dei casi, il nodo contenente l'anello di replica con l'ID transazione più recente è il nodo migliore da utilizzare per ripristinare la configurazione del cluster. Il `cluster ring show` il comando a livello di privilegio avanzato consente di visualizzare un elenco degli anelli replicati disponibili su ciascun nodo del cluster.

- Un file di backup della configurazione del cluster

Se non si riesce a identificare un nodo con la corretta configurazione del cluster o se il cluster è costituito da un singolo nodo, è possibile utilizzare un file di backup della configurazione del cluster per ripristinare il cluster.

Se si sta ripristinando il cluster da un file di backup della configurazione, le modifiche apportate alla configurazione dopo l'esecuzione del backup andranno perse. Dopo il ripristino, è necessario risolvere eventuali discrepanze tra il file di backup della configurazione e la configurazione attuale. Consultare l'articolo della Knowledge base ["Guida alla risoluzione dei problemi di backup per la configurazione di ONTAP"](#) per indicazioni sulla risoluzione dei problemi.

#### 2. Se si sceglie di utilizzare un file di backup della configurazione del cluster, rendere il file disponibile per il nodo che si intende utilizzare per ripristinare il cluster.

Se si trova il file di backup della configurazione...	Quindi...
A un URL remoto	Utilizzare <code>system configuration backup download</code> al livello di privilegio avanzato per scaricarlo nel nodo di ripristino.

Se si trova il file di backup della configurazione...	Quindi...
Su un nodo del cluster	<p>a. Utilizzare <code>system configuration backup show</code> al livello di privilegio avanzato per trovare un file di backup della configurazione del cluster creato quando il cluster si trovava nella configurazione desiderata.</p> <p>b. Se il file di backup della configurazione del cluster non si trova nel nodo che si intende utilizzare per ripristinare il cluster, utilizzare <code>system configuration backup copy</code> comando per copiarlo nel nodo di ripristino.</p>

## Ripristinare una configurazione del cluster da una configurazione esistente

Per ripristinare una configurazione del cluster da una configurazione esistente in seguito a un errore del cluster, ricrearlo utilizzando la configurazione del cluster scelta e resa disponibile al nodo di ripristino, quindi riconnettersi ciascun nodo aggiuntivo al nuovo cluster.

### A proposito di questa attività

Questa attività deve essere eseguita solo per il ripristino da un disastro che ha causato la perdita della configurazione del cluster.



Se si sta ricreando il cluster da un file di backup della configurazione, contattare il supporto tecnico per risolvere eventuali discrepanze tra il file di backup della configurazione e la configurazione presente nel cluster.

Se si sta ripristinando il cluster da un file di backup della configurazione, le modifiche apportate alla configurazione dopo l'esecuzione del backup andranno perse. Dopo il ripristino, è necessario risolvere eventuali discrepanze tra il file di backup della configurazione e la configurazione attuale. Consultare l'articolo della Knowledge base ["Guida alla risoluzione dei problemi per il backup della configurazione di ONTAP"](#).

### Fasi

1. Disattivare il failover dello storage per ciascuna coppia ha:

```
storage failover modify -node node_name -enabled false
```

È necessario disattivare il failover dello storage una sola volta per ogni coppia ha. Quando si disattiva il failover dello storage per un nodo, anche il failover dello storage viene disattivato sul partner del nodo.

2. Arrestare ciascun nodo ad eccezione del nodo di ripristino:

```
system node halt -node node_name -reason "text"
```

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

4. Nel nodo di ripristino, utilizzare **system configuration recovery cluster recreate** per ricreare il cluster.

In questo esempio viene ricreato il cluster utilizzando le informazioni di configurazione memorizzate nel nodo di ripristino:

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
        rebuild a new single-node cluster consisting of this node
        and its current configuration. This feature should only be
        used to recover from a disaster. Do not perform any other
        recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

Viene creato un nuovo cluster sul nodo di ripristino.

5. Se si sta ricreando il cluster da un file di backup della configurazione, verificare che il ripristino del cluster sia ancora in corso:

```
system configuration recovery cluster show
```

Non è necessario verificare lo stato di ripristino del cluster se si sta ricreando il cluster da un nodo integro.

```
cluster1::*> system configuration recovery cluster show
Recovery Status: in-progress
Is Recovery Status Persisted: false
```

6. Avviare ogni nodo che deve essere ricongiungersi al cluster ricreato.

È necessario riavviare i nodi uno alla volta.

7. Per ogni nodo che deve essere Unito al cluster ricreato, procedere come segue:

a. Da un nodo integro nel cluster ricreato, ricongiungersi al nodo di destinazione:

```
system configuration recovery cluster rejoin -node node_name
```

Questo esempio ricongiunge il nodo di destinazione "node2" al cluster ricreato:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
cluster, potentially overwriting critical cluster
configuration files. This command should only be used
to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress.
This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

Il nodo di destinazione viene riavviato e quindi Unito al cluster.

- b. Verificare che il nodo di destinazione sia integro e che abbia formato il quorum con gli altri nodi del cluster:

```
cluster show -eligibility true
```

Il nodo di destinazione deve riconnettersi al cluster ricreato prima di poter riconnettersi a un altro nodo.

```
cluster1::*> cluster show -eligibility true
Node           Health Eligibility  Epsilon
-----
node0           true   true        false
node1           true   true        false
2 entries were displayed.
```

8. Se il cluster è stato ricreato da un file di backup della configurazione, impostare lo stato di ripristino su complete (completo):

```
system configuration recovery cluster modify -recovery-status complete
```

9. Tornare al livello di privilegio admin:

```
set -privilege admin
```

10. Se il cluster è costituito da due soli nodi, utilizzare **cluster ha modify** Comando per riabilitare il cluster ha.
11. Utilizzare **storage failover modify** Comando per riabilitare il failover dello storage per ogni coppia ha.

#### Al termine

Se il cluster dispone di relazioni peer SnapMirror, è necessario ricrearle. Per ulteriori informazioni, vedere ["Protezione dei dati"](#).

#### Sincronizzare un nodo con il cluster

Se esiste un quorum a livello di cluster, ma uno o più nodi non sono sincronizzati con il

cluster, è necessario sincronizzare il nodo per ripristinare il database replicato (RDB) sul nodo e portarlo in quorum.

### Fase

1. Da un nodo integro, utilizzare `system configuration recovery cluster sync` al livello di privilegio avanzato per sincronizzare il nodo non sincronizzato con la configurazione del cluster.

Questo esempio sincronizza un nodo (*node2*) con il resto del cluster:

```
cluster1::*> system configuration recovery cluster sync -node node2
```

```
Warning: This command will synchronize node "node2" with the cluster
configuration, potentially overwriting critical cluster
configuration files on the node. This feature should only be
used to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress. This
command will cause all the cluster applications on node
"node2" to restart, interrupting administrative CLI and Web
interface on that node.
```

```
Do you want to continue? {y|n}: y
```

```
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

### Risultato

L'RDB viene replicato nel nodo e il nodo diventa idoneo a partecipare al cluster.

## Gestire i core dump (solo amministratori del cluster)

Quando un nodo esegue il panic, si verifica un core dump e il sistema crea un core dump file che il supporto tecnico può utilizzare per risolvere il problema. È possibile configurare o visualizzare gli attributi di core dump. È inoltre possibile salvare, visualizzare, segmentare, caricare o eliminare un file core dump.

Puoi gestire i core dump nei seguenti modi:

- Configurazione dei core dump e visualizzazione delle impostazioni di configurazione
- Visualizzazione delle informazioni di base, dello stato e degli attributi dei core dump

I file di dump e i report principali vengono memorizzati in `/mroot/etc/crash/` directory di un nodo. È possibile visualizzare il contenuto della directory utilizzando `system node coredump` o un browser web.




- Salvare il contenuto del core dump e caricare il file salvato in una posizione specifica o nel supporto tecnico

ONTAP impedisce di avviare il salvataggio di un file di dump core durante un takeover, un trasferimento aggregato o un giveback.

- Eliminazione dei file core dump non più necessari

## Comandi per la gestione dei core dump

Si utilizza `system node coredump config` comandi per gestire la configurazione dei core dump, il `system node coredump` comandi per gestire i file core dump e il `system node coredump reports` comandi per gestire i report principali dell'applicazione.

Se si desidera...	Utilizzare questo comando...
Configurare i core dump	<code>system node coredump config modify</code>
Visualizzare le impostazioni di configurazione per i core dump	<code>system node coredump config show</code>
Visualizza informazioni di base sui core dump	<code>system node coredump show</code>
Attivare manualmente un core dump quando si riavvia un nodo	<code>system node reboot</code> con entrambi <code>-dump</code> e <code>-skip-lif-migration-before-reboot</code> parametri   Il <code>skip-lif-migration-before-reboot</code> Parametro specifica che la migrazione LIF prima di un riavvio verrà ignorata.
Attivare manualmente un core dump quando si chiude un nodo	<code>system node halt</code> con entrambi <code>-dump</code> e <code>-skip-lif-migration-before-shutdown</code> parametri   Il <code>skip-lif-migration-before-shutdown</code> Parametro specifica che la migrazione LIF prima di un arresto verrà ignorata.
Salvare un core dump specificato	<code>system node coredump save</code>
Salva tutti i core dump non salvati che si trovano su un nodo specificato	<code>system node coredump save-all</code>
Generare e inviare un messaggio AutoSupport con un file core dump specificato	<code>system node autosupport invoke-core-upload</code>   Il <code>-uri</code> Il parametro opzionale specifica una destinazione alternativa per il messaggio AutoSupport.
Visualizza informazioni sullo stato dei core dump	<code>system node coredump status</code>
Eliminare un core dump specificato	<code>system node coredump delete</code>

Se si desidera...	Utilizzare questo comando...
Eliminare tutti i core dump non salvati o tutti i file core salvati su un nodo	<code>system node coredump delete-all</code>
Visualizza i report di dump del core dell'applicazione	<code>system node coredump reports show</code>
Eliminare un report di dump del core dell'applicazione	<code>system node coredump reports delete</code>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

## Gestione di dischi e Tier (aggregato)

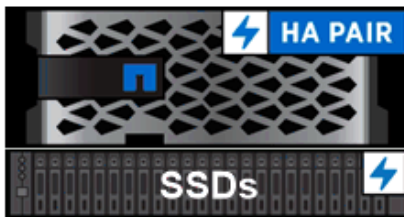
### Panoramica su dischi e Tier locali (aggregati)

È possibile gestire lo storage fisico di ONTAP utilizzando Gestione di sistema e l'interfaccia CLI. È possibile creare, espandere e gestire i Tier locali (aggregati), lavorare con i Tier locali di Flash Pool (aggregati), gestire i dischi e gestire le policy RAID.

#### Quali sono i Tier locali (aggregati)

*Tier locali* (denominati anche *aggregati*) sono contenitori per i dischi gestiti da un nodo. È possibile utilizzare i Tier locali per isolare i carichi di lavoro con esigenze di performance diverse, per tierare i dati con diversi modelli di accesso o per separare i dati per scopi normativi.

- Per le applicazioni business-critical che richiedono la latenza più bassa possibile e le performance più elevate, è possibile creare un Tier locale composto interamente da SSD.
- Per tierare i dati con diversi modelli di accesso, è possibile creare un *Tier locale ibrido*, implementando la flash come cache dalle performance elevate per un set di dati funzionante, utilizzando al contempo HDD a basso costo o storage a oggetti per i dati ad accesso meno frequente.
  - Un *Flash Pool* è costituito da SSD e HDD.
  - Un *FabricPool* è costituito da un Tier locale all-SSD con un archivio di oggetti collegato.
- Se è necessario separare i dati archiviati dai dati attivi per scopi normativi, è possibile utilizzare un Tier locale costituito da HDD con capacità o una combinazione di HDD con capacità e performance.



Datacenter



Cloud

*You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.*

### Lavorare con i Tier locali (aggregati)

È possibile eseguire le seguenti operazioni:

- ["Gestire i Tier locali \(aggregati\)"](#)
- ["Gestire i dischi"](#)
- ["Gestire le configurazioni RAID"](#)
- ["Gestire i Tier di Flash Pool"](#)

Eseguire queste attività se si verificano le seguenti condizioni:

- Non si desidera utilizzare uno strumento di scripting automatico.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Si dispone di una configurazione MetroCluster e si stanno seguendo le procedure descritte in ["MetroCluster"](#) documentazione per la configurazione iniziale e linee guida per tier locali (aggregati) e gestione dei dischi.

### Informazioni correlate

- ["Gestire i Tier cloud FabricPool"](#)

## Gestire i Tier locali (aggregati)

### Gestire i Tier locali (aggregati)

Puoi utilizzare System Manager o la CLI di ONTAP per aggiungere Tier locali (aggregati), gestirne l'utilizzo e aggiungere capacità (dischi) agli stessi.

È possibile eseguire le seguenti operazioni:



- ["Aggiungere \(creare\) un Tier locale \(aggregato\)"](#)

Per aggiungere un Tier locale, si segue un workflow specifico. Si determina il numero di dischi o partizioni di dischi necessari per il Tier locale e si decide quale metodo utilizzare per creare il Tier locale. È possibile aggiungere automaticamente i Tier locali consentendo a ONTAP di assegnare la configurazione oppure specificarla manualmente.

- ["Gestire l'utilizzo di Tier locali \(aggregati\)"](#)

Per i Tier locali esistenti, è possibile rinominarli, impostarne i costi dei supporti o determinare le informazioni sul disco e sul gruppo RAID. È possibile modificare la configurazione RAID di un Tier locale e assegnare Tier locali alle VM di storage (SVM). È possibile modificare la configurazione RAID di un Tier locale e assegnare Tier locali alle VM di storage (SVM). È possibile determinare quali volumi risiedono su un Tier locale e la quantità di spazio utilizzata su un Tier locale. È possibile controllare lo spazio che i volumi possono utilizzare. È possibile trasferire la proprietà del Tier locale con una coppia ha. È anche possibile eliminare un Tier locale.

- ["Aggiunta di capacità \(dischi\) a un Tier locale \(aggregato\)"](#)

Utilizzando metodi diversi, si segue un workflow specifico per aggiungere capacità. È possibile aggiungere dischi a un Tier locale e dischi a un nodo o a uno shelf. Se necessario, è possibile correggere le partizioni sparse disallineate.

## **Aggiungere (creare) un Tier locale (aggregato)**

### **Aggiunta di un Tier locale (creazione di un aggregato)**

Per aggiungere un Tier locale (creare un aggregato), si segue un workflow specifico.

Si determina il numero di dischi o partizioni di dischi necessari per il Tier locale e si decide quale metodo utilizzare per creare il Tier locale. È possibile aggiungere automaticamente i Tier locali consentendo a ONTAP di assegnare la configurazione oppure specificarla manualmente.

- ["Workflow per aggiungere un Tier locale \(aggregato\)"](#)
- ["Determinare il numero di dischi o partizioni richiesto per un Tier locale \(aggregato\)"](#)
- ["Decidere quale metodo di creazione del Tier locale \(aggregato\) utilizzare"](#)
- ["Aggiungere automaticamente i Tier locali \(aggregati\)"](#)
- ["Aggiungere manualmente i Tier locali \(aggregati\)"](#)

### **Workflow per aggiungere un Tier locale (aggregato)**

La creazione di Tier locali (aggregati) fornisce storage ai volumi del sistema.

Il flusso di lavoro per la creazione di Tier locali (aggregati) è specifico dell'interfaccia utilizzata: System Manager o CLI:

## **Workflow di System Manager**

### **Utilizzare System Manager per aggiungere (creare) un Tier locale**

System Manager crea Tier locali in base alle Best practice consigliate per la configurazione dei Tier locali.

A partire da ONTAP 9.11.1, è possibile configurare manualmente i Tier locali se si desidera una configurazione diversa da quella consigliata durante il processo automatico per aggiungere un Tier locale.



## Workflow CLI

### Utilizzare la CLI per aggiungere (creare) un aggregato

A partire da ONTAP 9.2, ONTAP è in grado di fornire le configurazioni consigliate per la creazione di aggregati (provisioning automatico). Se le configurazioni consigliate, basate sulle Best practice, sono appropriate nel proprio ambiente, è possibile accettarle per creare gli aggregati. In caso contrario, è possibile creare gli aggregati manualmente.



#### Determinare il numero di dischi o partizioni richiesto per un Tier locale (aggregato)

È necessario disporre di un numero di dischi o partizioni di dischi sufficiente nel Tier locale (aggregato) per soddisfare i requisiti di sistema e di business. Per ridurre al minimo il potenziale di perdita di dati, si consiglia di utilizzare il numero consigliato di dischi hot spare o partizioni hot spare.

La partizione dei dati root è attivata per impostazione predefinita in alcune configurazioni. I sistemi con partizione dei dati root abilitata utilizzano partizioni di dischi per creare Tier locali. I sistemi che non hanno la partizione dei dati root abilitata utilizzano dischi non partizionati.

È necessario disporre di dischi o partizioni sufficienti per soddisfare il numero minimo richiesto per la policy RAID e per soddisfare i requisiti minimi di capacità.



In ONTAP, lo spazio utilizzabile del disco è inferiore alla capacità fisica del disco. È possibile trovare lo spazio utilizzabile di un disco specifico e il numero minimo di dischi o partizioni richiesto per ogni criterio RAID in ["Hardware Universe"](#).

#### Determinare lo spazio utilizzabile di un disco specifico


La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

### Utilizzare System Manager per determinare lo spazio utilizzabile dei dischi

Per visualizzare le dimensioni utilizzabili di un disco, procedere come segue:

#### Fasi

1. Accedere a **Storage > Tier**
2. Fare clic su  accanto al nome del tier locale.
3. Selezionare la scheda **Disk Information** (informazioni disco).

#### CLI

### Utilizzare la CLI per determinare lo spazio utilizzabile dei dischi

Per visualizzare le dimensioni utilizzabili di un disco, procedere come segue:

#### Fase

1. Visualizzare le informazioni sul disco spare:

```
storage aggregate show-spare-disks
```

Oltre al numero di dischi o partizioni di dischi necessari per creare il gruppo RAID e soddisfare i requisiti di capacità, è necessario disporre del numero minimo di dischi hot spare o di partizioni di dischi hot spare consigliato per l'aggregato:

- Per tutti gli aggregati flash, è necessario disporre di almeno un disco hot spare o di una partizione del disco.



Per impostazione predefinita, AFF C190 non dispone di unità spare. Questa eccezione è completamente supportata.

- Per gli aggregati omogenei non flash, è necessario disporre di almeno due dischi hot spare o partizioni di dischi.
- Per i pool di storage SSD, è necessario disporre di almeno un disco hot spare per ogni coppia ha.
- Per gli aggregati Flash Pool, è necessario disporre di almeno due dischi di riserva per ogni coppia ha. Per ulteriori informazioni sui criteri RAID supportati per gli aggregati di Flash Pool, consultare la sezione ["Hardware Universe"](#).
- Per supportare l'utilizzo del Centro di manutenzione ed evitare problemi causati da guasti a più dischi simultanei, è necessario disporre di un minimo di quattro hot spare nei carrier multi-disco.

#### Informazioni correlate

["NetApp Hardware Universe"](#)

["Report tecnico di NetApp 3838: Guida alla configurazione del sottosistema di storage"](#)

#### Decidere quale metodo utilizzare per creare Tier locali (aggregati)

Sebbene ONTAP fornisca consigli sulle Best practice per l'aggiunta automatica di Tier locali (creazione di aggregati con provisioning automatico), è necessario determinare se

le configurazioni consigliate sono supportate nel proprio ambiente. In caso contrario, è necessario prendere decisioni in merito alla policy RAID e alla configurazione del disco, quindi creare manualmente i Tier locali.

Quando viene creato automaticamente un Tier locale, ONTAP analizza i dischi spare disponibili nel cluster e genera un consiglio su come utilizzare i dischi spare per aggiungere Tier locali in base alle Best practice. ONTAP visualizza le configurazioni consigliate. È possibile accettare i consigli o aggiungere manualmente i Tier locali.

### Prima di poter accettare le raccomandazioni ONTAP

In presenza di una delle seguenti condizioni di disco, è necessario affrontarle prima di accettare le raccomandazioni di ONTAP:

- Dischi mancanti
- Fluttuazione nei numeri dei dischi spare
- Dischi non assegnati
- Parti di ricambio non azzerate
- Dischi sottoposti a test di manutenzione

Il `storage aggregate auto-provision` la pagina man contiene ulteriori informazioni su questi requisiti.

### Quando è necessario utilizzare il metodo manuale

In molti casi, il layout consigliato del Tier locale sarà ottimale per il tuo ambiente. Tuttavia, se nel cluster è in esecuzione ONTAP 9.1 o versioni precedenti o se l'ambiente include le seguenti configurazioni, è necessario creare il Tier locale utilizzando il metodo manuale.



A partire da ONTAP 9.11.1, è possibile aggiungere manualmente i Tier locali con Gestore di sistema.

- Aggregati che utilizzano LUN di array di terze parti
- Dischi virtuali con Cloud Volumes ONTAP o ONTAP Select
- Sistema MetroCluster
- SyncMirror
- Dischi MSATA
- Tier FlashPool (aggregati)
- Al nodo sono collegati diversi tipi o dimensioni di dischi

### Selezionare il metodo per creare Tier locali (aggregati)

Scegliere il metodo da utilizzare:

- ["Aggiungere \(creare\) livelli locali \(aggregati\) automaticamente"](#)
- ["Aggiungere \(creare\) Tier locali \(aggregati\) manualmente"](#)

### Informazioni correlate

["Comandi di ONTAP 9"](#)

### **Aggiunta automatica di Tier locali (creazione di aggregati con provisioning automatico)**

Se il consiglio delle Best practice fornito da ONTAP per l'aggiunta automatica di un Tier locale (creazione di un aggregato con provisioning automatico) è appropriato nel tuo ambiente, puoi accettare il consiglio e lasciare che ONTAP aggiunga il Tier locale.

#### **Prima di iniziare**

I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato). Se il cluster non è configurato per l'utilizzo dell'assegnazione automatica della proprietà del disco, è necessario ["assegnare la proprietà manualmente"](#).

## System Manager

### Fasi

1. In System Manager, fare clic su **Storage > Tier**.
2. Nella pagina **Tier**, fare clic su [+ Add Local Tier](#) per creare un nuovo tier locale:

La pagina **Add Local Tier** mostra il numero consigliato di Tier locali che possono essere creati sui nodi e lo storage utilizzabile disponibile.

3. Fare clic su **Recommended details** (Dettagli consigliati) per visualizzare la configurazione consigliata da System Manager.

System Manager visualizza le seguenti informazioni a partire da ONTAP 9.8:

- **Nome livello locale** (è possibile modificare il nome del livello locale che inizia con ONTAP 9.10.1)
- **Nome nodo**
- **Dimensione utilizzabile**
- **Tipo di storage**

A partire da ONTAP 9.10.1, vengono visualizzate ulteriori informazioni:

- **Dischi**: Indica il numero, la dimensione e il tipo dei dischi
- **Layout**: Mostra il layout del gruppo RAID, inclusi i dischi di parità o dati e gli slot non utilizzati.
- **Dischi di riserva**: Indica il nome del nodo, il numero e la dimensione dei dischi di riserva e il tipo di storage.

4. Eseguire una delle seguenti operazioni:

Se si desidera...	Quindi eseguire questa operazione...
Accettare i consigli di System Manager.	Passare a. <a href="#">La procedura per la configurazione di Onboard Key Manager per la crittografia</a> .
Configurare manualmente i Tier locali e <b>NOT</b> utilizzare i consigli di System Manager.	Passare a. <a href="#">"Aggiungere manualmente un Tier locale (creare aggregato)"</a> : <ul style="list-style-type: none"><li>• Per ONTAP 9.10.1 e versioni precedenti, seguire la procedura per utilizzare la CLI.</li><li>• A partire da ONTAP 9.11.1, seguire la procedura per utilizzare Gestione sistema.</li></ul>

5. (opzionale): Se è stato installato Onboard Key Manager, è possibile configurarlo per la crittografia. Selezionare la casella di controllo **Configura Onboard Key Manager per la crittografia**.
  - a. Inserire una passphrase.
  - b. Immettere nuovamente la passphrase per confermarla.
  - c. Salvare la passphrase per utilizzarla in futuro in caso di ripristino del sistema.
  - d. Eseguire il backup del database delle chiavi per un utilizzo futuro.
6. Fare clic su **Save** (Salva) per creare il Tier locale e aggiungerlo alla soluzione di storage.



## CLI

Viene eseguito il `storage aggregate auto-provision` comando per generare consigli di layout aggregati. È quindi possibile creare aggregati dopo aver esaminato e approvato i consigli di ONTAP.

### Di cosa hai bisogno

ONTAP 9.2 o versione successiva deve essere in esecuzione sul cluster.

### A proposito di questa attività

Il riepilogo predefinito generato con `storage aggregate auto-provision` il comando elenca gli aggregati consigliati da creare, inclusi i nomi e le dimensioni utilizzabili. È possibile visualizzare l'elenco e determinare se si desidera creare gli aggregati consigliati quando richiesto.

È inoltre possibile visualizzare un riepilogo dettagliato utilizzando `-verbose` che visualizza i seguenti report:

- Riepilogo per nodo dei nuovi aggregati da creare, delle riserve rilevate e dei dischi e delle partizioni di riserva rimanenti dopo la creazione dell'aggregato
- Nuovi aggregati di dati da creare con il numero di dischi e partizioni da utilizzare
- Layout del gruppo RAID che mostra come verranno utilizzati i dischi e le partizioni spare nei nuovi aggregati di dati da creare
- Dettagli sui dischi e le partizioni spare rimanenti dopo la creazione dell'aggregato

Se si conosce il metodo di provisioning automatico e l'ambiente è stato preparato correttamente, è possibile utilizzare `-skip-confirmation` opzione per creare l'aggregato consigliato senza visualizzazione e conferma. Il `storage aggregate auto-provision` La sessione CLI non influisce sul comando `-confirmations` impostazione.

Il `[storage aggregate auto-provision man page^]` contiene ulteriori informazioni sui suggerimenti per il layout aggregato.

### Fasi

1. Eseguire `storage aggregate auto-provision` con le opzioni di visualizzazione desiderate.
  - Nessuna opzione: Visualizza il riepilogo standard
  - `-verbose` Opzione: Visualizza un riepilogo dettagliato
  - `-skip-confirmation` Opzione: Creazione di aggregati consigliati senza visualizzazione o conferma
2. Eseguire una delle seguenti operazioni:

Se si desidera...	Quindi eseguire questa operazione...
-------------------	--------------------------------------

Accetta le raccomandazioni di ONTAP.

Esaminare la visualizzazione degli aggregati consigliati, quindi rispondere alla richiesta di creare gli aggregati consigliati.

```
myA400-44556677::> storage aggregate auto-
provision
Node                               New Data Aggregate
Usable Size
-----
-----
myA400-364                         myA400_364_SSD_1
3.29TB
myA400-363                         myA400_363_SSD_1
1.46TB
-----
-----
Total:                             2      new data aggregates
4.75TB

Do you want to create recommended
aggregates? {y
```

n): y

Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress.

myA400-44556677::>

----

Configurare manualmente i Tier locali e **NOT** utilizzare i consigli di ONTAP.

## Informazioni correlate

["Comandi di ONTAP 9"](#)

### Aggiungere manualmente i Tier locali (creare aggregati)

Se non si desidera aggiungere un Tier locale (creare un aggregato) utilizzando le Best practice di ONTAP, è possibile eseguire il processo manualmente.

### Prima di iniziare

I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato). Se il cluster non è configurato per l'utilizzo dell'assegnazione automatica della proprietà del disco, è necessario ["assegnare la proprietà manualmente"](#).

## System Manager

A partire da ONTAP 9.11.1, se non si desidera utilizzare la configurazione consigliata da Gestore di sistema per creare un Tier locale, è possibile specificare la configurazione desiderata.

### Fasi

1. In System Manager, fare clic su **Storage > Tier**.
2. Nella pagina **Tier**, fare clic su **+ Add Local Tier** per creare un nuovo tier locale:

La pagina **Add Local Tier** mostra il numero consigliato di Tier locali che possono essere creati sui nodi e lo storage utilizzabile disponibile.

3. Quando System Manager visualizza le raccomandazioni relative allo storage per il Tier locale, fare clic su **Switch to Manual Local Tier Creation** (passa alla creazione manuale del Tier locale) nella sezione **Spare Disks**.

La pagina **Add Local Tier** (Aggiungi livello locale) visualizza i campi utilizzati per configurare il livello locale.

4. Nella prima sezione della pagina **Add Local Tier** (Aggiungi livello locale), completare quanto segue:
  - a. Immettere il nome del Tier locale.
  - b. (Facoltativo): Selezionare la casella di controllo **Mirror this local Tier** (Esegui mirroring del livello locale) se si desidera eseguire il mirroring del livello locale.
  - c. Selezionare un tipo di disco.
  - d. Selezionare il numero di dischi.
5. Nella sezione **Configurazione RAID**, completare quanto segue:
  - a. Selezionare il tipo di RAID.
  - b. Selezionare la dimensione del gruppo RAID.
  - c. Fare clic su RAID allocation (allocazione RAID) per visualizzare la modalità di allocazione dei dischi nel gruppo.
6. (Facoltativo): Se Onboard Key Manager è stato installato, è possibile configurarlo per la crittografia nella sezione **Encryption** della pagina. Selezionare la casella di controllo **Configura Onboard Key Manager per la crittografia**.
  - a. Inserire una passphrase.
  - b. Immettere nuovamente la passphrase per confermarla.
  - c. Salvare la passphrase per utilizzarla in futuro in caso di ripristino del sistema.
  - d. Eseguire il backup del database delle chiavi per un utilizzo futuro.
7. Fare clic su **Save** (Salva) per creare il Tier locale e aggiungerlo alla soluzione di storage.

### CLI

Prima di creare gli aggregati manualmente, è necessario rivedere le opzioni di configurazione del disco e simulare la creazione.

A questo punto, è possibile eseguire il `storage aggregate create` controllare e verificare i risultati.

### Di cosa hai bisogno

È necessario determinare il numero di dischi e il numero di dischi hot spare necessari nell'aggregato.

### A proposito di questa attività

Se la partizione root-data-data è attivata e si dispone di 24 unità a stato solido (SSD) o meno nella configurazione, si consiglia di assegnare le partizioni dei dati a nodi diversi.

La procedura per la creazione di aggregati su sistemi con partizione dei dati root e partizione dei dati root abilitata è la stessa della procedura per la creazione di aggregati su sistemi che utilizzano dischi non partizionati. Se la partizione dei dati root è abilitata sul sistema, utilizzare il numero di partizioni del disco per `-diskcount` opzione. Per la partizione root-data-data, il `-diskcount` l'opzione specifica il numero di dischi da utilizzare.



Quando si creano più aggregati per l'utilizzo con FlexGroups, gli aggregati devono avere dimensioni il più possibile vicine.

Il `storage aggregate create` la pagina man contiene ulteriori informazioni sulle opzioni e sui requisiti di creazione degli aggregati.

### Fasi

1. Visualizzare l'elenco delle partizioni dei dischi di riserva per verificare di disporre di una quantità sufficiente per creare l'aggregato:

```
storage aggregate show-spare-disks -original-owner node_name
```

Le partizioni dei dati sono visualizzate in `Local Data Usable`. Non è possibile utilizzare una partizione root come spare.

2. Simulare la creazione dell'aggregato:

```
storage aggregate create -aggregate aggregate_name -node node_name  
-raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
```

3. Se dal comando simulato vengono visualizzate delle avvertenze, regolare il comando e ripetere la simulazione.

4. Creare l'aggregato:

```
storage aggregate create -aggregate aggr_name -node node_name -raidtype  
raid_dp -diskcount number_of_disks_or_partitions
```

5. Visualizzare l'aggregato per verificare che sia stato creato:

```
storage aggregate show-status aggregate_name
```

### Informazioni correlate

["Comandi di ONTAP 9"](#)

### Gestire l'utilizzo di Tier locali (aggregati)

#### Gestire l'utilizzo di Tier locali (aggregati)

Dopo aver creato i Tier locali (aggregati), è possibile gestire il modo in cui vengono utilizzati.

È possibile eseguire le seguenti operazioni:

- "Rinominare un Tier locale (aggregato)"
- "Impostare il costo dei supporti di un Tier locale (aggregato)"
- "Determinare le informazioni su unità e gruppi RAID per un Tier locale (aggregato)"
- "Assegnazione di Tier locali (aggregati) alle macchine virtuali storage (SVM)"
- "Determinare quali volumi risiedono su un Tier locale (aggregato)"
- "Determinare e controllare l'utilizzo dello spazio di un volume in un Tier locale (aggregato)"
- "Determinare l'utilizzo dello spazio in un Tier locale (aggregato)"
- "Spostare la proprietà del Tier locale (aggregato) all'interno di una coppia ha"
- "Eliminazione di un Tier locale (aggregato)"

#### Rinominare un Tier locale (aggregato)


È possibile rinominare un Tier locale (aggregato). Il metodo che si segue dipende dall'interfaccia in uso - System Manager o CLI:

##### System Manager

##### Utilizzare System Manager per rinominare un Tier locale (aggregato)

A partire da ONTAP 9.10.1, è possibile modificare il nome di un Tier locale (aggregato).

##### Fasi

1. In System Manager, fare clic su **Storage > Tier**.
2. Fare clic su  accanto al nome del tier locale.
3. Selezionare **Rinomina**.
4. Specificare un nuovo nome per il Tier locale.

##### CLI

##### Utilizzare la CLI per rinominare un Tier locale (aggregato)

##### Fase

1. Utilizzando la CLI, rinominare il Tier locale (aggregato):

```
storage aggregate rename -aggregate aggr-name -newname aggr-new-name
```

Nell'esempio riportato di seguito un aggregato denominato "aggr5" viene rinominato come "sales-aggr":

```
> storage aggregate rename -aggregate aggr5 -newname sales-aggr
```

#### Impostare il costo dei supporti di un Tier locale (aggregato)

A partire da ONTAP 9.11.1, è possibile utilizzare Gestione sistema per impostare il costo

dei supporti di un Tier locale (aggregato).

#### Fasi

1. In System Manager, fare clic su **Storage > Tier**, quindi fare clic su **Set Media Cost** (Imposta costo supporti) nelle sezioni Local Tier (aggregato) desiderate.
2. Selezionare **Tier attivi e inattivi** per attivare il confronto.
3. Inserire un tipo di valuta e un importo.

Quando si inserisce o si modifica il costo del supporto, la modifica viene apportata a tutti i tipi di supporto.

#### Azzeramento rapido manuale dei dischi

Sui sistemi appena installati con ONTAP 9.4 o versione successiva e sui sistemi reinizializzati con ONTAP 9.4 o versione successiva, viene utilizzato il *azzeramento rapido* per azzerare i dischi.

Con il *azzeramento rapido*, i dischi vengono azzerati in pochi secondi. Questa operazione viene eseguita automaticamente prima del provisioning e riduce notevolmente il tempo necessario per inizializzare il sistema, creare aggregati o espandere aggregati quando vengono aggiunti dischi di riserva.

*Azzeramento rapido* è supportato su SSD e HDD.



*Azzeramento rapido* non è supportato sui sistemi aggiornati da ONTAP 9.3 o versioni precedenti. ONTAP 9.4 o versione successiva deve essere installato di recente o il sistema deve essere reinizializzato. In ONTAP 9.3 e versioni precedenti, anche i dischi vengono azzerati automaticamente da ONTAP, tuttavia il processo richiede più tempo.

Se è necessario azzerare manualmente un disco, è possibile utilizzare uno dei seguenti metodi. In ONTAP 9.4 e versioni successive, l'azzeramento manuale di un disco richiede solo pochi secondi.

## Comando CLI

### Utilizzare un comando CLI per azzerare rapidamente i dischi

#### A proposito di questa attività

Per utilizzare questo comando sono necessari privilegi di amministratore.

#### Fasi

1. Immettere il comando CLI:

```
storage disk zerospares
```

## Opzioni del menu di boot

### Selezionare le opzioni dal menu di boot per azzerare i dischi fast-zero

#### A proposito di questa attività

- La funzione di azzeramento rapido non supporta i sistemi aggiornati da una release precedente a ONTAP 9.4.
- Se un nodo del cluster contiene un Tier locale (aggregato) con dischi con azzeramento rapido, non è possibile ripristinare il cluster a ONTAP 9.2 o versione precedente.

#### Fasi

1. Dal menu di avvio, selezionare una delle seguenti opzioni:
  - (4) pulizia della configurazione e inizializzazione di tutti i dischi
  - (9a) dispartizione di tutti i dischi e rimozione delle informazioni di proprietà
  - (9b) pulizia della configurazione e inizializzazione del nodo con interi dischi

## Assegnare manualmente la proprietà del disco

I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato).

#### A proposito di questa attività

- Se stai assegnando manualmente la proprietà a una coppia ha che non viene inizializzata e che non ha solo DS460C shelf, utilizza l'opzione 1.
- Se stai inizializzando una coppia ha con solo DS460C shelf, puoi utilizzare l'opzione 2 per assegnare manualmente la proprietà dei dischi root.

## Opzione 1: Maggior parte delle coppie ha

Per una coppia ha non inizializzata e che non dispone solo di DS460C shelf, utilizza questa procedura per assegnare manualmente la proprietà.

### A proposito di questa attività

- I dischi per i quali si assegna la proprietà devono trovarsi in uno shelf collegato fisicamente al nodo a cui si assegna la proprietà.
- Se si utilizzano dischi in un Tier locale (aggregato):
  - I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato).
  - Non è possibile riassegnare la proprietà di un disco in uso in un Tier locale (aggregato).

### Fasi

1. Utilizzare la CLI per visualizzare tutti i dischi non posseduti:

```
storage disk show -container-type unassigned
```

2. Assegnare ciascun disco:

```
storage disk assign -disk disk_name -owner owner_name
```

È possibile utilizzare il carattere jolly per assegnare più di un disco alla volta. Se si sta riassegnando un disco spare già di proprietà di un nodo diverso, è necessario utilizzare l'opzione “-force”.



## Opzione 2: Coppia ha con solo DS460C shelf

Per una coppia ha in fase di inizializzazione e dotata di soli DS460C shelf, utilizza questa procedura per assegnare manualmente la proprietà dei dischi root.

### A proposito di questa attività

- Quando esegui l'inizializzazione di una coppia ha con soli DS460C shelf, devi assegnare manualmente i dischi root in modo che siano conformi alla policy a mezzo cassetto.

Dopo l'inizializzazione (boot up) della coppia ha, l'assegnazione automatica della proprietà del disco viene attivata automaticamente e utilizza la policy a mezzo cassetto per assegnare la proprietà ai dischi rimanenti (diversi dai dischi root) e a tutti i dischi aggiunti in futuro, come ad esempio la sostituzione dei dischi guasti, in risposta a un messaggio di "low spare", o aggiungere capacità.

Scoprite la politica di metà cassetto nell'argomento ["Informazioni sull'assegnazione automatica della proprietà del disco"](#).

- RAID richiede un minimo di 10 dischi per ciascuna coppia ha (5 per ogni nodo) per ogni più grande di 8TB dischi NL-SAS in uno shelf DS460C.

### Fasi

1. Se gli shelf DS460C non sono completamente popolati, completare i seguenti passaggi secondari; in caso contrario, passare alla fase successiva.

- a. Innanzitutto, installare le unità nella fila anteriore (alloggiamenti 0, 3, 6 e 9) di ciascun cassetto.

L'installazione dei comandi nella fila anteriore di ciascun cassetto consente il corretto flusso d'aria ed evita il surriscaldamento.

- b. Per i dischi rimanenti, distribuirli in modo uniforme in ciascun cassetto.

Riempire le file dei cassette dalla parte anteriore a quella posteriore. Se non hai dischi sufficienti per riempire le file, installali in coppia in modo che i dischi occupino uniformemente il lato sinistro e destro di un cassetto.

L'illustrazione seguente mostra la numerazione degli alloggiamenti delle unità e le posizioni in un cassetto DS460C.



2. Effettua l'accesso al cluster usando la LIF di gestione nodi o la LIF di gestione cluster.
3. Assegnare manualmente le unità principali in ciascun cassetto in modo che siano conformi al criterio del mezzo cassetto, attenendosi alla seguente procedura:

Nel criterio A mezzo cassetto è stata assegnata la metà sinistra delle unità di un cassetto (alloggiamenti da 0 a 5) al nodo A e la metà destra delle unità di un cassetto (alloggiamenti da 6 a 11) al nodo B.

- a. Visualizza tutti i dischi non posseduti:

```
storage disk show -container-type unassigned`
```

- b. Assegnare i dischi principali:

```
storage disk assign -disk disk_name -owner owner_name
```

È possibile utilizzare il carattere jolly per assegnare più di un disco alla volta.

#### Determinare le informazioni su unità e gruppi RAID per un Tier locale (aggregato)

Alcune attività di amministrazione del Tier locale (aggregato) richiedono di conoscere i tipi di dischi che compongono il Tier locale, le loro dimensioni, checksum e stato, se sono condivisi con altri Tier locali e le dimensioni e la composizione dei gruppi RAID.

#### Fase

1. Mostra i dischi per l'aggregato, in base al gruppo RAID:

```
storage aggregate show-status aggr_name
```

I dischi vengono visualizzati per ciascun gruppo RAID nell'aggregato.

È possibile visualizzare il tipo RAID del disco (dati, parità, dparity) in `Position` colonna. Se il `Position` viene visualizzata la colonna `shared`, Quindi l'unità viene condivisa: Se si tratta di un disco HDD, si tratta di un disco partizionato; se si tratta di un disco SSD, fa parte di un pool di storage.

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

Owner Node: cluster1-a

Aggregate: nodeA\_fp\_1 (online, mixed\_raid\_type, hybrid) (block checksums)

Plex: /nodeA\_fp\_1/plex0 (online, normal, active, pool0)

RAID Group /nodeA\_fp\_1/plex0/rg0 (normal, block checksums, raid\_dp)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.1	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.3	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.5	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.7	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.9	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.11	0	SAS	10000	472.9GB	547.1GB	(normal)

RAID Group /nodeA\_flashpool\_1/plex0/rg1

(normal, block checksums, raid4) (Storage Pool: SmallSP)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.13	0	SSD	-	186.2GB	745.2GB	(normal)
shared	2.0.12	0	SSD	-	186.2GB	745.2GB	(normal)

8 entries were displayed.

### Assegnazione di Tier locali (aggregati) alle macchine virtuali storage (SVM)

Se si assegnano uno o più Tier locali (aggregati) a una macchina virtuale di storage (VM di storage o SVM, precedentemente nota come Vserver), è possibile utilizzare solo questi Tier locali per contenere i volumi per la VM di storage (SVM).

#### Di cosa hai bisogno

La VM di storage e i Tier locali che si desidera assegnare a quella VM di storage devono già esistere.

#### A proposito di questa attività

L'assegnazione di Tier locali alle VM di storage consente di mantenere le VM di storage isolate l'una dall'altra; ciò è particolarmente importante in un ambiente multi-tenancy.

#### Fasi

1. Controllare l'elenco dei Tier locali (aggregati) già assegnati alla SVM:

```
vserver show -fields aggr-list
```

Vengono visualizzati gli aggregati attualmente assegnati alla SVM. Se non sono assegnati aggregati, viene

visualizzato “-”.

2. Aggiungere o rimuovere gli aggregati assegnati, a seconda dei requisiti:

Se si desidera...	Utilizzare questo comando...
Assegnare aggregati aggiuntivi	<code>vserver add-aggregates</code>
Annullare l'assegnazione degli aggregati	<code>vserver remove-aggregates</code>

Gli aggregati elencati vengono assegnati o rimossi dalla SVM. Se la SVM dispone già di volumi che utilizzano un aggregato non assegnato alla SVM, viene visualizzato un messaggio di avviso, ma il comando viene completato correttamente. Tutti gli aggregati già assegnati alla SVM e non denominati nel comando non sono interessati.

### Esempio

Nell'esempio seguente, gli aggregati `aggr1` e `aggr2` sono assegnati a SVM `svm1`:

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

### Determinare quali volumi risiedono su un Tier locale (aggregato)

Potrebbe essere necessario determinare quali volumi risiedono su un Tier locale (aggregato) prima di eseguire operazioni sul Tier locale, ad esempio spostandolo o portandolo offline.

### Fasi

1. Per visualizzare i volumi che risiedono su un aggregato, immettere

```
volume show -aggregate aggregate_name
```

Vengono visualizzati tutti i volumi che risiedono nell'aggregato specificato.

### Determinare e controllare l'utilizzo dello spazio di un volume in un Tier locale (aggregato)

È possibile determinare quali volumi FlexVol utilizzano la maggior parte dello spazio in un Tier locale (aggregato) e in particolare quali funzionalità all'interno del volume.

Il `volume show-footprint` il comando fornisce informazioni sull'impatto di un volume o sull'utilizzo dello spazio all'interno dell'aggregato contenente.

Il `volume show-footprint` il comando mostra i dettagli sull'utilizzo dello spazio di ciascun volume in un aggregato, inclusi i volumi offline. Questo comando colma la distanza tra l'output di `volume show-space` e `aggregate show-space` comandi. Tutte le percentuali sono calcolate come percentuale della dimensione dell'aggregato.

Nell'esempio riportato di seguito viene illustrato il `volume show-footprint` output di comando per un volume chiamato `testvol`:

```
cluster1::> volume show-footprint testvol
```

```
Vserver : thevs
Volume  : testvol
```

Feature	Used	Used%
-----	-----	-----
Volume Data Footprint	120.6MB	4%
Volume Guarantee	1.88GB	71%
Flexible Volume Metadata	11.38MB	0%
Delayed Frees	1.36MB	0%
Total Footprint	2.01GB	76%

La seguente tabella illustra alcune delle righe principali dell'output di `volume show-footprint` e cosa si può fare per cercare di ridurre l'utilizzo dello spazio in base a tale funzione:

Nome riga/funzione	Descrizione/contenuto della riga	Alcuni modi per diminuire
Volume Data Footprint	La quantità totale di spazio utilizzata nell'aggregato contenente dai dati di un volume nel file system attivo e lo spazio utilizzato dalle copie Snapshot del volume. Questa riga non include lo spazio riservato.	<ul style="list-style-type: none"> <li>• Eliminazione dei dati dal volume.</li> <li>• Eliminazione delle copie Snapshot dal volume.</li> </ul>
Volume Guarantee	La quantità di spazio riservato dal volume nell'aggregato per le scritture future. La quantità di spazio riservato dipende dal tipo di garanzia del volume.	Modifica del tipo di garanzia per il volume in none.
Flexible Volume Metadata	La quantità totale di spazio utilizzata nell'aggregato dai file di metadati del volume.	Nessun metodo diretto di controllo.
Delayed Frees	Blocchi utilizzati da ONTAP per le performance e che non possono essere immediatamente liberati. Per le destinazioni SnapMirror, questa riga ha un valore di 0 e non vengono visualizzati.	Nessun metodo diretto di controllo.
File Operation Metadata	La quantità totale di spazio riservato ai metadati delle operazioni del file.	Nessun metodo diretto di controllo.

Total Footprint	La quantità totale di spazio utilizzata dal volume nell'aggregato. È la somma di tutte le righe.	Uno dei metodi utilizzati per ridurre lo spazio utilizzato da un volume.
-----------------	--	--

## Informazioni correlate

["Report tecnico di NetApp 3483: Thin provisioning in un ambiente NetApp SAN o IP SAN Enterprise"](#)

### Determinare l'utilizzo dello spazio in un Tier locale (aggregato)

È possibile visualizzare la quantità di spazio utilizzata da tutti i volumi in uno o più Tier locali (aggregati) in modo da poter intraprendere azioni per liberare più spazio.

WAFL riserva il 10% dello spazio totale su disco per le performance e i metadati a livello aggregato. Lo spazio utilizzato per mantenere i volumi nell'aggregato esce dalla WAFL Reserve e non può essere modificato.



A partire da ONTAP 9.12.1 e versioni successive, la riserva WAFL per gli aggregati superiori a 30TB si riduce dal 10% al 5% per le piattaforme AFF e FAS500f. A partire dal sistema ONTAP 9.14.1, questa stessa riduzione si applica agli aggregati su tutte le piattaforme FAS, producendo il 5% di spazio utilizzabile in più negli aggregati.

È possibile visualizzare l'utilizzo dello spazio da parte di tutti i volumi in uno o più aggregati con `aggregate show-space` comando. In questo modo, è possibile individuare i volumi che consumano più spazio nei relativi aggregati di contenimento, in modo da poter intraprendere azioni per liberare più spazio.

Lo spazio utilizzato in un aggregato è direttamente influenzato dallo spazio utilizzato nei volumi FlexVol in esso contenuti. Le misure adottate per aumentare lo spazio in un volume influiscono anche sullo spazio nell'aggregato.

Le seguenti righe sono incluse in `aggregate show-space` output del comando:

- **Volume Footprint**

Il totale di tutte le impronte di volume all'interno dell'aggregato. Include tutto lo spazio utilizzato o riservato da tutti i dati e i metadati di tutti i volumi nell'aggregato contenente.

- **Metadati aggregati**

I metadati totali del file system richiesti dall'aggregato, come ad esempio bitmap di allocazione e file inode.

- **Snapshot Reserve**

La quantità di spazio riservato per le copie Snapshot aggregate, in base alle dimensioni del volume. Viene considerato spazio utilizzato e non è disponibile per il volume o l'aggregazione di dati o metadati.

- **Snapshot Reserve inutilizzabile**

La quantità di spazio allocato originariamente per la riserva Snapshot aggregata che non è disponibile per le copie Snapshot aggregate perché viene utilizzata dai volumi associati all'aggregato. Può verificarsi solo per gli aggregati con una riserva Snapshot aggregata diversa da zero.

- **Totale utilizzato**

La somma di tutto lo spazio utilizzato o riservato nell'aggregato in base a volumi, metadati o copie Snapshot.

- **Totale fisico utilizzato**

La quantità di spazio utilizzata per i dati ora (anziché essere riservata per uso futuro). Include lo spazio utilizzato dalle copie Snapshot aggregate.

Nell'esempio riportato di seguito viene illustrato il `aggregate show-space` Output di comando per un aggregato la cui riserva Snapshot è del 5%. Se la riserva Snapshot era 0, la riga non veniva visualizzata.

```
cluster1::> storage aggregate show-space
```

Aggregate : wqa\_gx106\_aggr1

Feature	Used	Used%
-----	-----	-----
Volume Footprints	101.0MB	0%
Aggregate Metadata	300KB	0%
Snapshot Reserve	5.98GB	5%
 Total Used	 6.07GB	 5%
Total Physical Used	34.82KB	0%

#### Informazioni correlate

- ["Articolo della Knowledge base: Utilizzo dello spazio"](#)
- ["Liberate fino al 5% della vostra capacità di storage eseguendo l'upgrade a ONTAP 9.12.1"](#)

#### Trasferire la proprietà di un Tier locale (aggregato) all'interno di una coppia ha

È possibile modificare la proprietà dei Tier locali (aggregati) tra i nodi di una coppia ha senza interrompere il servizio dai Tier locali.

Entrambi i nodi di una coppia ha sono fisicamente collegati tra loro a dischi o LUN di array. Ogni LUN di dischi o array è di proprietà di uno dei nodi.

La proprietà di tutti i dischi o le LUN degli array all'interno di un Tier locale (aggregato) cambia temporaneamente da un nodo all'altro quando si verifica un Takeover. Tuttavia, le operazioni di trasferimento dei Tier locali possono anche modificare in modo permanente la proprietà (ad esempio, se eseguite per il bilanciamento del carico). La proprietà cambia senza alcun processo di copia dei dati o spostamento fisico dei dischi o delle LUN degli array.

#### A proposito di questa attività

- Poiché i limiti del numero di volumi vengono validati a livello di programmazione durante le operazioni di trasferimento dei livelli locali, non è necessario controllarli manualmente.

Se il numero di volumi supera il limite supportato, l'operazione di trasferimento del Tier locale non riesce e viene visualizzato un messaggio di errore pertinente.

- Non è consigliabile avviare il trasferimento locale del Tier quando sono in corso operazioni a livello di sistema sul nodo di origine o di destinazione; allo stesso modo, non è necessario avviare queste operazioni durante il trasferimento locale del Tier.

Queste operazioni possono includere quanto segue:

- Takeover
- Giveback
- Spegnerne
- Un'altra operazione di trasferimento locale del Tier
- Modifica della proprietà del disco
- Operazioni di configurazione locale di livelli o volumi
- Sostituzione del controller storage
- Aggiornamento di ONTAP
- Indirizzamento ONTAP
- Se si dispone di una configurazione MetroCluster, non è necessario avviare il trasferimento locale del Tier durante le operazioni di disaster recovery (*switchover*, *healing* o *switchback*).
- Se si dispone di una configurazione MetroCluster e si avvia il trasferimento locale del Tier su un Tier locale switchover, l'operazione potrebbe non riuscire perché supera il numero di limiti di volume del partner DR.
- Non è consigliabile avviare il trasferimento locale del Tier su aggregati corrotti o in fase di manutenzione.
- Prima di iniziare il trasferimento locale del Tier, salvare i core dump sui nodi di origine e di destinazione.

## Fasi

1. Visualizzare gli aggregati sul nodo per confermare quali aggregati spostare e assicurarsi che siano online e in buone condizioni:

```
storage aggregate show -node source-node
```

Il comando seguente mostra sei aggregati sui quattro nodi del cluster. Tutti gli aggregati sono online. Node1 e node3 formano una coppia ha e Node2 e node4 formano una coppia ha.



```
cluster::> storage aggregate show
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID	Status
aggr_0	239.0GB	11.13GB	95%	online	1	node1	raid_dp,	normal
aggr_1	239.0GB	11.13GB	95%	online	1	node1	raid_dp,	normal
aggr_2	239.0GB	11.13GB	95%	online	1	node2	raid_dp,	normal
aggr_3	239.0GB	11.13GB	95%	online	1	node2	raid_dp,	normal
aggr_4	239.0GB	238.9GB	0%	online	5	node3	raid_dp,	normal
aggr_5	239.0GB	239.0GB	0%	online	4	node4	raid_dp,	normal

6 entries were displayed.

## 2. Emettere il comando per avviare il trasferimento dell'aggregato:

```
storage aggregate relocation start -aggregate-list aggregate-1, aggregate-2...
-node source-node -destination destination-node
```

Il seguente comando sposta gli aggregati aggr\_1 e aggr\_2 da Node1 a node3. Node3 è il partner ha di Node1. Gli aggregati possono essere spostati solo all'interno della coppia ha.

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

## 3. Monitorare l'avanzamento del trasferimento degli aggregati con storage aggregate relocation show comando:

```
storage aggregate relocation show -node source-node
```

Il seguente comando mostra l'avanzamento degli aggregati che vengono spostati al nodo 3:

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate      Destination      Relocation Status
-----
node1
      aggr_1          node3            In progress, module: waf1
      aggr_2          node3            Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

Al termine del trasferimento, l'output di questo comando mostra ogni aggregato con uno stato di trasferimento di "Done".

### Eliminazione di un Tier locale (aggregato)

È possibile eliminare un Tier locale (aggregato) se non sono presenti volumi nel Tier locale.

Il `storage aggregate delete` il comando elimina un aggregato di storage. Il comando non riesce se sono presenti volumi nell'aggregato. Se all'aggregato è associato un archivio di oggetti, oltre all'eliminazione dell'aggregato, il comando elimina anche gli oggetti nell'archivio di oggetti. Non vengono apportate modifiche alla configurazione dell'archivio di oggetti come parte di questo comando.

Nell'esempio seguente viene eliminato un aggregato denominato "aggr1":

```
> storage aggregate delete -aggregate aggr1
```

### Comandi per il trasferimento degli aggregati

Esistono comandi ONTAP specifici per spostare la proprietà dell'aggregato all'interno di una coppia ha.

Se si desidera...	Utilizzare questo comando...
Avviare il processo di trasferimento degli aggregati	<code>storage aggregate relocation start</code>
Monitorare il processo di trasferimento degli aggregati	<code>storage aggregate relocation show</code>

### Informazioni correlate

["Comandi di ONTAP 9"](#)

### Comandi per la gestione degli aggregati

Si utilizza `storage aggregate` comando per gestire gli aggregati.

Se si desidera...	Utilizzare questo comando...
Visualizza le dimensioni della cache per tutti gli aggregati di Flash Pool	<code>storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size-total &gt;0</code>
Visualizza le informazioni e lo stato del disco per un aggregato	<code>storage aggregate show-status</code>
Visualizza dischi spare per nodo	<code>storage aggregate show-spare-disks</code>
Visualizzare gli aggregati root nel cluster	<code>storage aggregate show -has-mroot true</code>
Visualizza le informazioni di base e lo stato degli aggregati	<code>storage aggregate show</code>
Visualizza il tipo di storage utilizzato in un aggregato	<code>storage aggregate show -fields storage-type</code>
Porta online un aggregato	<code>storage aggregate online</code>
Eliminare un aggregato	<code>storage aggregate delete</code>
Mettere un aggregato nello stato limitato	<code>storage aggregate restrict</code>
Rinominare un aggregato	<code>storage aggregate rename</code>
Portare un aggregato offline	<code>storage aggregate offline</code>
Modificare il tipo di RAID per un aggregato	<code>storage aggregate modify -raidtype</code>

## Informazioni correlate

["Comandi di ONTAP 9"](#)

## Aggiunta di capacità (dischi) a un Tier locale (aggregato)

### Aggiunta di capacità (dischi) a un Tier locale (aggregato)

Utilizzando metodi diversi, si segue un workflow specifico per aggiungere capacità.

- ["Workflow per aggiungere capacità a un Tier locale \(aggregato\)"](#)
- ["Metodi per creare spazio in un Tier locale \(aggregato\)"](#)

È possibile aggiungere dischi a un Tier locale e dischi a un nodo o a uno shelf.

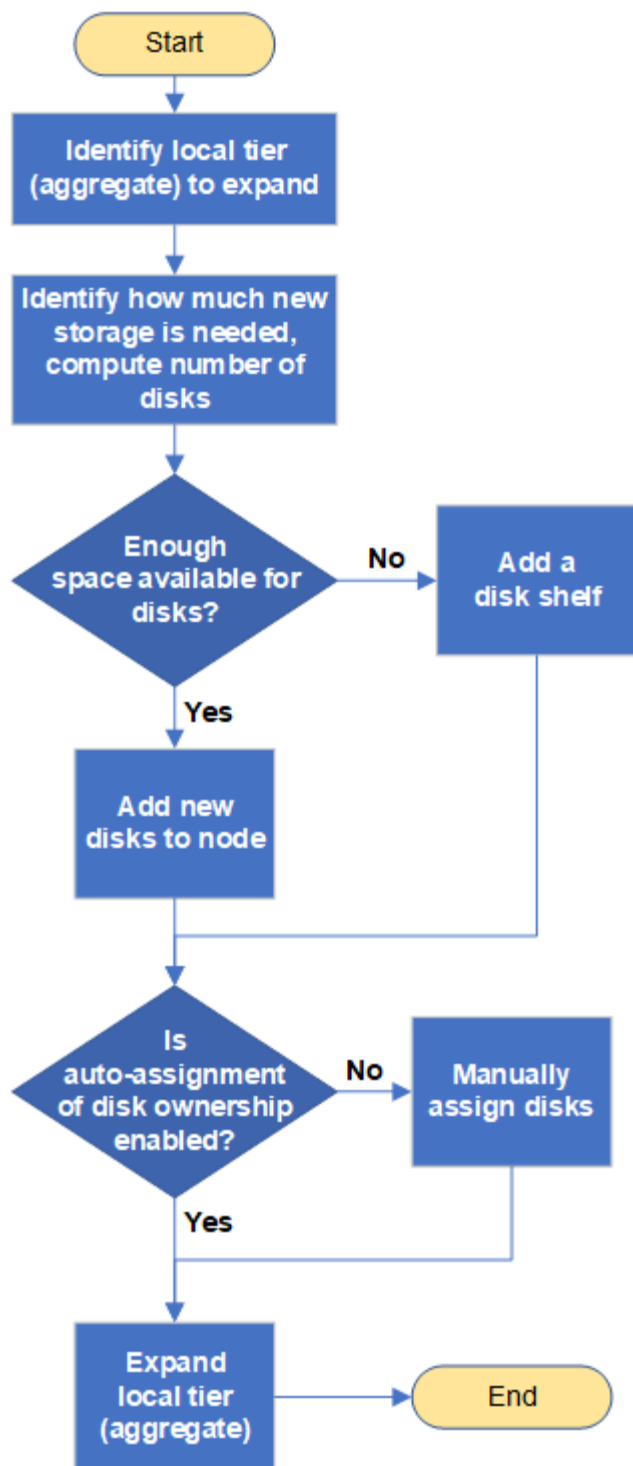
Se necessario, è possibile correggere le partizioni spare disallineate.

- "Aggiunta di dischi a un Tier locale (aggregato)"
- "Aggiungere dischi a un nodo o a uno shelf"
- "Correggere le partizioni sparse disallineate"

#### **Workflow per aggiungere capacità a un Tier locale (espansione di un aggregato)**

Per aggiungere capacità a un Tier locale (espandere un aggregato), è necessario prima identificare il Tier locale a cui si desidera aggiungere, determinare la quantità di nuovo storage necessaria, installare nuovi dischi, assegnare la proprietà del disco e creare un nuovo gruppo RAID, se necessario.

È possibile utilizzare System Manager o CLI per aggiungere capacità.



#### Metodi per creare spazio in un Tier locale (aggregato)

Se un Tier locale (aggregato) esaurisce lo spazio libero, possono verificarsi diversi problemi, dalla perdita di dati alla disattivazione della garanzia di un volume. Esistono diversi modi per creare più spazio in un Tier locale.

Tutti i metodi hanno diverse conseguenze. Prima di intraprendere qualsiasi azione, leggere la relativa sezione della documentazione.

Di seguito sono riportati alcuni metodi comuni per creare spazio nel Tier locale, in ordine da minimo a maggior

parte delle conseguenze:

- Aggiungere dischi al Tier locale.
- Spostare alcuni volumi in un altro Tier locale con spazio disponibile.
- Ridurre le dimensioni dei volumi garantiti dal volume nel Tier locale.
- Eliminare le copie Snapshot del volume non necessarie se il tipo di garanzia del volume è "none".
- Eliminare i volumi non necessari.
- Abilitare funzionalità per il risparmio di spazio, come deduplica o compressione.
- (Temporaneamente) disattivare le funzionalità che utilizzano una grande quantità di metadati .

**Aggiunta di capacità a un Tier locale (aggiunta di dischi a un aggregato)**

È possibile aggiungere dischi a un Tier locale (aggregato) in modo che possa fornire più storage ai volumi associati.

## Gestore di sistema (ONTAP 9.8 e versioni successive)

### Utilizzare Gestione di sistema per aggiungere capacità (ONTAP 9.8 e versioni successive)

È possibile aggiungere capacità a un Tier locale aggiungendo dischi di capacità.




A partire da ONTAP 9.12.1, è possibile utilizzare Gestore di sistema per visualizzare la capacità impegnata di un Tier locale e determinare se è necessaria una capacità aggiuntiva per il Tier locale. Vedere "[Monitorare la capacità in System Manager](#)".

#### A proposito di questa attività

Questa operazione viene eseguita solo se è stato installato ONTAP 9.8 o versione successiva. Se è stata installata una versione precedente di ONTAP, fare riferimento alla scheda (o alla sezione) denominata "Gestore di sistema (ONTAP 9.7 e versioni precedenti)".

#### Fasi

1. Fare clic su **Storage > Tier**.
2. Fare clic su  accanto al nome del tier locale al quale si desidera aggiungere capacità.
3. Fare clic su **Add Capacity** (Aggiungi capacità).



Se non sono presenti dischi di riserva che è possibile aggiungere, l'opzione **Add Capacity** (Aggiungi capacità) non viene visualizzata e non è possibile aumentare la capacità del Tier locale.

4. Attenersi alla seguente procedura, in base alla versione di ONTAP installata:

Se questa versione di ONTAP è installata...	Eseguire questa procedura...
ONTAP 9.8, 9.9 o 9.10.1	<ol style="list-style-type: none"><li>a. Se il nodo contiene più livelli di storage, selezionare il numero di dischi che si desidera aggiungere al livello locale. In caso contrario, se il nodo contiene solo un singolo Tier di storage, la capacità aggiunta viene stimata automaticamente.</li><li>b. Fare clic su <b>Aggiungi</b>.</li></ol>
A partire da ONTAP 9.11.1	<ol style="list-style-type: none"><li>a. Selezionare il tipo di disco e il numero di dischi.</li><li>b. Se si desidera aggiungere dischi a un nuovo gruppo RAID, selezionare la casella di controllo. Viene visualizzata l'allocazione RAID.</li><li>c. Fare clic su <b>Save</b> (Salva).</li></ol>

5. (Facoltativo) il completamento del processo richiede un po' di tempo. Se si desidera eseguire il processo in background, selezionare **Esegui in background**.
6. Al termine del processo, è possibile visualizzare l'aumento della capacità nelle informazioni del Tier locale in **Storage > Tier**.

## Gestore di sistema (ONTAP 9.7 e versioni precedenti)

### Utilizzare Gestione di sistema per aggiungere capacità (ONTAP 9.7 e versioni precedenti)

È possibile aggiungere capacità a un Tier locale (aggregato) aggiungendo dischi di capacità.

### A proposito di questa attività

Questa operazione viene eseguita solo se è stato installato ONTAP 9.7 o una versione precedente. Se è stato installato ONTAP 9.8 o versione successiva, consultare la sezione [Utilizzo di Gestione sistema per aggiungere capacità \(ONTAP 9.8 o versione successiva\)](#).

### Fasi

1. (Solo per ONTAP 9.7) fare clic su **(Torna alla versione classica)**.
2. Fare clic su **hardware e diagnostica > aggregati**.
3. Selezionare l'aggregato a cui si desidera aggiungere dischi di capacità, quindi fare clic su **azioni > Aggiungi capacità**.



È necessario aggiungere dischi delle stesse dimensioni degli altri dischi dell'aggregato.

4. (Solo per ONTAP 9.7) fare clic su **passa alla nuova esperienza**.
5. Fare clic su **Storage > Tier** per verificare le dimensioni del nuovo aggregato.

### CLI

#### Utilizzare la CLI per aggiungere capacità

La procedura per l'aggiunta di dischi partizionati a un aggregato è simile alla procedura per l'aggiunta di dischi non partizionati.

#### Di cosa hai bisogno

È necessario conoscere le dimensioni del gruppo RAID per l'aggregato a cui si aggiunge lo storage.

### A proposito di questa attività

Quando si espande un aggregato, è necessario sapere se si stanno aggiungendo partizioni o dischi non partizionati all'aggregato. Quando si aggiungono unità non partizionate a un aggregato esistente, la dimensione dei gruppi RAID esistenti viene ereditata dal nuovo gruppo RAID, che può influire sul numero di dischi di parità richiesti. Se un disco non partizionato viene aggiunto a un gruppo RAID composto da dischi partizionati, il nuovo disco viene partizionato, lasciando una partizione spare inutilizzata.

Quando si effettua il provisioning delle partizioni, è necessario assicurarsi di non lasciare il nodo senza un disco con entrambe le partizioni come spare. In caso contrario, e il nodo subisce un'interruzione del controller, è possibile che non siano disponibili informazioni preziose sul problema (il file principale) da fornire al supporto tecnico.



Non utilizzare `disklist` per espandere gli aggregati. Ciò potrebbe causare un disallineamento delle partizioni.

### Fasi

1. Mostrare lo storage di riserva disponibile sul sistema proprietario dell'aggregato:

```
storage aggregate show-spare-disks -original-owner node_name
```

È possibile utilizzare `-is-disk-shared` parametro che mostra solo dischi partizionati o solo dischi non partizionati.



```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

				Local	
Local				Data	
Root Physical					
Disk			Type	RPM	Checksum Usable
Usable	Size	Status			
-----					
1.0.1			BSAS	7200	block 753.8GB
73.89GB	828.0GB	zeroed			
1.0.2			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.3			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.4			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.8			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.9			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.10			BSAS	7200	block 0B
73.89GB	828.0GB	zeroed			
2 entries were displayed.					

## 2. Mostra i gruppi RAID correnti per l'aggregato:

```
storage aggregate show-status aggr_name
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1
```

Owner Node: cl1-s2

Aggregate: data\_1 (online, raid\_dp) (block checksums)

Plex: /data\_1/plex0 (online, normal, active, pool0)

RAID Group /data\_1/plex0/rg0 (normal, block checksums)

	Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
	-----	-----	----	----	-----	-----	-----	
-----								
shared	1.0.10	0	BSAS	7200	753.8GB	828.0GB		
(normal)								
shared	1.0.5	0	BSAS	7200	753.8GB	828.0GB		
(normal)								
shared	1.0.6	0	BSAS	7200	753.8GB	828.0GB		
(normal)								
shared	1.0.11	0	BSAS	7200	753.8GB	828.0GB		
(normal)								
shared	1.0.0	0	BSAS	7200	753.8GB	828.0GB		
(normal)								

5 entries were displayed.

### 3. Simulare l'aggiunta dello storage all'aggregato:

```
storage aggregate add-disks -aggregate aggr_name -diskcount  
number_of_disks_or_partitions -simulate true
```

È possibile vedere il risultato dell'aggiunta dello storage senza eseguire il provisioning effettivo dello storage. Se dal comando simulato vengono visualizzate delle avvertenze, è possibile regolare il comando e ripetere la simulazione.

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true
```

Disks would be added to aggregate "aggr\_test" on node "cl1-s2" in the following manner:

First Plex

```
RAID Group rg0, 5 disks (block checksum, raid_dp)

Physical                                     Usable
Position  Disk                               Type      Size
Size
-----
shared    1.11.4                             SSD      415.8GB
415.8GB
shared    1.11.18                            SSD      415.8GB
415.8GB
shared    1.11.19                            SSD      415.8GB
415.8GB
shared    1.11.20                            SSD      415.8GB
415.8GB
shared    1.11.21                            SSD      415.8GB
415.8GB
```

Aggregate capacity available for volume use would be increased by 1.83TB.

#### 4. Aggiungere lo storage all'aggregato:

```
storage aggregate add-disks -aggregate aggr_name -raidgroup new -diskcount
number_of_disks_or_partitions
```

Quando si crea un aggregato Flash Pool, se si aggiungono dischi con un checksum diverso dall'aggregato o se si aggiungono dischi a un aggregato di checksum misto, è necessario utilizzare `-checksumstyle` parametro.

Se si aggiungono dischi a un aggregato di Flash Pool, è necessario utilizzare `-disktype` parametro per specificare il tipo di disco.

È possibile utilizzare `-disksize` parametro per specificare la dimensione dei dischi da aggiungere. Per l'aggiunta all'aggregato vengono selezionati solo i dischi con dimensioni approssimativamente specificate.

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. Verificare che lo storage sia stato aggiunto correttamente:

```
storage aggregate show-status -aggregate aggr_name
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
Aggregate: data_1 (online, raid_dp) (block checksums)
Plex: /data_1/plex0 (online, normal, active, pool0)
RAID Group /data_1/plex0/rg0 (normal, block checksums)

Physical                                                                 Usable
Position Disk                                Pool Type      RPM      Size
Size Status
-----
-----
shared    1.0.10                                0    BSAS      7200    753.8GB
828.0GB (normal)
shared    1.0.5                                0    BSAS      7200    753.8GB
828.0GB (normal)
shared    1.0.6                                0    BSAS      7200    753.8GB
828.0GB (normal)
shared    1.0.11                               0    BSAS      7200    753.8GB
828.0GB (normal)
shared    1.0.0                                0    BSAS      7200    753.8GB
828.0GB (normal)
shared    1.0.2                                0    BSAS      7200    753.8GB
828.0GB (normal)
shared    1.0.3                                0    BSAS      7200    753.8GB
828.0GB (normal)
shared    1.0.4                                0    BSAS      7200    753.8GB
828.0GB (normal)
shared    1.0.8                                0    BSAS      7200    753.8GB
828.0GB (normal)
shared    1.0.9                                0    BSAS      7200    753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. Verificare che il nodo disponga ancora di almeno un disco con la partizione root e la partizione dati come spare:

```
storage aggregate show-spare-disks -original-owner node_name
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

				Local
				Data
Root Physical				
Disk	Type	RPM	Checksum	Usable
Usable Size Status				
1.0.1	BSAS	7200	block	753.8GB
73.89GB 828.0GB zeroed				
1.0.10	BSAS	7200	block	0B
73.89GB 828.0GB zeroed				
2 entries were displayed.				

#### Aggiungere dischi a un nodo o a uno shelf

È possibile aggiungere dischi a un nodo o a uno shelf per aumentare il numero di hot spare o aggiungere spazio al Tier locale (aggregato).

#### Prima di iniziare

L'unità che si desidera aggiungere deve essere supportata dalla piattaforma. È possibile confermare utilizzando ["NetApp Hardware Universe"](#).

Il numero minimo di dischi da aggiungere in una singola procedura è sei. L'aggiunta di un singolo disco potrebbe ridurre le prestazioni.

#### Procedura per l'NetApp Hardware Universe

1. Nel menu a discesa **prodotti**, selezionare la configurazione hardware
2. Selezionare la piattaforma.
3. Selezionare la versione di ONTAP che si sta eseguendo quindi **Mostra risultati**.
4. Sotto l'immagine, selezionare **fare clic qui per visualizzare le viste alternative**. Scegliere la visualizzazione corrispondente alla configurazione.



## Procedura per l'installazione delle unità

1. Controllare ["Sito di supporto NetApp"](#) Per firmware di dischi e shelf più recenti e file di Disk Qualification Package.

Se il nodo o lo shelf non dispone delle versioni più recenti, aggiornarle prima di installare il nuovo disco.

Il firmware del disco viene aggiornato automaticamente (senza interruzioni) sui nuovi dischi che non dispongono delle versioni firmware correnti.

2. Mettere a terra l'utente.
3. Rimuovere delicatamente il pannello frontale dalla parte anteriore della piattaforma.
4. Identificare lo slot corretto per il nuovo disco.



Gli slot corretti per l'aggiunta di dischi variano a seconda del modello di piattaforma e della versione di ONTAP. In alcuni casi è necessario aggiungere unità a slot specifici in sequenza. Ad esempio, in un AFF A800 si aggiungono i dischi a intervalli specifici lasciando cluster di slot vuoti. Mentre in un AFF A220 si aggiungono nuove unità ai successivi slot vuoti che vanno dall'esterno verso il centro dello shelf.

Fare riferimento alla procedura descritta in **prima di iniziare** per identificare gli slot corretti per la configurazione in uso in ["NetApp Hardware Universe"](#).

5. Inserire il nuovo disco:
  - a. Con la maniglia della camma in posizione aperta, inserire il nuovo disco con entrambe le mani.
  - b. Premere fino all'arresto del disco.
  - c. Chiudere la maniglia della camma in modo che l'unità sia completamente inserita nel piano intermedio e la maniglia scatti in posizione. Chiudere lentamente la maniglia della camma in modo che sia allineata correttamente con la superficie dell'unità.
6. Verificare che il LED di attività del disco (verde) sia acceso.

Quando il LED di attività del disco è acceso, significa che il disco è alimentato. Quando il LED di attività del disco lampeggia, significa che il disco è alimentato e che l'i/o è in corso. Se il firmware del disco viene aggiornato automaticamente, il LED lampeggia.

7. Per aggiungere un'altra unità, ripetere i passaggi da 4 a 6.

I nuovi dischi non vengono riconosciuti fino a quando non vengono assegnati a un nodo. È possibile assegnare i nuovi dischi manualmente oppure attendere che ONTAP assegni automaticamente i nuovi dischi se il nodo segue le regole per l'assegnazione automatica dei dischi.

8. Una volta riconosciuti tutti i nuovi dischi, verificare che siano stati aggiunti e che la proprietà sia specificata correttamente.

## Procedura per confermare l'installazione

1. Visualizzare l'elenco dei dischi:

```
storage aggregate show-spare-disks
```

Dovrebbero essere visualizzati i nuovi dischi, di proprietà del nodo corretto.

2. **Facoltativamente (solo per ONTAP 9,3 e versioni precedenti)**, azzerare le unità appena aggiunte:

```
storage disk zerospares
```

I dischi utilizzati in precedenza in un Tier locale (aggregato) ONTAP devono essere azzerati prima di poter essere aggiunti a un altro aggregato. In ONTAP 9.3 e versioni precedenti, il completamento dell'azzeramento può richiedere ore, a seconda delle dimensioni dei dischi non azzerati nel nodo.

L'azzeramento dei dischi consente di evitare ritardi nel caso in cui sia necessario aumentare rapidamente le dimensioni di un Tier locale. Questo non è un problema in ONTAP 9.4 o versioni successive, in cui i dischi vengono azzerati utilizzando *l'azzeramento rapido* che richiede solo secondi.

## Risultati

I nuovi dischi sono pronti. È possibile aggiungerli a un Tier locale (aggregato), inserirli nell'elenco delle hot spare o aggiungerli quando si crea un nuovo Tier locale.

## Correggere le partizioni spare disallineate

Quando si aggiungono dischi partizionati a un Tier locale (aggregato), è necessario lasciare un disco con sia la partizione root che quella di dati disponibili come spare per ogni nodo. In caso contrario, ONTAP non è in grado di eseguire il dump del core nella partizione dei dati di riserva.

## Prima di iniziare

È necessario disporre di una partizione di dati spare e di una partizione root spare sullo stesso tipo di disco di proprietà dello stesso nodo.

## Fasi

1. Usando la CLI, visualizzare le partizioni spare per il nodo:

```
storage aggregate show-spare-disks -original-owner node_name
```

Si noti quale disco ha una partizione di dati spare (spare\_data) e quale disco ha una partizione root spare (spare\_root). La partizione spare mostra un valore diverso da zero sotto Local Data Usable oppure Local Root Usable colonna.

2. Sostituire il disco con una partizione di dati spare con il disco con la partizione root spare:

```
storage disk replace -disk spare_data -replacement spare_root -action start
```

È possibile copiare i dati in entrambe le direzioni; tuttavia, il completamento della copia della partizione root richiede meno tempo.

3. Monitorare l'avanzamento della sostituzione del disco:

```
storage aggregate show-status -aggregate aggr_name
```

4. Una volta completata l'operazione di sostituzione, visualizzare nuovamente le parti di ricambio per confermare che si dispone di un disco libero completo:

```
storage aggregate show-spare-disks -original-owner node_name
```

In "Local Data usable" (dati locali utilizzabili) e nella sezione viene visualizzato un disco spare con spazio utilizzabile Local Root Usable.

## Esempio

Visualizzare le partizioni spare per il nodo c1-01 e verificare che le partizioni spare non siano allineate:

```
c1::> storage aggregate show-spare-disks -original-owner c1-01
```

Original Owner: c1-01

Pool0

Shared HDD Spares

Disk	Type	RPM	Checksum	Local Data Usable	Local Root Usable	Physical Size
1.0.1	BSAS	7200	block	753.8GB	0B	828.0GB
1.0.10	BSAS	7200	block	0B	73.89GB	828.0GB

Viene avviato il processo di sostituzione del disco:

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

Durante l'attesa del completamento dell'operazione di sostituzione, viene visualizzato il seguente stato di avanzamento:

```
c1::> storage aggregate show-status -aggregate aggr0_1
```

Owner Node: c1-01

Aggregate: aggr0\_1 (online, raid\_dp) (block checksums)

Plex: /aggr0\_1/plex0 (online, normal, active, pool0)

RAID Group /aggr0\_1/plex0/rg0 (normal, block checksums)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	1.0.1	0	BSAS	7200	73.89GB	828.0GB	(replacing, copy in progress)
shared	1.0.10	0	BSAS	7200	73.89GB	828.0GB	(copy 63% completed)
shared	1.0.0	0	BSAS	7200	73.89GB	828.0GB	(normal)
shared	1.0.11	0	BSAS	7200	73.89GB	828.0GB	(normal)
shared	1.0.6	0	BSAS	7200	73.89GB	828.0GB	(normal)
shared	1.0.5	0	BSAS	7200	73.89GB	828.0GB	(normal)

Una volta completata l'operazione di sostituzione, verificare di disporre di un disco libero completo:



```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01
```

Original Owner: c1-01

Pool0

Shared HDD Spares

				Local Data Usable	Local Root Usable	Physical Size
Disk	Type	RPM	Checksum			
1.0.1	BSAS	7200	block	753.8GB	73.89GB	828.0GB

## Gestire i dischi

### Panoramica sulla gestione dei dischi

È possibile eseguire varie procedure per gestire i dischi nel sistema.

- **Aspetti della gestione dei dischi**

- ["Quando è necessario aggiornare il Disk Qualification Package"](#)
- ["Funzionamento dei dischi hot spare"](#)
- ["Gli avvisi di riserva bassi possono aiutarti a gestire i dischi spare"](#)
- ["Opzioni aggiuntive di gestione della partizione dei dati root"](#)

- **Proprietà di dischi e partizioni**

- ["Proprietà di dischi e partizioni"](#)

- **Rimozione del disco non riuscita**

- ["Rimuovere un disco guasto"](#)

- **Pulizia del disco**

- ["Pulizia dei dischi"](#)

### Funzionamento dei dischi hot spare

Un disco hot spare è un disco assegnato a un sistema di storage ed è pronto per l'uso, ma non è in uso da un gruppo RAID e non conserva alcun dato.

Se si verifica un guasto al disco all'interno di un gruppo RAID, il disco hot spare viene assegnato automaticamente al gruppo RAID per sostituire i dischi guasti. I dati del disco guasto vengono ricostruiti sul disco sostitutivo hot spare in background dal disco di parità RAID. L'attività di ricostruzione viene registrata in /etc/message Viene inviato un file e un messaggio AutoSupport.

Se il disco hot spare disponibile non ha le stesse dimensioni del disco guasto, viene scelto un disco di dimensioni maggiori successive e quindi ridimensionato in modo da corrispondere alle dimensioni del disco che si sta sostituendo.

## Requisiti di riserva per i dischi portanti multi-disco

Mantenere il numero corretto di dischi di riserva nei carrier multi-disco è fondamentale per ottimizzare la ridondanza dello storage e ridurre al minimo il tempo che ONTAP deve dedicare alla copia dei dischi per ottenere un layout ottimale dei dischi.

È necessario mantenere un minimo di due hot spare per i dischi portanti multi-disco in ogni momento. Per supportare l'utilizzo del Centro di manutenzione ed evitare problemi causati da guasti a più dischi simultanei, è necessario mantenere almeno quattro hot spare per il funzionamento a stato stazionario e sostituire tempestivamente i dischi guasti.

Se due dischi si guastano contemporaneamente con solo due hot spare disponibili, ONTAP potrebbe non essere in grado di scambiare il contenuto del disco guasto e del relativo carrier mate con i dischi spare. Questo scenario è chiamato stallo. In questo caso, viene inviata una notifica tramite messaggi EMS e messaggi AutoSupport. Quando i supporti sostitutivi diventano disponibili, è necessario seguire le istruzioni fornite dai messaggi EMS. Per ulteriori informazioni, consultare l'articolo della Knowledge base ["Impossibile eseguire la calibrazione automatica del layout RAID - messaggio AutoSupport"](#)

## Gli avvisi di riserva bassi possono aiutarti a gestire i dischi spare

Per impostazione predefinita, gli avvisi vengono inviati alla console e ai registri se si dispone di meno di un disco hot spare che corrisponde agli attributi di ciascun disco nel sistema di storage.

È possibile modificare il valore di soglia per questi messaggi di avviso per garantire che il sistema rispetti le Best practice.

### A proposito di questa attività

Impostare l'opzione RAID "min\_spare\_count" su "2" per assicurarsi di disporre sempre del numero minimo di dischi di riserva consigliato.

### Fase

1. Impostare l'opzione su "2":

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

## Opzioni aggiuntive di gestione della partizione dei dati root

A partire da ONTAP 9.2, dal menu di avvio è disponibile una nuova opzione di partizione dei dati root, che offre funzionalità di gestione aggiuntive per i dischi configurati per la partizione dei dati root.

Le seguenti funzionalità di gestione sono disponibili nell'opzione del menu di avvio 9.

- **Dispartizione di tutti i dischi e rimozione delle informazioni di proprietà**

Questa opzione è utile se il sistema è configurato per la partizione dei dati root ed è necessario reinizializzarlo con una configurazione diversa.

- **Pulizia della configurazione e inizializzazione del nodo con dischi partizionati**

Questa opzione è utile per:

- Il sistema non è configurato per la partizione dei dati root e si desidera configurarlo per la partizione dei dati root
- Il sistema non è configurato correttamente per la partizione dei dati root ed è necessario correggerla
- Si dispone di una piattaforma AFF o FAS con solo SSD collegati e configurati per la versione precedente della partizione dei dati root e si desidera aggiornarla alla versione più recente della partizione dei dati root per aumentare l'efficienza dello storage

- **Pulizia della configurazione e inizializzazione del nodo con interi dischi**

Questa opzione è utile per:

- Dispartizione delle partizioni esistenti
- Rimuovere la proprietà del disco locale
- Reinizializzare il sistema con interi dischi utilizzando RAID-DP

### **Quando è necessario aggiornare il Disk Qualification Package**

Il Disk Qualification Package (DQP) aggiunge il supporto completo per i dischi appena qualificati. Prima di aggiornare il firmware del disco o aggiungere nuovi tipi o dimensioni di disco a un cluster, è necessario aggiornare il DQP. Una Best practice consiste nell'aggiornare regolarmente il DQP, ad esempio ogni trimestre o semestrale.

È necessario scaricare e installare DQP nelle seguenti situazioni:

- Ogni volta che si aggiunge un nuovo tipo di disco o una nuova dimensione al nodo

Ad esempio, se si dispone già di dischi da 1 TB e si aggiungono dischi da 2 TB, è necessario verificare la disponibilità dell'aggiornamento DQP più recente.

- Ogni volta che si aggiorna il firmware del disco
- Ogni volta che sono disponibili firmware del disco o file DQP più recenti
- Ogni volta che si esegue l'aggiornamento a una nuova versione di ONTAP.

Il DQP non viene aggiornato come parte di un aggiornamento del ONTAP.

### **Informazioni correlate**

["Download NetApp: Pacchetto di qualificazione dei dischi"](#)

["Download NetApp: Firmware del disco"](#)

### **Proprietà di dischi e partizioni**

#### **Proprietà di dischi e partizioni**

È possibile gestire la proprietà di dischi e partizioni.

È possibile eseguire le seguenti operazioni:

- **"Visualizzare la proprietà di dischi e partizioni"**

È possibile visualizzare la proprietà del disco per determinare quale nodo controlla lo storage. È inoltre

possibile visualizzare la proprietà della partizione sui sistemi che utilizzano dischi condivisi.

- **"Modificare le impostazioni per l'assegnazione automatica della proprietà del disco"**

È possibile selezionare un criterio non predefinito per assegnare automaticamente la proprietà del disco o disattivare l'assegnazione automatica della proprietà del disco.

- **"Assegnare manualmente la proprietà dei dischi non partizionati"**

Se il cluster non è configurato per utilizzare l'assegnazione automatica della proprietà del disco, è necessario assegnare la proprietà manualmente.

- **"Assegnare manualmente la proprietà dei dischi partizionati"**

È possibile impostare la proprietà del disco container o delle partizioni manualmente o utilizzando l'assegnazione automatica, proprio come avviene per i dischi non partizionati.

- **"Rimuovere un disco guasto"**

Un disco che si è guastato completamente non è più considerato da ONTAP come un disco utilizzabile ed è possibile scollegare immediatamente il disco dallo shelf.

- **"Rimuovere la proprietà da un disco"**

ONTAP scrive le informazioni sulla proprietà del disco sul disco. Prima di rimuovere un disco spare o il relativo shelf da un nodo, è necessario rimuovere le relative informazioni di proprietà in modo che possano essere correttamente integrate in un altro nodo.

#### Informazioni sull'assegnazione automatica della proprietà del disco

L'assegnazione automatica dei dischi non proprietari è attivata per impostazione predefinita. L'assegnazione automatica della proprietà del disco avviene 10 minuti dopo l'inizializzazione della coppia ha e ogni cinque minuti durante il normale funzionamento del sistema.

Quando Aggiungi un nuovo disco a una coppia ha, ad esempio quando si sostituisce un disco guasto, si risponde a un messaggio di "low spare" o si aggiunge capacità, la policy predefinita di assegnazione automatica assegna la proprietà del disco a un nodo come spare.

La policy di assegnazione automatica predefinita si basa su caratteristiche specifiche della piattaforma o sullo shelf DS460C, se la coppia ha dispone solo di questi shelf, e utilizza uno dei seguenti metodi (policy) per assegnare la proprietà dei dischi:

Metodo di assegnazione	Effetto sulle assegnazioni dei nodi	Configurazioni di piattaforma predefinite per il metodo di assegnazione
baia	Gli alloggiamenti con numero pari sono assegnati al nodo A e quelli con numero dispari al nodo B.	Sistemi entry-level in una configurazione ha Pair con un singolo shelf condiviso.

shelf	Tutti i dischi nello shelf sono assegnati al nodo A.	Sistemi entry-level in configurazione con coppia ha con uno stack di due o più shelf e configurazioni MetroCluster con uno stack per nodo, due o più shelf.
shelf separato  Questa politica rientra nel valore "default" per il <code>-autoassign -policy</code> del parametro <code>storage disk option</code> comando per le configurazioni di piattaforma e shelf applicabili.	I dischi sul lato sinistro dello shelf sono assegnati al nodo A e sul lato destro al nodo B. Gli shelf parziali sulle coppie ha vengono spediti dalla fabbrica con dischi popolati dal bordo dello shelf verso il centro.	La maggior parte delle piattaforme AFF e alcune configurazioni MetroCluster.
impilare	Tutti i dischi nello stack vengono assegnati al nodo A.	Sistemi entry-level autonomi e tutte le altre configurazioni.
mezzo cassetto  Questa politica rientra nel valore "default" per il <code>-autoassign -policy</code> del parametro <code>storage disk option</code> comando per le configurazioni di piattaforma e shelf applicabili.	<p>Tutti i dischi nella metà sinistra di un cassetto da DS460C GB (alloggiamenti per unità da 0 a 5) sono assegnati al nodo A; tutti i dischi nella metà destra di un cassetto (alloggiamenti per unità da 6 a 11) sono assegnati al nodo B.</p> <p>Quando si inizializza una coppia ha con solo DS460C shelf, l'assegnazione automatica della proprietà del disco non è supportata. È necessario assegnare manualmente la proprietà per le unità contenenti unità root/container che hanno la partizione root in base al criterio half-cassetti.</p>	<p>Coppie HA con solo DS460C shelf, dopo l'inizializzazione della coppia ha (avvio).</p> <p>Dopo l'avvio di una coppia ha, l'assegnazione automatica della proprietà del disco viene attivata automaticamente e utilizza la policy a mezzo cassetto per assegnare la proprietà ai dischi rimanenti (ad eccezione dei dischi root/container che hanno la partizione root) e a eventuali dischi aggiunti in futuro.</p> <p>Se la coppia ha ha DS460C shelf oltre agli altri modelli, non verrà utilizzata la policy a mezzo cassetto. Il criterio predefinito utilizzato è dettato dalle caratteristiche specifiche della piattaforma.</p>

#### Impostazioni e modifiche dell'assegnazione automatica:

- È possibile visualizzare le impostazioni di assegnazione automatica correnti (on/off) con `storage disk option show` comando.
- È possibile disattivare l'assegnazione automatica utilizzando `storage disk option modify` comando.
- Se il criterio di assegnazione automatica predefinito non è consigliabile nell'ambiente in uso, è possibile specificare (modificare) il metodo di assegnazione alloggiamento, shelf o stack utilizzando `-autoassign -policy` nel `storage disk option modify` comando.

Scopri come ["Modificare le impostazioni per l'assegnazione automatica della proprietà del disco"](#).



I criteri di assegnazione automatica predefiniti a mezzo cassetto e a scaffale diviso sono univoci perché non possono essere impostati dagli utenti come i criteri di alloggiamento, scaffale e stack.

Nei sistemi ADP (Advanced Drive Partitioning), per eseguire l'assegnazione automatica di shelf half-popled, i dischi devono essere installati negli alloggiamenti corretti in base al tipo di shelf di cui si dispone:

- Se il tuo shelf non è uno shelf da DS460C, installa i dischi in maniera equilibrata sul lato sinistro e sul lato destro, spostandoti al centro. Ad esempio, sei dischi negli alloggiamenti 0-5 e sei dischi negli alloggiamenti 18-23 di uno shelf DS224C.
- Se lo shelf è DS460C, installare i dischi della prima fila (alloggiamenti 0, 3, 6 e 9) di ciascun cassetto. Per le unità rimanenti, distribuirle uniformemente su ciascun cassetto riempiendo le file dei cassette dalla parte anteriore a quella posteriore. Se non hai dischi sufficienti per riempire le file, installali in coppia in modo che i dischi occupino uniformemente il lato sinistro e destro di un cassetto.

L'installazione dei comandi nella fila anteriore di ciascun cassetto consente il corretto flusso d'aria ed evita il surriscaldamento.



Se i dischi non sono installati negli alloggiamenti corretti sugli shelf popolati a metà, in caso di guasto e sostituzione del disco di un container, ONTAP non assegna automaticamente la proprietà. In questo caso, l'assegnazione della nuova unità contenitore deve essere eseguita manualmente. Dopo aver assegnato la proprietà ai dischi del container, ONTAP gestisce automaticamente tutte le assegnazioni necessarie per le partizioni e il partizionamento dei dischi.

In alcune situazioni in cui l'assegnazione automatica non funziona, è necessario assegnare manualmente la proprietà del disco tramite `storage disk assign` comando:

- Se si disattiva l'assegnazione automatica, i nuovi dischi non sono disponibili come spare fino a quando non verranno assegnati manualmente a un nodo.
- Se si desidera che i dischi vengano assegnati automaticamente e si dispone di più stack o shelf che devono avere proprietà diverse, un disco deve essere stato assegnato manualmente su ogni stack o shelf in modo che l'assegnazione automatica della proprietà funzioni su ogni stack o shelf.
- Se l'assegnazione automatica è attivata e si assegna manualmente un singolo disco a un nodo non specificato nel criterio attivo, l'assegnazione automatica smette di funzionare e viene visualizzato un messaggio EMS.

Scopri come ["Assegnare manualmente la proprietà dei dischi non partizionati"](#).

Scopri come ["Assegnare manualmente la proprietà dei dischi partizionati"](#).

#### Visualizzare la proprietà di dischi e partizioni

È possibile visualizzare la proprietà del disco per determinare quale nodo controlla lo storage. È inoltre possibile visualizzare la proprietà della partizione sui sistemi che utilizzano dischi condivisi.

#### Fasi

1. Visualizzare la proprietà dei dischi fisici:

```
storage disk show -ownership
```

```
cluster::> storage disk show -ownership
Disk      Aggregate Home      Owner      DR Home  Home ID      Owner ID      DR
Home ID   Reserver   Pool
-----
1.0.0     aggr0_2    node2      node2      -          2014941509  2014941509  -
2014941509 Pool0
1.0.1     aggr0_2    node2      node2      -          2014941509  2014941509  -
2014941509 Pool0
1.0.2     aggr0_1    node1      node1      -          2014941219  2014941219  -
2014941219 Pool0
1.0.3     -          node1      node1      -          2014941219  2014941219  -
2014941219 Pool0
```

2. Se si dispone di un sistema che utilizza dischi condivisi, è possibile visualizzare la proprietà della partizione:

```
storage disk show -partition-ownership
```

```
cluster::> storage disk show -partition-ownership
                                     Root      Data
Container  Container
Disk      Aggregate Root Owner  Owner ID      Data Owner  Owner ID      Owner
Owner ID
-----
1.0.0     -          node1      1886742616  node1      1886742616  node1
1886742616
1.0.1     -          node1      1886742616  node1      1886742616  node1
1886742616
1.0.2     -          node2      1886742657  node2      1886742657  node2
1886742657
1.0.3     -          node2      1886742657  node2      1886742657  node2
1886742657
```

#### Modificare le impostazioni per l'assegnazione automatica della proprietà del disco

È possibile utilizzare `storage disk option modify` per selezionare una policy non predefinita per l'assegnazione automatica della proprietà del disco o per la disattivazione dell'assegnazione automatica della proprietà del disco.

Scopri di più ["assegnazione automatica della proprietà del disco"](#).

## A proposito di questa attività

Se disponi di una coppia ha con solo DS460C shelf, il criterio di assegnazione automatica predefinito è a metà cassetto. Non è possibile passare a un criterio non predefinito (alloggiamento, shelf, stack).

### Fasi

#### 1. Modificare l'assegnazione automatica dei dischi:

- a. Se si desidera selezionare un criterio non predefinito, immettere:

```
storage disk option modify -autoassign-policy autoassign_policy -node  
node_name
```

- Utilizzare *stack* come *autoassign\_policy* per configurare la proprietà automatica a livello di stack o loop.
- Utilizzare *shelf* come *autoassign\_policy* per configurare la proprietà automatica a livello di shelf.
- Utilizzare *bay* come *autoassign\_policy* per configurare la proprietà automatica a livello di alloggiamento.

- b. Se si desidera disattivare l'assegnazione automatica della proprietà del disco, immettere:

```
storage disk option modify -autoassign off -node node_name
```

#### 2. Verificare le impostazioni di assegnazione automatica dei dischi:

```
storage disk option show
```

```
cluster1::> storage disk option show
```

Node	BKg. FW. Upd.	Auto Copy	Auto Assign	Auto Assign Policy
-----	-----	-----	-----	-----
cluster1-1	on	on	on	default
cluster1-2	on	on	on	default

## Assegnare manualmente la proprietà dei dischi non partizionati

Se la coppia ha non è configurata per l'utilizzo dell'assegnazione automatica della proprietà del disco, devi assegnare manualmente la proprietà. Se stai inizializzando una coppia ha con solo DS460C shelf, devi assegnare manualmente la proprietà dei dischi root.

## A proposito di questa attività

- Se stai assegnando manualmente la proprietà a una coppia ha che non viene inizializzata e che non ha solo DS460C shelf, utilizza l'opzione 1.
- Se stai inizializzando una coppia ha con solo DS460C shelf, puoi utilizzare l'opzione 2 per assegnare manualmente la proprietà dei dischi root.



## Opzione 1: Maggior parte delle coppie ha

Per una coppia ha non inizializzata e che non dispone solo di DS460C shelf, utilizza questa procedura per assegnare manualmente la proprietà.

### A proposito di questa attività

- I dischi per i quali si assegna la proprietà devono trovarsi in uno shelf collegato fisicamente al nodo a cui si assegna la proprietà.
- Se si utilizzano dischi in un Tier locale (aggregato):
  - I dischi devono essere di proprietà di un nodo prima di poter essere utilizzati in un Tier locale (aggregato).
  - Non è possibile riassegnare la proprietà di un disco in uso in un Tier locale (aggregato).

### Fasi

1. Utilizzare la CLI per visualizzare tutti i dischi non posseduti:

```
storage disk show -container-type unassigned
```

2. Assegnare ciascun disco:

```
storage disk assign -disk disk_name -owner owner_name
```

È possibile utilizzare il carattere jolly per assegnare più di un disco alla volta. Se si sta riassegnando un disco spare già di proprietà di un nodo diverso, è necessario utilizzare l'opzione “-force”.

## Opzione 2: Coppia ha con solo DS460C shelf

Per una coppia ha in fase di inizializzazione e dotata di soli DS460C shelf, utilizza questa procedura per assegnare manualmente la proprietà dei dischi root.

### A proposito di questa attività

- Quando esegui l'inizializzazione di una coppia ha con soli DS460C shelf, devi assegnare manualmente i dischi root in modo che siano conformi alla policy a mezzo cassetto.

Dopo l'inizializzazione (boot up) della coppia ha, l'assegnazione automatica della proprietà del disco viene attivata automaticamente e utilizza la policy a mezzo cassetto per assegnare la proprietà ai dischi rimanenti (diversi dai dischi root) e a tutti i dischi aggiunti in futuro, come ad esempio la sostituzione dei dischi guasti, in risposta a un messaggio di "low spare", o aggiungere capacità.

Scoprite la politica di metà cassetto nell'argomento ["Informazioni sull'assegnazione automatica della proprietà del disco"](#).

- RAID richiede un minimo di 10 dischi per ciascuna coppia ha (5 per ogni nodo) per ogni più grande di 8TB dischi NL-SAS in uno shelf DS460C.

### Fasi

1. Se gli shelf DS460C non sono completamente popolati, completare i seguenti passaggi secondari; in caso contrario, passare alla fase successiva.

- a. Innanzitutto, installare le unità nella fila anteriore (alloggiamenti 0, 3, 6 e 9) di ciascun cassetto.

L'installazione dei comandi nella fila anteriore di ciascun cassetto consente il corretto flusso d'aria ed evita il surriscaldamento.

- b. Per i dischi rimanenti, distribuirli in modo uniforme in ciascun cassetto.

Riempire le file dei cassette dalla parte anteriore a quella posteriore. Se non hai dischi sufficienti per riempire le file, installali in coppia in modo che i dischi occupino uniformemente il lato sinistro e destro di un cassetto.

L'illustrazione seguente mostra la numerazione degli alloggiamenti delle unità e le posizioni in un cassetto DS460C.



2. Effettua l'accesso al cluster usando la LIF di gestione nodi o la LIF di gestione cluster.
3. Assegnare manualmente le unità principali in ciascun cassetto in modo che siano conformi al criterio del mezzo cassetto, attenendosi alla seguente procedura:

Nel criterio A mezzo cassetto è stata assegnata la metà sinistra delle unità di un cassetto (alloggiamenti da 0 a 5) al nodo A e la metà destra delle unità di un cassetto (alloggiamenti da 6 a 11) al nodo B.

- a. Visualizza tutti i dischi non posseduti:

```
storage disk show -container-type unassigned`
```

- b. Assegnare i dischi principali:

```
storage disk assign -disk disk_name -owner owner_name
```

È possibile utilizzare il carattere jolly per assegnare più di un disco alla volta.

### Assegnare manualmente la proprietà dei dischi partizionati

Puoi assegnare manualmente la proprietà del disco del container o delle partizioni sui sistemi ADP (Advanced Disk Partitioning). Se si sta inizializzando una coppia ha con solo DS460C shelf, è necessario assegnare manualmente la proprietà per i dischi dei container che includeranno le partizioni root.

#### A proposito di questa attività

- Il tipo di sistema di storage stabilito determina il metodo di ADP supportato, root-data (RD) o root-data-data (RD2).

I sistemi storage FAS utilizzano la RD e i sistemi storage AFF RD2.

- Se si assegna manualmente la proprietà in una coppia ha che non viene inizializzata e non ha solo DS460C shelf, utilizzare l'opzione 1 per assegnare manualmente i dischi con partizione root-data (RD) oppure utilizzare l'opzione 2 per assegnare manualmente i dischi con partizione root-data-data (RD2).
- Se si sta inizializzando una coppia ha con solo DS460C shelf, utilizzare l'opzione 3 per assegnare

manualmente la proprietà ai dischi dei container che hanno la partizione root.

**Opzione 1: Assegnazione manuale dei dischi con partizione root-data (RD)**

Per la partizione dei dati root, esistono tre entità possedute (il disco container e le due partizioni) collettivamente di proprietà della coppia ha.

**A proposito di questa attività**

- Il disco container e le due partizioni non devono essere tutte di proprietà dello stesso nodo della coppia ha, purché siano tutte di proprietà di uno dei nodi della coppia ha. Tuttavia, quando si utilizza una partizione in un Tier locale (aggregato), questa deve essere di proprietà dello stesso nodo proprietario del Tier locale.
- Se un disco contenitore si guasta in uno shelf mezzo popolato e viene sostituito, potrebbe essere necessario assegnare manualmente la proprietà del disco perché in questo caso ONTAP non sempre assegna automaticamente la proprietà.
- Una volta assegnato il disco del container, il software ONTAP gestisce automaticamente tutte le partizioni e le assegnazioni necessarie.

**Fasi**

1. Utilizzare la CLI per visualizzare la proprietà corrente del disco partizionato:

```
storage disk show -disk disk_name -partition-ownership
```

2. Impostare il livello di privilegio CLI su Advanced (avanzato):

```
set -privilege advanced
```

3. Immettere il comando appropriato, a seconda dell'entità di proprietà per cui si desidera assegnare la proprietà:

Se una delle entità di proprietà è già di proprietà, devi includere l'opzione “-force”.

Se si desidera assegnare la proprietà per...	Utilizzare questo comando...
Disco container	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i></code>
Partizione dei dati	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data true</code>
Partizione root	<code>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -root true</code>

**Opzione 2: Assegnazione manuale dei dischi con partizione root-data-data (RD2)**

Per la partizione root-data-data, esistono quattro entità possedute (il disco container e le tre partizioni) collettivamente di proprietà della coppia ha. La partizione root-data-data crea una partizione piccola come partizione root e due partizioni più grandi e di pari dimensioni per i dati.

**A proposito di questa attività**

- I parametri devono essere utilizzati con `disk assign` comando per assegnare la partizione corretta di un disco partizionato root-data-data. Non è possibile utilizzare questi parametri con dischi che fanno parte di un pool di storage. Il valore predefinito è “false”.
  - Il `-data1 true` il parametro assegna la partizione “data1” di un disco partizionato root-data1-data2.
  - Il `-data2 true` il parametro assegna la partizione “data2” di un disco partizionato root-data1-data2.
- Se un disco contenitore si guasta in uno shelf mezzo popolato e viene sostituito, potrebbe essere necessario assegnare manualmente la proprietà del disco perché in questo caso ONTAP non sempre assegna automaticamente la proprietà.
- Una volta assegnato il disco del container, il software ONTAP gestisce automaticamente tutte le partizioni e le assegnazioni necessarie.

**Fasi**

1. Utilizzare la CLI per visualizzare la proprietà corrente del disco partizionato:

```
storage disk show -disk disk_name -partition-ownership
```

2. Impostare il livello di privilegio CLI su Advanced (avanzato):

```
set -privilege advanced
```

3. Immettere il comando appropriato, a seconda dell'entità di proprietà per cui si desidera assegnare la proprietà:

Se una delle entità di proprietà è già di proprietà, devi includere l'opzione “-force”.

Se si desidera assegnare la proprietà per...	Utilizzare questo comando...
Disco container	<code>storage disk assign -disk disk_name -owner owner_name</code>
Partizione Data1	<code>storage disk assign -disk disk_name -owner owner_name -data1 true</code>
Partizione Data2	<code>storage disk assign -disk disk_name -owner owner_name -data2 true</code>
Partizione root	<code>storage disk assign -disk disk_name -owner owner_name -root true</code>

### Opzione 3: Assegnare manualmente DS460C unità contenitore che hanno la partizione root

Se si sta inizializzando una coppia ha con solo DS460C shelf, occorre assegnare manualmente la proprietà per i dischi dei container che hanno la partizione root, conformemente al criterio half-cassetto.

#### A proposito di questa attività

- Quando si inizializza una coppia ha con solo DS460C shelf, le opzioni 9a e 9b del menu di boot ADP (disponibile con ONTAP 9,2 e versioni successive) non supportano l'assegnazione automatica della proprietà dei dischi. È necessario assegnare manualmente le unità contenitore che hanno la partizione root in base al criterio half-cassetti.

Dopo l'inizializzazione (avvio) della coppia ha, l'assegnazione automatica della proprietà del disco viene attivata automaticamente e utilizza la policy a mezzo cassetto per assegnare la proprietà ai dischi rimanenti (diversi dai dischi dei container che hanno la partizione root) e a eventuali dischi aggiunti in futuro, come ad esempio la sostituzione dei dischi guasti, risposta a un messaggio di "riserva insufficiente" o aggiunta di capacità.

- Scoprite la politica di metà cassetto nell'argomento ["Informazioni sull'assegnazione automatica della proprietà del disco"](#).

#### Fasi

1. Se gli shelf DS460C non sono completamente popolati, completare i seguenti passaggi secondari; in caso contrario, passare alla fase successiva.

- a. Innanzitutto, installare le unità nella fila anteriore (alloggiamenti 0, 3, 6 e 9) di ciascun cassetto.

L'installazione dei comandi nella fila anteriore di ciascun cassetto consente il corretto flusso d'aria ed evita il surriscaldamento.

- b. Per i dischi rimanenti, distribuirli in modo uniforme in ciascun cassetto.

Riempire le file dei cassette dalla parte anteriore a quella posteriore. Se non hai dischi sufficienti per riempire le file, installali in coppia in modo che i dischi occupino uniformemente il lato sinistro e destro di un cassetto.

L'illustrazione seguente mostra la numerazione degli alloggiamenti delle unità e le posizioni in un cassetto DS460C.



2. Effettua l'accesso al cluster usando la LIF di gestione nodi o la LIF di gestione cluster.
3. Per ogni cassetto, assegnare manualmente le unità contenitore che hanno la partizione root in base al criterio Half-Drawer utilizzando i seguenti passaggi secondari:

Nel criterio A mezzo cassetto è stata assegnata la metà sinistra delle unità di un cassetto (alloggiamenti da 0 a 5) al nodo A e la metà destra delle unità di un cassetto (alloggiamenti da 6 a 11) al nodo B.

- a. Visualizza tutti i dischi non posseduti:  
`storage disk show -container-type unassigned`
- b. Assegnare le unità contenitore che hanno la partizione root:  
`storage disk assign -disk disk_name -owner owner_name`

È possibile utilizzare il carattere jolly per assegnare più unità alla volta.

#### Impostare una configurazione Active-passive sui nodi utilizzando la partizione dei dati root

Quando una coppia ha viene configurata in fabbrica per utilizzare la partizione dei dati root, la proprietà delle partizioni dei dati viene divisa tra entrambi i nodi della coppia per essere utilizzata in una configurazione Active-Active. Se si desidera utilizzare la coppia ha in una configurazione Active-passive, è necessario aggiornare la proprietà della partizione prima di creare il livello locale dei dati (aggregato).

#### Di cosa hai bisogno

- Si dovrebbe aver deciso quale nodo sarà il nodo attivo e quale nodo sarà il nodo passivo.
- Il failover dello storage deve essere configurato sulla coppia ha.

#### A proposito di questa attività

Questa attività viene eseguita su due nodi: Il nodo A e il nodo B.

Questa procedura è progettata per i nodi per i quali non è stato creato alcun Tier locale di dati (aggregato) dai dischi partizionati.

Scopri di più ["partizione avanzata dei dischi"](#).

**Fasi**

Tutti i comandi vengono immessi nella shell del cluster.

- 1. Visualizzare la proprietà corrente delle partizioni dei dati:

```
storage aggregate show-spare-disks
```

L'output mostra che metà delle partizioni di dati appartiene a un nodo e metà all'altro. Tutte le partizioni dei dati devono essere spare.

```
cluster1::> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
  Partitioned Spares
    Local
    Local
    Root Physical
    Disk
    Usable      Size
    -----
    1.0.0
    0B  828.0GB
    1.0.1
    73.89GB  828.0GB
    1.0.5
    0B  828.0GB
    1.0.6
    0B  828.0GB
    1.0.10
    0B  828.0GB
    1.0.11
    0B  828.0GB
    Type      RPM Checksum      Usable
    BSAS      7200 block      753.8GB
    BSAS      7200 block      753.8GB
    BSAS      7200 block      753.8GB
    BSAS      7200 block      753.8GB
    BSAS      7200 block      753.8GB
    BSAS      7200 block      753.8GB
    BSAS      7200 block      753.8GB

Original Owner: cluster1-02
Pool0
  Partitioned Spares
    Local
    Local
    Root Physical
    Disk
    Usable      Size
    -----
    Type      RPM Checksum      Usable
```



```

-----
1.0.2                BSAS      7200 block      753.8GB
0B  828.0GB
1.0.3                BSAS      7200 block      753.8GB
0B  828.0GB
1.0.4                BSAS      7200 block      753.8GB
0B  828.0GB
1.0.7                BSAS      7200 block      753.8GB
0B  828.0GB
1.0.8                BSAS      7200 block      753.8GB
73.89GB  828.0GB
1.0.9                BSAS      7200 block      753.8GB
0B  828.0GB
12 entries were displayed.

```

2. Immettere il livello di privilegio avanzato:

```
set advanced
```

3. Per ciascuna partizione di dati di proprietà del nodo che sarà il nodo passivo, assegnarla al nodo attivo:

```
storage disk assign -force -data true -owner active_node_name -disk disk_name
```

Non è necessario includere la partizione come parte del nome del disco.

Immettere un comando simile all'esempio seguente per ciascuna partizione di dati da riassegnare:

```
storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3
```

4. Verificare che tutte le partizioni siano assegnate al nodo attivo.

```

cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
  Partitioned Spares
                                Local
Local
                                Data
Root Physical
Disk          Type      RPM Checksum      Usable
Usable      Size
-----
-----
1.0.0                BSAS      7200 block      753.8GB
0B  828.0GB

```

```

1.0.1          BSAS      7200 block      753.8GB
73.89GB  828.0GB
1.0.2          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.3          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.4          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.5          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.6          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.7          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.8          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.9          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.10         BSAS      7200 block      753.8GB
0B  828.0GB
1.0.11         BSAS      7200 block      753.8GB
0B  828.0GB

```

Original Owner: cluster1-02

Pool0

Partitioned Spares

Local

Local

Data

Root Physical

Disk

Type

RPM Checksum

Usable

Usable      Size

```

-----
-----
1.0.8          BSAS      7200 block      0B

```

73.89GB 828.0GB

13 entries were displayed.

Si noti che il cluster1-02 possiede ancora una partizione root spare.

5. Tornare al privilegio amministrativo:

```
set admin
```

6. Crea il tuo aggregato di dati, lasciando almeno una partizione di dati come spare:

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
```

*active\_node\_name*

L'aggregato di dati viene creato e appartiene al nodo attivo.

#### Impostare una configurazione Active-passive sui nodi utilizzando la partizione root-data-data

Quando una coppia ha viene configurata per utilizzare la partizione dei dati root in fabbrica, la proprietà delle partizioni dei dati viene divisa tra entrambi i nodi della coppia per essere utilizzata in una configurazione Active-Active. Se si desidera utilizzare la coppia ha in una configurazione Active-passive, è necessario aggiornare la proprietà della partizione prima di creare il livello locale dei dati (aggregato).

#### Di cosa hai bisogno

- Si dovrebbe aver deciso quale nodo sarà il nodo attivo e quale nodo sarà il nodo passivo.
- Il failover dello storage deve essere configurato sulla coppia ha.

#### A proposito di questa attività

Questa attività viene eseguita su due nodi: Il nodo A e il nodo B.

Questa procedura è progettata per i nodi per i quali non è stato creato alcun Tier locale di dati (aggregato) dai dischi partizionati.

Scopri di più ["partizione avanzata dei dischi"](#).

#### Fasi

Tutti i comandi vengono immessi nella shell del cluster.

1. Visualizzare la proprietà corrente delle partizioni dei dati:

```
storage aggregate show-spare-disks -original-owner passive_node_name -fields  
local-usable-data1-size, local-usable-data2-size
```

L'output mostra che metà delle partizioni di dati appartiene a un nodo e metà all'altro. Tutte le partizioni dei dati devono essere spare.

2. Immettere il livello di privilegio avanzato:

```
set advanced
```

3. Per ogni partizione data1 di proprietà del nodo che sarà il nodo passivo, assegnarla al nodo attivo:

```
storage disk assign -force -data1 -owner active_node_name -disk disk_name
```

Non è necessario includere la partizione come parte del nome del disco

4. Per ogni partizione data2 di proprietà del nodo che sarà il nodo passivo, assegnarla al nodo attivo:

```
storage disk assign -force -data2 -owner active_node_name -disk disk_name
```

Non è necessario includere la partizione come parte del nome del disco

5. Verificare che tutte le partizioni siano assegnate al nodo attivo:

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
Partitioned Spares

Local
Local
Data
Root Physical
Disk          Type      RPM Checksum  Usable
Usable      Size
-----
-----
1.0.0        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.1        BSAS      7200 block    753.8GB
73.89GB  828.0GB
1.0.2        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.3        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.4        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.5        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.6        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.7        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.8        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.9        BSAS      7200 block    753.8GB
0B  828.0GB
1.0.10       BSAS      7200 block    753.8GB
0B  828.0GB
1.0.11       BSAS      7200 block    753.8GB
0B  828.0GB

Original Owner: cluster1-02
Pool0
Partitioned Spares

Local
Local
Data
```

```

Root Physical
Disk                               Type      RPM  Checksum      Usable
Usable      Size
-----
1.0.8                               BSAS      7200  block          0B
73.89GB    828.0GB
13 entries were displayed.

```

Si noti che il cluster1-02 possiede ancora una partizione root spare.

#### 6. Tornare al privilegio amministrativo:

```
set admin
```

#### 7. Crea il tuo aggregato di dati, lasciando almeno una partizione di dati come spare:

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
active_node_name
```

L'aggregato di dati viene creato e appartiene al nodo attivo.

#### 8. In alternativa, è possibile utilizzare il layout aggregato consigliato da ONTAP, che include Best practice per il layout dei gruppi RAID e il numero di spare:

```
storage aggregate auto-provision
```

### Rimuovere la proprietà da un disco

ONTAP scrive le informazioni sulla proprietà del disco sul disco. Prima di rimuovere un disco spare o il relativo shelf da un nodo, è necessario rimuovere le relative informazioni di proprietà in modo che possano essere correttamente integrate in un altro nodo.



Se il disco è partizionato per la partizione root-dati e si sta eseguendo ONTAP 9.10.1 o versioni successive, contattare il supporto tecnico di NetApp per assistenza nella rimozione della proprietà. Per ulteriori informazioni, consultare ["Articolo della Knowledge base: Impossibile rimuovere il proprietario del disco"](#).

### Di cosa hai bisogno

Il disco da cui si desidera rimuovere la proprietà deve soddisfare i seguenti requisiti:

- Deve essere un disco spare.

Non è possibile rimuovere la proprietà da un disco utilizzato in un Tier locale (aggregato).

- Non può trovarsi nel centro di manutenzione.
- Non può essere sottoposto a sanificazione.
- Non è possibile eseguire il guasto.

Non è necessario rimuovere la proprietà da un disco guasto.

### A proposito di questa attività

Se l'assegnazione automatica dei dischi è attivata, ONTAP potrebbe riassegnare automaticamente la proprietà prima di rimuovere il disco dal nodo. Per questo motivo, si disattiva l'assegnazione automatica della proprietà fino a quando il disco non viene rimosso, quindi si riattiva.

#### Fasi

1. Se l'assegnazione automatica della proprietà del disco è attivata, utilizzare la CLI per disattivarla:

```
storage disk option modify -node node_name -autoassign off
```

2. Se necessario, ripetere il passaggio precedente per il partner ha del nodo.
3. Rimuovere le informazioni di proprietà del software dal disco:

```
storage disk removeowner disk_name
```

Per rimuovere le informazioni di proprietà da più dischi, utilizzare un elenco separato da virgole.

Esempio:

```
storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
```

4. Se il disco è partizionato per la partizione root-dati e si esegue ONTAP 9.9.1 o versioni precedenti, rimuovere la proprietà dalle partizioni:

```
storage disk removeowner -disk disk_name -root true
```

```
storage disk removeowner -disk disk_name -data true
```

Entrambe le partizioni non sono più di proprietà di alcun nodo.

5. Se in precedenza è stata disattivata l'assegnazione automatica della proprietà del disco, attivarla dopo la rimozione o la riassegnazione del disco:

```
storage disk option modify -node node_name -autoassign on
```

6. Se necessario, ripetere il passaggio precedente per il partner ha del nodo.

### Rimuovere un disco guasto

Un disco completamente guasto non viene più conteggiato da ONTAP come disco utilizzabile ed è possibile scollegare immediatamente il disco dallo shelf. Tuttavia, si consiglia di lasciare un disco parzialmente guasto collegato abbastanza a lungo per il completamento del processo di ripristino RAID rapido.

### A proposito di questa attività

Se si rimuove un disco perché si è verificato un errore o perché genera messaggi di errore eccessivi, non utilizzare nuovamente il disco in questo o in qualsiasi altro sistema di storage.

#### Fasi

1. Utilizzare l'interfaccia CLI per individuare l'ID del disco guasto:

```
storage disk show -broken
```

Se il disco non compare nell'elenco dei dischi guasti, potrebbe essersi verificato un errore parziale, con un ripristino RAID rapido in corso. In questo caso, prima di rimuovere il disco, è necessario attendere che il disco sia presente nell'elenco dei dischi guasti (il che significa che il processo di ripristino RAID rapido è completo).

2. Determinare la posizione fisica del disco che si desidera rimuovere:

```
storage disk set-led -action on -disk disk_name 2
```

Il LED di errore sulla parte anteriore del disco è acceso.

3. Rimuovere il disco dallo shelf seguendo le istruzioni riportate nella guida hardware del modello di shelf.

## Pulizia dei dischi

### Panoramica sulla disinfezione dei dischi

La sanificazione del disco è il processo di cancellazione fisica dei dati mediante la sovrascrittura di dischi o SSD con modelli di byte specifici o dati casuali, in modo che il ripristino dei dati originali diventi impossibile. L'utilizzo del processo di sanificazione garantisce che nessuno possa ripristinare i dati sui dischi.

Questa funzionalità è disponibile attraverso il nodeshell in tutte le release di ONTAP 9 e a partire da ONTAP 9.6 in modalità di manutenzione.

Il processo di sanificazione del disco utilizza tre modelli di sovrascrittura dei byte predefiniti o specificati dall'utente per un massimo di sette cicli per operazione. Il modello di sovrascrittura casuale viene ripetuto per ogni ciclo.

A seconda della capacità del disco, dei modelli e del numero di cicli, il processo può richiedere diverse ore. La sanitizzazione viene eseguita in background. È possibile avviare, arrestare e visualizzare lo stato del processo di disinfezione. Il processo di sanificazione contiene due fasi: La "fase di formattazione" e la "fase di sovrascrittura del modello".

### Fase di formattazione

L'operazione eseguita per la fase di formattazione dipende dalla classe di dischi da sanificare, come mostrato nella tabella seguente:

Classe di dischi	Operazione della fase di formattazione
Capacità HDD	Ignorato
HDD dalle performance elevate	Funzionamento in formato SCSI
SSD	Operazione di sanificazione SCSI

### Fase di sovrascrittura del modello

I modelli di sovrascrittura specificati vengono ripetuti per il numero di cicli specificato.

Una volta completato il processo di sanificazione, i dischi specificati si trovano in uno stato di sanificazione. Non vengono ripristinati automaticamente lo stato spare. È necessario restituire i dischi sanitizzati al pool di spare prima che i dischi appena sanitizzati siano disponibili per essere aggiunti a un altro aggregato.

## Quando non è possibile eseguire la sanificazione del disco

La pulizia dei dischi non è supportata per tutti i tipi di dischi. Inoltre, in alcuni casi non è possibile eseguire la sanificazione del disco.

- Non è supportato su tutti i codici prodotto SSD.

Per informazioni sui codici prodotto SSD che supportano la disinfezione dei dischi, consultare "[Hardware Universe](#)".

- Non è supportato in modalità Takeover per i sistemi in una coppia ha.
- Non può essere eseguito su dischi che si sono guastati a causa di problemi di leggibilità o di scrivibilità.
- Non esegue la relativa fase di formattazione sui dischi ATA.
- Se si utilizza il modello random, non è possibile eseguirlo su più di 100 dischi alla volta.
- Non è supportato sui LUN degli array.
- Se si disigienizzano entrambi i dischi SES nello stesso shelf ESH contemporaneamente, vengono visualizzati errori sulla console relativi all'accesso a tale shelf e gli avvisi sullo shelf non vengono segnalati per la durata della sanitizzazione.

Tuttavia, l'accesso ai dati a tale shelf non viene interrotto.

## Cosa succede se la pulizia del disco viene interrotta

Se la sanificazione del disco viene interrotta da un intervento dell'utente o da un evento imprevisto, ad esempio un'interruzione dell'alimentazione, ONTAP esegue un'azione per riportare i dischi sottoposti a sanitizzazione a uno stato noto, ma è necessario eseguire un'azione prima che il processo di sanitizzazione possa terminare.

La sanificazione dei dischi è un'operazione a esecuzione prolungata. Se il processo di sanificazione viene interrotto da un'interruzione dell'alimentazione, dal panico del sistema o da un intervento manuale, il processo di sanificazione deve essere ripetuto dall'inizio. Il disco non è stato progettato come sanitizzato.

Se la fase di formattazione della disinfezione del disco viene interrotta, ONTAP deve ripristinare i dischi danneggiati dall'interruzione. Dopo un riavvio del sistema e una volta ogni ora, ONTAP verifica la presenza di eventuali dischi di destinazione per la sanificazione che non hanno completato la fase di formattazione della relativa sanificazione. Se vengono rilevati dischi di questo tipo, ONTAP li ripristina. Il metodo di ripristino dipende dal tipo di disco. Una volta ripristinato un disco, è possibile rieseguire il processo di pulizia su tale disco; per gli HDD, è possibile utilizzare `-s` opzione per specificare che la fase di formattazione non viene ripetuta.

## Suggerimenti per la creazione e il backup di Tier locali (aggregati) contenenti dati da sanificare

Se si creano o eseguono il backup di Tier locali (aggregati) per contenere dati che potrebbero dover essere sanificati, seguire alcune semplici linee guida ridurrà il tempo necessario per la sanificazione dei dati.

- Assicurati che i livelli locali contenenti dati sensibili non siano più grandi di quanto sia necessario.

Se sono più grandi del necessario, la sanitizzazione richiede più tempo, spazio su disco e larghezza di banda.



- Quando si esegue il backup dei Tier locali contenenti dati sensibili, evitare di eseguirne il backup su Tier locale che contenga anche grandi quantità di dati non sensibili.

In questo modo si riducono le risorse necessarie per spostare i dati non sensibili prima di procedere alla pulizia dei dati sensibili.

#### **Igienizzare un disco**

La sanificazione di un disco consente di rimuovere i dati da un disco o da un set di dischi su sistemi decommissionati o inutilizzabili, in modo che i dati non possano mai essere ripristinati.

Sono disponibili due metodi per la sanificazione dei dischi mediante l'interfaccia CLI:

## Sanificazione di un disco con & 8220;modalità di manutenzione& 8221; comandi (ONTAP 9.6 e versioni successive)

A partire da ONTAP 9.6, è possibile eseguire la pulizia del disco in modalità di manutenzione.

### Prima di iniziare

- I dischi non possono essere dischi con crittografia automatica (SED).

È necessario utilizzare `storage encryption disk sanitize` Comando per sanificare un SED.

"Crittografia dei dati inattivi"

### Fasi

1. Avviare in modalità di manutenzione.

- a. Uscire dalla shell corrente immettendo `halt`.

Viene visualizzato il prompt DEL CARICATORE.

- b. Accedere alla modalità di manutenzione immettendo `boot_ontap maint`.

Una volta visualizzate alcune informazioni, viene visualizzato il prompt della modalità di manutenzione.

2. Se i dischi da sanificare sono partizionati, dispartizionare ciascun disco:



Il comando per dispartizionare un disco è disponibile solo a livello di DIAG e deve essere eseguito solo sotto la supervisione del supporto NetApp. Si consiglia vivamente di contattare il supporto NetApp prima di procedere. Consultare anche l'articolo della Knowledge base "[Come dispartizionare un disco spare in ONTAP](#)"

```
disk unpartition disk_name
```

3. Igienizzare i dischi specificati:

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c cycle_count] disk_list
```



Non spegnere il nodo, interrompere la connettività dello storage o rimuovere i dischi di destinazione durante la pulizia. Se la pulizia viene interrotta durante la fase di formattazione, la fase di formattazione deve essere riavviata e completata prima che i dischi siano stati sanitizzati e pronti per essere restituiti al pool di riserva. Se è necessario interrompere il processo di sanificazione, è possibile farlo utilizzando `disk sanitize abort` comando. Se i dischi specificati sono sottoposti alla fase di formattazione della disinfezione, l'interruzione non avviene fino al completamento della fase.

``-p` `_pattern1_` `-p` `_pattern2_` `-p` `_pattern3_`` specifica un ciclo di uno o tre modelli di sovrascrittura di byte esadecimali definiti dall'utente che possono essere applicati in successione ai dischi da sanificare. Il modello predefinito è tre passaggi, utilizzando 0x55 per il primo passaggio, 0xaa per il secondo passaggio e 0x3c per il terzo passaggio.

`-r` sostituisce una sovrascrittura ripetuta con una sovrascrittura casuale per uno o tutti i passaggi.

`-c cycle_count` specifica il numero di volte in cui vengono applicati i modelli di sovrascrittura specificati. Il valore predefinito è un ciclo. Il valore massimo è di sette cicli.

`disk_list` Specifica un elenco degli ID dei dischi spare da sanificare, separati da spazio.

4. Se lo si desidera, controllare lo stato del processo di pulizia del disco:

```
disk sanitize status [disk_list]
```

5. Una volta completato il processo di sanificazione, riportare i dischi allo stato spare per ciascun disco:

```
disk sanitize release disk_name
```

6. Uscire dalla modalità di manutenzione.

## Sanificazione di un disco con i comandi 8220; nodeshell 8221; (tutte le release di ONTAP 9)

Per tutte le versioni di ONTAP 9, quando la disinfezione del disco viene attivata utilizzando comandi nodeshell, alcuni comandi ONTAP di basso livello sono disattivati. Una volta attivata la sanificazione del disco su un nodo, non è possibile disattivarla.

### Prima di iniziare

- I dischi devono essere dischi spare; devono essere di proprietà di un nodo, ma non devono essere utilizzati in un Tier locale (aggregato).

Se i dischi sono partizionati, nessuna partizione può essere utilizzata in un Tier locale (aggregato).

- I dischi non possono essere dischi con crittografia automatica (SED).

È necessario utilizzare `storage encryption disk sanitize` Comando per sanificare un SED.

#### "Crittografia dei dati inattivi"

- I dischi non possono far parte di un pool di storage.

### Fasi

1. Se i dischi da sanificare sono partizionati, dispartizionare ciascun disco:



Il comando per dispartizionare un disco è disponibile solo a livello di DIAG e deve essere eseguito solo sotto la supervisione del supporto NetApp. **Si consiglia vivamente di contattare il supporto NetApp prima di procedere.** è inoltre possibile consultare l'articolo della Knowledge base ["Come dispartizionare un disco spare in ONTAP"](#).

```
disk unpartition disk_name
```

2. Immettere il nodeshell per il nodo proprietario dei dischi che si desidera disinfettare:

```
system node run -node node_name
```

3. Abilitare la sanificazione del disco:

```
options licensed_feature.disk_sanitization.enable on
```

Viene richiesto di confermare il comando perché è irreversibile.

4. Passa al livello avanzato di privilegi più avanzato:

```
priv set advanced
```

5. Igienizzare i dischi specificati:

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c cycle_count] disk_list
```



Non spegnere il nodo, interrompere la connettività dello storage o rimuovere i dischi di destinazione durante la pulizia. Se la pulizia viene interrotta durante la fase di formattazione, la fase di formattazione deve essere riavviata e completata prima che i dischi siano stati sanitizzati e pronti per essere restituiti al pool di riserva. Se è necessario interrompere il processo di sanificazione, è possibile farlo utilizzando il comando `disk sanitize abortor`. Se i dischi specificati sono sottoposti alla fase di formattazione della disinfezione, l'interruzione non avviene fino al completamento della fase.

`-p pattern1 -p pattern2 -p pattern3` specifica un ciclo di uno o tre modelli di sovrascrittura di byte esadecimali definiti dall'utente che possono essere applicati in successione ai dischi da sanificare. Il modello predefinito è tre passaggi, utilizzando 0x55 per il primo passaggio, 0xaa per il secondo passaggio e 0x3c per il terzo passaggio.

`-r` sostituisce una sovrascrittura ripetuta con una sovrascrittura casuale per uno o tutti i passaggi.

`-c cycle_count` specifica il numero di volte in cui vengono applicati i modelli di sovrascrittura specificati.

Il valore predefinito è un ciclo. Il valore massimo è di sette cicli.

`disk_list` Specifica un elenco degli ID dei dischi spare da sanificare, separati da spazio.

6. Se si desidera controllare lo stato del processo di pulizia del disco:

```
disk sanitize status [disk_list]
```

7. Una volta completato il processo di sanificazione, riportare i dischi allo stato spare:

```
disk sanitize release disk_name
```

8. Torna al livello di privilegio admin nodeshell:

```
priv set admin
```

9. Tornare all'interfaccia utente di ONTAP:

```
exit
```

10. Determinare se tutti i dischi sono stati riportati allo stato spare:

```
storage aggregate show-spare-disks
```

Se...	Quindi...
Tutti i dischi sanitizzati sono elencati come spare	Hai finito. I dischi sono stati sanitizzati e in stato spare.

Alcuni dischi sanitizzati non sono elencati come dischi di riserva

Attenersi alla seguente procedura:

a. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

b. Assegnare i dischi sanitizzati non assegnati al nodo appropriato per ciascun disco:

```
storage disk assign -disk disk_name -owner  
node_name
```

c. Riportare i dischi allo stato spare per ciascun disco:

```
storage disk unfail -disk disk_name -s -q
```

d. Tornare alla modalità amministrativa:

```
set -privilege admin
```

## Risultato

I dischi specificati vengono sanitizzati e designati come hot spare. I numeri di serie dei dischi sanitizzati vengono scritti in `/etc/log/sanitized_disks`.

Vengono scritti i log di disk sanitization che mostrano gli elementi completati su ogni disco  
`/mroot/etc/log/sanitization.log`.

## Comandi per la gestione dei dischi

È possibile utilizzare `storage disk` e `storage aggregate` comandi per gestire i dischi.

Se si desidera...	Utilizzare questo comando...
Visualizza un elenco di dischi di riserva, inclusi i dischi partizionati, per proprietario	<code>storage aggregate show-spare-disks</code>
Visualizza il tipo di RAID del disco, l'utilizzo corrente e il gruppo RAID per aggregato	<code>storage aggregate show-status</code>
Visualizzare il tipo di RAID, l'utilizzo corrente, l'aggregato e il gruppo RAID, inclusi i ricambi, per i dischi fisici	<code>storage disk show -raid</code>
Visualizza un elenco di dischi guasti	<code>storage disk show -broken</code>

Visualizzare il nome del disco pre-cluster (nodescope) per un disco	<code>storage disk show -primary-paths (avanzato)</code>
Accendere il LED di un disco o di uno shelf specifico	<code>storage disk set-led</code>
Visualizza il tipo di checksum per un disco specifico	<code>storage disk show -fields checksum-compatibility</code>
Visualizza il tipo di checksum per tutti i dischi spare	<code>storage disk show -fields checksum-compatibility -container-type spare</code>
Visualizzazione delle informazioni sulla connettività e sul posizionamento dei dischi	<code>storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay</code>
Visualizzare i nomi dei dischi pre-cluster per dischi specifici	<code>storage disk show -disk diskname -fields diskpathnames</code>
Visualizzare l'elenco dei dischi nel centro di manutenzione	<code>storage disk show -maintenance</code>
Mostra la durata dell'unità SSD	<code>storage disk show -ssd-wear</code>
Dispartizione di un disco condiviso	<code>storage disk unpartition (disponibile a livello diagnostico)</code>
Azzerare tutti i dischi non azzerati	<code>storage disk zerospares</code>
Interrompere un processo di sanificazione in corso su uno o più dischi specificati	<code>system node run -node nodename -command disk sanitize</code>
Visualizzare le informazioni sul disco di crittografia dello storage	<code>storage encryption disk show</code>
Recuperare le chiavi di autenticazione da tutti i server di gestione delle chiavi collegati	<code>security key-manager restore</code>

## Informazioni correlate

["Comandi di ONTAP 9"](#)

## Comandi per la visualizzazione delle informazioni sull'utilizzo dello spazio

Si utilizza `storage aggregate` e `volume` Comandi per vedere come viene utilizzato lo spazio negli aggregati, nei volumi e nelle relative copie Snapshot.

Per visualizzare informazioni su...	Utilizzare questo comando...
Aggregati, inclusi i dettagli sulle percentuali di spazio utilizzate e disponibili, le dimensioni della riserva Snapshot e altre informazioni sull'utilizzo dello spazio	<code>storage aggregate show</code> <code>storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code>
Modalità di utilizzo dei dischi e dei gruppi RAID in un aggregato e nello stato RAID	<code>storage aggregate show-status</code>
La quantità di spazio su disco che verrebbe recuperata se si elimina una copia Snapshot specifica	<code>volume snapshot compute-reclaimable</code>
La quantità di spazio utilizzata da un volume	<code>volume show -fields size,used,available,percent-used</code> <code>volume show-space</code>
La quantità di spazio utilizzata da un volume nell'aggregato contenente	<code>volume show-footprint</code>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

#### Comandi per visualizzare informazioni sugli shelf di storage

Si utilizza `storage shelf show` comando per visualizzare le informazioni di configurazione e di errore per gli shelf di dischi.

Se si desidera visualizzare...	Utilizzare questo comando...
Informazioni generali sulla configurazione dello shelf e sullo stato dell'hardware	<code>storage shelf show</code>
Informazioni dettagliate per uno shelf specifico, incluso l'ID dello stack	<code>storage shelf show -shelf</code>
Errori irrisolti, gestibili dal cliente, per shelf	<code>storage shelf show -errors</code>
Informazioni sugli alloggiamenti	<code>storage shelf show -bay</code>
Informazioni sulla connettività	<code>storage shelf show -connectivity</code>
Informazioni sul raffreddamento, tra cui sensori di temperatura e ventole di raffreddamento	<code>storage shelf show -cooling</code>
Informazioni sui moduli i/O.	<code>storage shelf show -module</code>



Se si desidera visualizzare...	Utilizzare questo comando...
Informazioni sulla porta	<code>storage shelf show -port</code>
Informazioni sull'alimentazione, inclusi PSU (alimentatori), sensori di corrente e sensori di tensione	<code>storage shelf show -power</code>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

## Gestire le configurazioni RAID

### Panoramica sulla gestione delle configurazioni RAID

È possibile eseguire varie procedure per gestire le configurazioni RAID nel sistema.

- **Aspetti della gestione delle configurazioni RAID:**
  - ["Policy RAID predefinite per Tier locali \(aggregati\)"](#)
  - ["Livelli di protezione RAID per i dischi"](#)
- **Informazioni su unità e gruppi RAID per un Tier locale (aggregato)**
  - ["Determinare le informazioni su unità e gruppi RAID per un Tier locale \(aggregato\)"](#)
- **Conversioni della configurazione RAID**
  - ["Conversione da RAID-DP a RAID-TEC"](#)
  - ["Conversione da RAID-TEC a RAID-DP"](#)
- **Dimensionamento del gruppo RAID**
  - ["Considerazioni per il dimensionamento dei gruppi RAID"](#)
  - ["Personalizzare le dimensioni del gruppo RAID"](#)

### Policy RAID predefinite per Tier locali (aggregati)

RAID-DP o RAID-TEC è il criterio RAID predefinito per tutti i nuovi Tier locali (aggregati). Il criterio RAID determina la protezione di parità in caso di guasto del disco.

RAID-DP offre una protezione a doppia parità in caso di guasto di un disco singolo o doppio. RAID-DP è il criterio RAID predefinito per i seguenti tipi di Tier locale (aggregato):

- Tier locali All Flash
- Tier locali di Flash Pool
- Tier locali dei dischi rigidi (HDD) dalle performance elevate

RAID-TEC è supportato su tutti i tipi di dischi e su tutte le piattaforme, incluso AFF. I Tier locali che contengono dischi più grandi hanno una maggiore possibilità di guasti simultanei dei dischi. RAID-TEC aiuta a mitigare questo rischio fornendo una protezione a tripla parità in modo che i dati possano sopravvivere fino a tre guasti simultanei del disco. RAID-TEC è il criterio RAID predefinito per i Tier locali di capacità dei dischi rigidi con dischi di 6 TB o superiori.

Ogni tipo di policy RAID richiede un numero minimo di dischi:

- RAID-DP: Minimo 5 dischi
- RAID-TEC: Minimo 7 dischi

### **Livelli di protezione RAID per i dischi**

ONTAP supporta tre livelli di protezione RAID per Tier locali (aggregati). Il livello di protezione RAID determina il numero di dischi di parità disponibili per il ripristino dei dati in caso di guasti al disco.

Con la protezione RAID, se si verifica un guasto al disco dati in un gruppo RAID, ONTAP può sostituire il disco guasto con un disco spare e utilizzare i dati di parità per ricostruire i dati del disco guasto.

- **RAID4**

Con la protezione RAID4, ONTAP può utilizzare un disco spare per sostituire e ricostruire i dati da un disco guasto all'interno del gruppo RAID.

- **RAID-DP**

Con la protezione RAID-DP, ONTAP può utilizzare fino a due dischi di riserva per sostituire e ricostruire i dati da un massimo di due dischi guasti contemporaneamente all'interno del gruppo RAID.

- **RAID-TEC**

Con la protezione RAID-TEC, ONTAP può utilizzare fino a tre dischi di riserva per sostituire e ricostruire i dati da un massimo di tre dischi guasti contemporaneamente all'interno del gruppo RAID.

### **Informazioni su unità e gruppi RAID per un Tier locale (aggregato)**

Alcune attività di amministrazione del Tier locale (aggregato) richiedono di conoscere i tipi di dischi che compongono il Tier locale, le loro dimensioni, checksum e stato, se sono condivisi con altri Tier locali e le dimensioni e la composizione dei gruppi RAID.

#### **Fase**

1. Mostra i dischi per l'aggregato, in base al gruppo RAID:

```
storage aggregate show-status aggr_name
```

I dischi vengono visualizzati per ciascun gruppo RAID nell'aggregato.

È possibile visualizzare il tipo RAID del disco (dati, parità, dparity) in `Position` colonna. Se il `Position` viene visualizzata la colonna `shared`, Quindi l'unità viene condivisa: Se si tratta di un disco HDD, si tratta di un disco partizionato; se si tratta di un disco SSD, fa parte di un pool di storage.

```
cluster1::> storage aggregate show-status nodeA_fp_1
```

Owner Node: cluster1-a

Aggregate: nodeA\_fp\_1 (online, mixed\_raid\_type, hybrid) (block checksums)

Plex: /nodeA\_fp\_1/plex0 (online, normal, active, pool0)

RAID Group /nodeA\_fp\_1/plex0/rg0 (normal, block checksums, raid\_dp)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.1	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.3	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.5	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.7	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.9	0	SAS	10000	472.9GB	547.1GB	(normal)
shared	2.0.11	0	SAS	10000	472.9GB	547.1GB	(normal)

RAID Group /nodeA\_flashpool\_1/plex0/rg1

(normal, block checksums, raid4) (Storage Pool: SmallSP)

Position	Disk	Pool	Type	RPM	Usable Size	Physical Size	Status
shared	2.0.13	0	SSD	-	186.2GB	745.2GB	(normal)
shared	2.0.12	0	SSD	-	186.2GB	745.2GB	(normal)

8 entries were displayed.

## Conversione da RAID-DP a RAID-TEC

Se si desidera una protezione aggiuntiva della tripla parità, è possibile convertire da RAID-DP a RAID-TEC. RAID-TEC è consigliato se le dimensioni dei dischi utilizzati nel Tier locale (aggregato) sono superiori a 4 TiB.

### Di cosa hai bisogno

Il Tier locale (aggregato) da convertire deve avere un minimo di sette dischi.

### A proposito di questa attività

I Tier locali dei dischi rigidi possono essere convertiti da RAID-DP a RAID-TEC. Sono inclusi i Tier HDD nei Tier locali di Flash Pool.

### Fasi

1. Verificare che l'aggregato sia online e disponga di almeno sei dischi:

```
storage aggregate show-status -aggregate aggregate_name
```

## 2. Convertire l'aggregato da RAID-DP a RAID-TEC:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_tec
```

## 3. Verificare che il criterio RAID aggregato sia RAID-TEC:

```
storage aggregate show aggregate_name
```

### Conversione da RAID-TEC a RAID-DP

Se si riducono le dimensioni del Tier locale (aggregato) e non è più necessaria la tripla parità, è possibile convertire la policy RAID da RAID-TEC a RAID-DP e ridurre il numero di dischi necessari per la parità RAID.

#### Di cosa hai bisogno

La dimensione massima del gruppo RAID per RAID-TEC è superiore alla dimensione massima del gruppo RAID per RAID-DP. Se la dimensione massima del gruppo RAID-TEC non rientra nei limiti RAID-DP, non è possibile eseguire la conversione in RAID-DP.

#### Fasi

### 1. Verificare che l'aggregato sia online e disponga di almeno sei dischi:

```
storage aggregate show-status -aggregate aggregate_name
```

### 2. Convertire l'aggregato da RAID-TEC a RAID-DP:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
```

### 3. Verificare che il criterio RAID aggregato sia RAID-DP:

```
storage aggregate show aggregate_name
```

### Considerazioni per il dimensionamento dei gruppi RAID

La configurazione di una dimensione ottimale del gruppo RAID richiede un compromesso di fattori. È necessario decidere quali fattori: Velocità di ricostruzione RAID, garanzia contro il rischio di perdita di dati dovuta a guasti del disco, ottimizzazione delle performance i/o e massimizzazione dello spazio di storage dei dati, sono i fattori più importanti per l'aggregato (Tier locale) che si sta configurando.

Quando si creano gruppi RAID più grandi, si massimizza lo spazio disponibile per lo storage dei dati per la stessa quantità di storage utilizzata per la parità (nota anche come "parità fiscale"). D'altra parte, quando un disco si guasta in un gruppo RAID più grande, il tempo di ricostruzione aumenta, influenzando le prestazioni per un periodo di tempo più lungo. Inoltre, la presenza di più dischi in un gruppo RAID aumenta la probabilità di guasti a più dischi all'interno dello stesso gruppo RAID.

#### Gruppi RAID HDD o LUN array

Attenersi alle seguenti linee guida per il dimensionamento dei gruppi RAID composti da HDD o LUN di array:

- Tutti i gruppi RAID in un Tier locale (aggregato) devono avere lo stesso numero di dischi.

Anche se è possibile avere fino al 50% in meno o più del numero di dischi in diversi gruppi raid su un unico livello locale, in alcuni casi ciò potrebbe causare colli di bottiglia nelle performance, per cui è meglio evitarlo.

- L'intervallo consigliato di numeri di dischi del gruppo RAID è compreso tra 12 e 20.

L'affidabilità dei dischi dalle performance può supportare un gruppo RAID di dimensioni fino a 28, se necessario.

- Se è possibile soddisfare le prime due linee guida con più numeri di dischi di gruppo RAID, è necessario scegliere il numero maggiore di dischi.

#### **Gruppi RAID SSD nei Tier locali di Flash Pool (aggregati)**

Le dimensioni del gruppo RAID SSD possono essere diverse dalle dimensioni del gruppo RAID per i gruppi RAID HDD in un Tier locale di Flash Pool (aggregato). In genere, è necessario assicurarsi di disporre di un solo gruppo RAID SSD per un livello locale di Flash Pool, per ridurre al minimo il numero di SSD necessari per la parità.

#### **Gruppi RAID SSD in Tier locali SSD (aggregati)**

Attenersi alle seguenti linee guida per il dimensionamento dei gruppi RAID composti da SSD:

- Tutti i gruppi RAID in un Tier locale (aggregato) devono avere un numero di dischi simile.

I gruppi RAID non devono avere esattamente le stesse dimensioni, ma si consiglia di evitare di avere gruppi RAID di dimensioni inferiori alla metà di altri gruppi RAID nello stesso livello locale, se possibile.

- Per RAID-DP, l'intervallo consigliato per le dimensioni del gruppo RAID è compreso tra 20 e 28.

#### **Personalizzare le dimensioni dei gruppi RAID**

È possibile personalizzare le dimensioni dei gruppi RAID per garantire che le dimensioni dei gruppi RAID siano appropriate per la quantità di storage che si intende includere per un Tier locale (aggregato).

##### **A proposito di questa attività**

Per i Tier locali standard (aggregati), è possibile modificare separatamente la dimensione dei gruppi RAID per ciascun Tier locale. Per i Tier locali di Flash Pool, è possibile modificare le dimensioni del gruppo RAID per i gruppi RAID SSD e i gruppi RAID HDD in modo indipendente.

Il seguente elenco descrive alcuni fatti relativi alla modifica delle dimensioni del gruppo RAID:

- Per impostazione predefinita, se il numero di dischi o LUN degli array nel gruppo RAID creato più di recente è inferiore alla dimensione del nuovo gruppo RAID, i dischi o le LUN degli array verranno aggiunti al gruppo RAID creato più di recente fino a raggiungere la nuova dimensione.
- Tutti gli altri gruppi RAID esistenti in tale Tier locale rimangono delle stesse dimensioni, a meno che non si aggiungano esplicitamente dischi.
- Non è mai possibile fare in modo che un gruppo RAID diventi più grande della dimensione massima corrente del gruppo RAID per il Tier locale.
- Non è possibile ridurre le dimensioni dei gruppi RAID già creati.
- La nuova dimensione si applica a tutti i gruppi RAID in quel Tier locale (o, nel caso di un Tier locale di

Flash Pool, a tutti i gruppi RAID per il tipo di gruppo RAID interessato, ovvero SSD o HDD).

## Fasi

1. Utilizzare il comando applicabile:

Se si desidera...	Immettere il seguente comando...
Modificare la dimensione massima del gruppo RAID per i gruppi RAID SSD di un aggregato Flash Pool	<code>storage aggregate modify -aggregate aggr_name -cache-raid-group-size size</code>
Modificare la dimensione massima di qualsiasi altro gruppo RAID	<code>storage aggregate modify -aggregate aggr_name -maxraidsz size</code>

## Esempi

Il seguente comando modifica la dimensione massima del gruppo RAID dell'aggregato n1\_a4 in 20 dischi o LUN di array:

```
storage aggregate modify -aggregate n1_a4 -maxraidsz 20
```

Il seguente comando modifica la dimensione massima del gruppo RAID dei gruppi RAID della cache SSD dell'aggregato di Flash Pool n1\_cache\_a2 in 24:

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

## Gestire i Tier locali di Flash Pool (aggregati)

### Gestire i Tier di Flash Pool (aggregati)

È possibile eseguire varie procedure per gestire i Tier (aggregati) di Flash Pool nel sistema.

- **Criteri di caching**
  - ["Policy di caching del Tier locale \(aggregato\) di Flash Pool"](#)
  - ["Gestire le policy di caching di Flash Pool"](#)
- **Partizione SSD**
  - ["Partizione SSD di Flash Pool per Tier locali \(aggregati\) di Flash Pool utilizzando pool di storage"](#)
- **Candidature e dimensione della cache**
  - ["Determinare la candidatura di Flash Pool e le dimensioni ottimali della cache"](#)
- **Creazione di Flash Pool**
  - ["Creare un Tier locale \(aggregato\) di Flash Pool utilizzando SSD fisici"](#)
  - ["Creare un Tier locale Flash Pool \(aggregato\) utilizzando i pool di storage SSD"](#)

### Policy di caching del Tier locale (aggregato) di Flash Pool

Le policy di caching per i volumi in un Tier locale (aggregato) di Flash Pool consentono di implementare la Flash come cache dalle performance elevate per il set di dati di lavoro,

utilizzando al contempo HDD a basso costo per i dati ad accesso meno frequente. Se si fornisce la cache a due o più Tier locali di Flash Pool, è necessario utilizzare la partizione SSD di Flash Pool per condividere gli SSD tra i Tier locali di Flash Pool.

I criteri di caching vengono applicati ai volumi che risiedono nei Tier locali di Flash Pool. Prima di modificarle, è necessario comprendere il funzionamento delle policy di caching.

Nella maggior parte dei casi, il criterio di caching predefinito “auto” è il miglior criterio di caching da utilizzare. La policy di caching deve essere modificata solo se una policy diversa offre performance migliori per il carico di lavoro. La configurazione di una policy di caching errata può degradare notevolmente le performance dei volumi; il degrado delle performance potrebbe aumentare gradualmente nel tempo.

Le policy di caching combinano una policy di caching in lettura e una policy di caching in scrittura. Il nome del criterio concatena i nomi del criterio di caching in lettura e del criterio di caching in scrittura, separati da un trattino. Se non è presente un trattino nel nome del criterio, il criterio di caching in scrittura è “none”, ad eccezione del criterio “auto”.

Le policy di caching in lettura ottimizzano le performance di lettura future inserendo una copia dei dati nella cache oltre ai dati memorizzati sugli HDD. Per le policy di caching in lettura che inseriscono i dati nella cache per le operazioni di scrittura, la cache funziona come una cache *write-through*.

I dati inseriti nella cache utilizzando il criterio di caching in scrittura esistono solo nella cache; non è presente alcuna copia negli HDD. La cache di Flash Pool è protetta da RAID. L'attivazione del caching in scrittura rende immediatamente disponibili i dati delle operazioni di scrittura per le letture dalla cache, mentre rinviando la scrittura dei dati sugli HDD fino a quando non esaurisce la cache.

Se si sposta un volume da un livello locale di Flash Pool a un livello locale a livello singolo, il criterio di caching viene perso; se successivamente lo si sposta di nuovo su un livello locale di Flash Pool, viene assegnato il criterio di caching predefinito “auto”. Se si sposta un volume tra due livelli locali di Flash Pool, il criterio di caching viene mantenuto.

### **Modificare un criterio di caching**

È possibile utilizzare la CLI per modificare il criterio di caching per un volume che risiede su un livello locale di Flash Pool utilizzando `-caching-policy` con il `volume create` comando.

Quando si crea un volume su un Tier locale di Flash Pool, per impostazione predefinita, al volume viene assegnato il criterio di caching “auto”.

### **Gestire le policy di caching di Flash Pool**

#### **Panoramica sulla gestione delle policy di caching di Flash Pool**

Utilizzando la CLI, è possibile eseguire varie procedure per gestire le policy di caching di Flash Pool nel sistema.

- **Preparazione**

- ["Determinare se modificare la policy di caching dei Tier locali \(aggregati\) di Flash Pool"](#)

- **Modifica delle policy di caching**

- ["Modificare le policy di caching dei Tier locali di Flash Pool \(aggregati\)"](#)
- ["Impostare il criterio di conservazione della cache per i Tier locali \(aggregati\) di Flash Pool"](#)

## Determinare se modificare la policy di caching dei Tier locali (aggregati) di Flash Pool

È possibile assegnare criteri di conservazione della cache ai volumi nei Tier locali (aggregati) di Flash Pool per determinare la durata dei dati del volume nella cache di Flash Pool. Tuttavia, in alcuni casi, la modifica del criterio di conservazione della cache potrebbe non influire sul tempo in cui i dati del volume rimangono nella cache.

### A proposito di questa attività

Se i dati soddisfano una delle seguenti condizioni, la modifica della policy di conservazione della cache potrebbe non avere alcun impatto:

- Il carico di lavoro è sequenziale.
- Il carico di lavoro non rileggerà i blocchi casuali memorizzati nella cache dei dischi a stato solido (SSD).
- La dimensione della cache del volume è troppo piccola.

### Fasi

I seguenti passaggi verificano le condizioni che devono essere soddisfatte dai dati. L'attività deve essere eseguita utilizzando la CLI in modalità avanzata con privilegi.

1. Utilizzare la CLI per visualizzare il volume del carico di lavoro:

```
statistics start -object workload_volume
```

2. Determinare il modello di carico di lavoro del volume:

```
statistics show -object workload_volume -instance volume-workload -counter sequential_reads
```

3. Determinare la percentuale di hit del volume:

```
statistics show -object wafl_hya_vvol -instance volume -counter read_ops_replaced_ppercent|wc_write_blks_overwritten_percent
```

4. Determinare il Cacheable Read e Project Cache Alloc del volume:

```
system node run -node node_name wafl awa start aggr_name
```

5. Visualizzare il riepilogo AWA:

```
system node run -node node_name wafl awa print aggr_name
```

6. Confronta la percentuale di hit del volume con Cacheable Read.

Se la percentuale di hit del volume è maggiore di Cacheable Read, Quindi, il carico di lavoro non rileggerà i blocchi casuali memorizzati nella cache degli SSD.

7. Confrontare le dimensioni correnti della cache del volume con Project Cache Alloc.

Se la dimensione corrente della cache del volume è maggiore di Project Cache Alloc, quindi la dimensione della cache del volume è troppo piccola.



## Modificare le policy di caching dei Tier locali di Flash Pool (aggregati)

È necessario modificare il criterio di caching di un volume solo se si prevede che un diverso criterio di caching fornisca prestazioni migliori. È possibile modificare il criterio di caching di un volume su un Tier locale di Flash Pool (aggregato).

### Di cosa hai bisogno

È necessario determinare se si desidera modificare il criterio di caching.

### A proposito di questa attività

Nella maggior parte dei casi, il criterio di caching predefinito “auto” è il miglior criterio di caching che sia possibile utilizzare. La policy di caching deve essere modificata solo se una policy diversa offre performance migliori per il carico di lavoro. La configurazione di una policy di caching errata può degradare notevolmente le performance dei volumi; il degrado delle performance potrebbe aumentare gradualmente nel tempo. Prestare attenzione quando si modificano i criteri di caching. In caso di problemi di performance con un volume per il quale è stato modificato il criterio di caching, riportare il criterio di caching su “auto”.

### Fase

1. Utilizzare la CLI per modificare il criterio di caching del volume:

```
volume modify -volume volume_name -caching-policy policy_name
```

### Esempio

Nell'esempio riportato di seguito viene modificata la policy di caching di un volume denominato “vol2” nella policy “none”:

```
volume modify -volume vol2 -caching-policy none
```

## Impostare il criterio di conservazione della cache per i Tier locali (aggregati) di Flash Pool

È possibile assegnare criteri di conservazione della cache ai volumi nei Tier locali di Flash Pool (aggregati). I dati nei volumi con una policy di conservazione della cache elevata rimangono nella cache più a lungo e i dati nei volumi con una policy di conservazione della cache bassa vengono rimossi prima. Ciò aumenta le performance dei carichi di lavoro critici rendendo accessibili le informazioni ad alta priorità a una velocità più rapida per un periodo di tempo più lungo.

### Di cosa hai bisogno

È necessario sapere se il sistema presenta condizioni che potrebbero impedire al criterio di conservazione della cache di avere un impatto sulla durata dei dati nella cache.

### Fasi

Utilizzare la CLI in modalità avanzata dei privilegi per eseguire le seguenti operazioni:

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Verificare il criterio di conservazione della cache del volume:

Per impostazione predefinita, il criterio di conservazione della cache è “normal”.

### 3. Impostare il criterio di conservazione della cache:

Versione di ONTAP	Comando
ONTAP 9.0, 9.1	<pre>priority hybrid-cache set volume_name read-cache=read_cache_value write- cache=write_cache_value cache- retention- priority=cache_retention_policy</pre> <p>Impostare <code>cache_retention_policy</code> a <code>high</code> per i dati che si desidera conservare nella cache più a lungo. Impostare <code>cache_retention_policy</code> a <code>low</code> per i dati che si desidera rimuovere prima dalla cache.</p>
ONTAP 9.2 o versione successiva	<pre>volume modify -volume volume_name -vserver vservers_name -caching-policy policy_name.</pre>

4. Verificare che il criterio di conservazione della cache del volume sia stato modificato nell'opzione selezionata.

5. Restituire l'impostazione dei privilegi ad `admin`:

```
set -privilege admin
```

### Partizione SSD di Flash Pool per Tier locali (aggregati) di Flash Pool utilizzando pool di storage

Se si fornisce la cache a due o più Tier locali di Flash Pool (aggregati), è necessario utilizzare la partizione SSD (Solid state Drive) di Flash Pool. Il partizionamento degli SSD Flash Pool consente di condividere gli SSD con tutti i Tier locali che utilizzano Flash Pool. In questo modo, il costo di parità viene diffuso su più Tier locali, la flessibilità di allocazione della cache SSD aumenta e le performance SSD massimizzano.

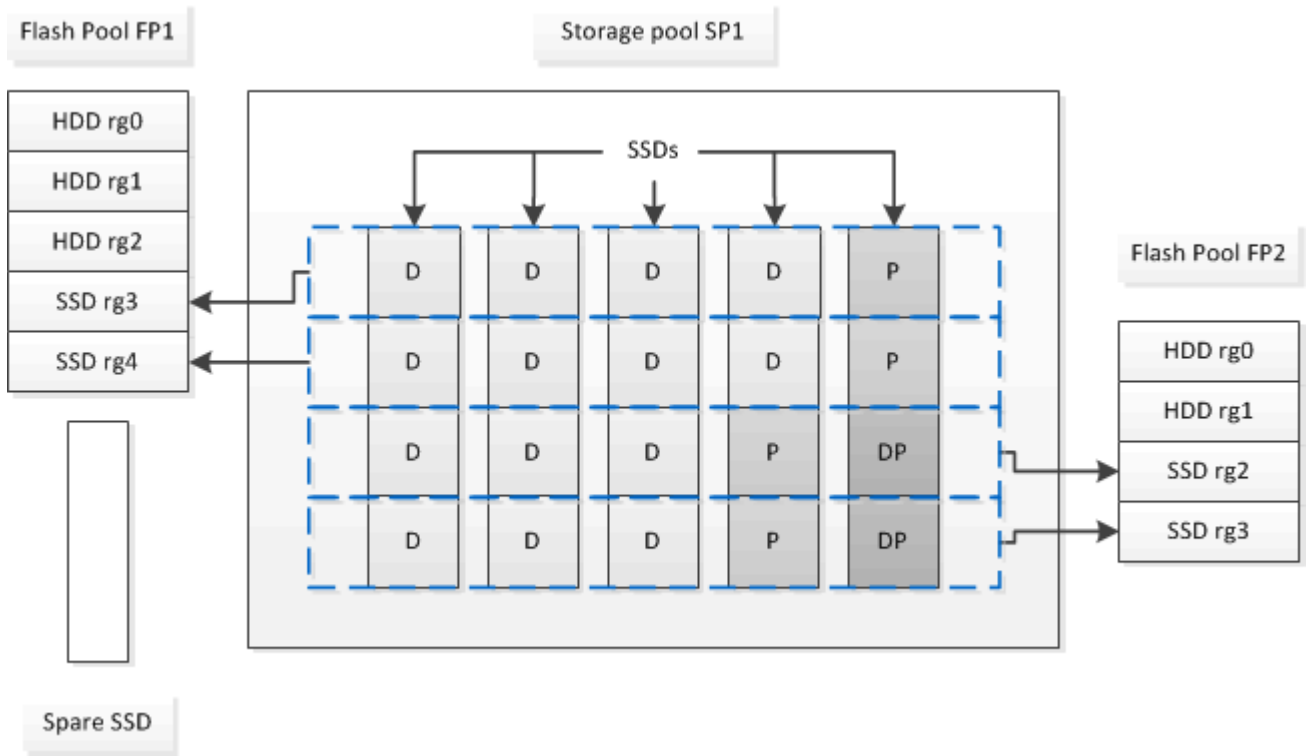
Affinché un SSD possa essere utilizzato in un Tier locale di Flash Pool, l'SSD deve essere collocato in un pool di storage. Non è possibile utilizzare SSD partizionati per la partizione dei dati root in un pool di storage. Una volta inserito l'SSD nel pool di storage, l'SSD non può più essere gestito come disco standalone e non può essere rimosso dal pool di storage a meno che non si distruggano i Tier locali associati a Flash Pool e si distrugga il pool di storage.

I pool di storage SSD sono suddivisi in quattro unità di allocazione uguali. Gli SSD aggiunti al pool di storage sono suddivisi in quattro partizioni e una partizione viene assegnata a ciascuna delle quattro unità di allocazione. Gli SSD nel pool di storage devono essere di proprietà della stessa coppia ha. Per impostazione predefinita, a ciascun nodo della coppia ha vengono assegnate due unità di allocazione. Le unità di allocazione devono essere di proprietà del nodo proprietario del Tier locale che sta servendo. Se per i Tier locali su uno dei nodi è necessaria una maggiore cache Flash, è possibile spostare il numero predefinito di unità di allocazione per diminuire il numero su un nodo e aumentare il numero sul nodo partner.

Si utilizzano SSD di riserva per aggiungerli a un pool di storage SSD. Se il pool di storage fornisce unità di allocazione ai Tier locali di Flash Pool di proprietà di entrambi i nodi della coppia ha, allora gli SSD spare

possono essere di proprietà di entrambi i nodi. Tuttavia, se il pool di storage fornisce unità di allocazione solo ai Tier locali di Flash Pool di proprietà di uno dei nodi della coppia ha, le unità di riserva SSD devono essere di proprietà dello stesso nodo.

La figura seguente mostra un esempio di partizione SSD Flash Pool. Il pool di storage SSD fornisce cache a due livelli locali di Flash Pool:



Lo Storage Pool SP1 è composto da cinque SSD e un SSD hot spare. Due delle unità di allocazione del pool di storage vengono allocate a Flash Pool FP1 e due a Flash Pool FP2. FP1 ha un tipo RAID cache di RAID4. Pertanto, le unità di allocazione fornite a FP1 contengono una sola partizione designata per la parità. FP2 ha un tipo di RAID-DP per la cache. Pertanto, le unità di allocazione fornite a FP2 includono una partizione di parità e una partizione di doppia parità.

In questo esempio, due unità di allocazione vengono allocate a ciascun Tier locale di Flash Pool. Tuttavia, se un livello locale di Flash Pool richiedeva una cache più grande, è possibile allocare tre unità di allocazione a quel livello locale di Flash Pool e una sola all'altra.

### Determinare la candidatura di Flash Pool e le dimensioni ottimali della cache

Prima di convertire un Tier locale (aggregato) esistente in un Tier locale di Flash Pool, è possibile determinare se il Tier locale è associato all'i/o e le migliori dimensioni della cache di Flash Pool per il carico di lavoro e il budget. È inoltre possibile controllare se la cache di un Tier locale di Flash Pool esistente è dimensionata correttamente.

### Di cosa hai bisogno

Dovresti sapere approssimativamente quando il Tier locale che stai analizzando sperimenta il suo carico di picco.

### Fasi

1. Accedere alla modalità avanzata:

```
set advanced
```

2. Se è necessario determinare se un Tier locale (aggregato) esistente sia un buon candidato per la conversione in un aggregato di Flash Pool, determinare la disponibilità dei dischi nell'aggregato durante un periodo di carico di picco e in che modo ciò influisce sulla latenza:

```
statistics show-periodic -object disk:raid_group -instance raid_group_name  
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

Puoi decidere se ridurre la latenza aggiungendo la cache di Flash Pool è utile per questo aggregato.

Il comando seguente mostra le statistiche per il primo gruppo RAID dell'aggregato "aggr1":

```
statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0  
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

3. Avviare Automated workload Analyzer (AWA):

```
storage automated-working-set-analyzer start -node node_name -aggregate  
aggr_name
```

AWA inizia a raccogliere i dati del carico di lavoro per i volumi associati all'aggregato specificato.

4. Uscire dalla modalità avanzata:

```
set admin
```

Consentire l'esecuzione di AWA fino a quando non si sono verificati uno o più intervalli di carico di picco. AWA raccoglie le statistiche dei carichi di lavoro per i volumi associati all'aggregato specificato e analizza i dati per una durata massima di una settimana. L'esecuzione di AWA per più di una settimana riporta solo i dati raccolti dalla settimana più recente. Le stime delle dimensioni della cache si basano sui carichi più elevati rilevati durante il periodo di raccolta dei dati; non è necessario che il carico sia elevato per l'intero periodo di raccolta dei dati.

5. Accedere alla modalità avanzata:

```
set advanced
```

6. Visualizzare l'analisi del carico di lavoro:

```
storage automated-working-set-analyzer show -node node_name -instance
```

7. Arrestare AWA:

```
storage automated-working-set-analyzer stop node_name
```

Tutti i dati dei workload vengono eliminati e non sono più disponibili per l'analisi.

8. Uscire dalla modalità avanzata:

```
set admin
```

## **Creare un Tier locale (aggregato) di Flash Pool utilizzando SSD fisici**

È possibile creare un Tier locale (aggregato) di Flash Pool abilitando la funzionalità su un Tier locale esistente composto da gruppi RAID HDD e aggiungendo uno o più gruppi RAID SSD a tale Tier locale. Ciò comporta due set di gruppi RAID per quel livello locale: Gruppi RAID SSD (la cache SSD) e gruppi RAID HDD.

### **A proposito di questa attività**

Dopo aver aggiunto una cache SSD a un Tier locale per creare un Tier locale di Flash Pool, non è possibile rimuovere la cache SSD per convertire di nuovo il Tier locale nella configurazione originale.

Per impostazione predefinita, il livello RAID della cache SSD è lo stesso del livello RAID dei gruppi RAID HDD. È possibile ignorare questa selezione predefinita specificando l'opzione "raidtype" quando si aggiungono i primi gruppi RAID SSD.

### **Prima di iniziare**

- È necessario aver identificato un Tier locale valido composto da HDD per la conversione in un Tier locale di Flash Pool.
- È necessario aver determinato l'idoneità del caching in scrittura dei volumi associati al Tier locale e aver completato tutte le procedure necessarie per risolvere i problemi di idoneità.
- È necessario aver determinato gli SSD da aggiungere e questi SSD devono essere di proprietà del nodo su cui si sta creando il Tier locale di Flash Pool.
- È necessario aver determinato i tipi di checksum sia degli SSD che si stanno aggiungendo che degli HDD già nel Tier locale.
- È necessario determinare il numero di SSD da aggiungere e la dimensione ottimale del gruppo RAID per i gruppi RAID SSD.

L'utilizzo di un numero inferiore di gruppi RAID nella cache SSD riduce il numero di dischi di parità richiesti, ma i gruppi RAID più grandi richiedono RAID-DP.

- È necessario determinare il livello RAID che si desidera utilizzare per la cache SSD.
- È necessario determinare le dimensioni massime della cache per il sistema e determinare che l'aggiunta della cache SSD al Tier locale non causerà il superamento di tale dimensione.
- È necessario aver acquisito dimestichezza con i requisiti di configurazione per i Tier locali di Flash Pool.



### **Fasi**

Puoi creare un aggregato di FlashPool utilizzando System Manager o l'interfaccia a riga di comando di ONTAP.

## System Manager

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione sistema per creare un Tier locale di Flash Pool utilizzando SSD fisici.

### Fasi

1. Selezionare **Storage > Tiers**, quindi selezionare un livello di archiviazione HDD locale esistente.
2. Selezionare  Quindi **Aggiungi Flash Pool cache**.
3. Selezionare **Usa SSD dedicati come cache**.
4. Selezionare un tipo di disco e il numero di dischi.
5. Scegliere un tipo di RAID.
6. Selezionare **Salva**.
7. Individuare il Tier di storage e selezionare .
8. Selezionare **altri dettagli**. Verificare che Flash Pool sia **abilitato**.

### CLI

#### Fasi

1. Contrassegna il Tier locale (aggregato) come idoneo per diventare un aggregato di Flash Pool:

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

Se questo passaggio non riesce, determinare l'idoneità del caching in scrittura per l'aggregato di destinazione.

2. Aggiungere gli SSD all'aggregato utilizzando `storage aggregate add` comando.
  - È possibile specificare gli SSD in base all'ID o utilizzando `diskcount` e `disktype` parametri.
  - Se gli HDD e gli SSD non hanno lo stesso tipo di checksum o se l'aggregato è un aggregato di checksum misto, è necessario utilizzare `checksumstyle` parametro per specificare il tipo di checksum dei dischi da aggiungere all'aggregato.
  - È possibile specificare un tipo RAID diverso per la cache SSD utilizzando `raidtype` parametro.
  - Se si desidera che la dimensione del gruppo RAID della cache sia diversa da quella predefinita per il tipo RAID in uso, è necessario modificarla ora utilizzando `-cache-raid-group-size` parametro.

## Creare un Tier locale Flash Pool (aggregato) utilizzando i pool di storage SSD

### Panoramica sulla creazione di un Tier locale (aggregato) di Flash Pool utilizzando i pool di storage SSD

È possibile eseguire varie procedure per creare un Tier locale (aggregato) di Flash Pool utilizzando i pool di storage SSD:

- **Preparazione**

- ["Determinare se un Tier locale \(aggregato\) di Flash Pool utilizza un pool di storage SSD"](#)

- **Creazione del pool di storage SSD**

- ["Creare un pool di storage SSD"](#)

- "Aggiungi SSD a un pool di storage SSD"
- **Creazione di Flash Pool con pool di storage SSD**
  - "Creare un Tier locale Flash Pool (aggregato) utilizzando le unità di allocazione del pool di storage SSD"
  - "Determinare l'impatto delle dimensioni della cache dell'aggiunta di SSD a un pool di storage SSD"

**Determinare se un Tier locale (aggregato) di Flash Pool utilizza un pool di storage SSD**

È possibile configurare un aggregato Flash Pool (Tier locale) aggiungendo una o più unità di allocazione da un pool di storage SSD a un Tier locale HDD esistente.

I Tier locali di Flash Pool vengono gestiti in modo diverso quando utilizzano pool di storage SSD per fornire la cache rispetto a quando utilizzano SSD discreti.

#### **Fase**

1. Visualizzare i dischi dell'aggregato in base al gruppo RAID:

```
storage aggregate show-status aggr_name
```

Se l'aggregato utilizza uno o più pool di storage SSD, il valore per `Position` La colonna per i gruppi RAID SSD viene visualizzata come ``Shared`` E il nome del pool di storage viene visualizzato accanto al nome del gruppo RAID.

**Aggiungere cache a un Tier locale (aggregato) creando un pool di storage SSD**

È possibile eseguire il provisioning della cache convertendo un Tier locale (aggregato) esistente in un Tier locale (aggregato) Flash Pool aggiungendo unità a stato solido (SSD).

È possibile creare pool di storage con unità a stato solido (SSD) per fornire cache SSD per due o quattro Tier locali di Flash Pool (aggregati). Gli aggregati di Flash Pool consentono di implementare la flash come cache dalle performance elevate per il set di dati di lavoro, utilizzando al contempo HDD a basso costo per i dati ad accesso meno frequente.

#### **A proposito di questa attività**

- Quando si creano o si aggiungono dischi a un pool di storage, è necessario fornire un elenco di dischi.
- I pool di storage non supportano un `diskcount` parametro.
- Gli SSD utilizzati nel pool di storage devono avere le stesse dimensioni.

## System Manager

### Utilizzare Gestione sistema per aggiungere una cache SSD (ONTAP 9.12.1 e versioni successive)

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione sistema per aggiungere una cache SSD.



Le opzioni del pool di storage non sono disponibili sui sistemi AFF.

#### Fasi

1. Fare clic su **Cluster > Disks**, quindi su **Show/Hide** (Mostra/Nascondi).
2. Selezionare **Type** (tipo) e verificare che sul cluster siano presenti SSD di riserva.
3. Fare clic su **Storage > Tier** e fare clic su **Add Storage Pool**.
4. Selezionare il tipo di disco.
5. Inserire una dimensione del disco.
6. Selezionare il numero di dischi da aggiungere al pool di storage.
7. Esaminare le dimensioni stimate della cache.

### Utilizzare Gestione sistema per aggiungere una cache SSD (solo ONTAP 9.7)



Utilizzare la procedura CLI se si utilizza una versione di ONTAP successiva a ONTAP 9.7 o precedente a ONTAP 9.12.1.

#### Fasi

1. Fare clic su **(Torna alla versione classica)**.
2. Fare clic su **Storage > Aggregates & Disks > Aggregates**.
3. Selezionare il Tier locale (aggregato), quindi fare clic su **Actions > Add cache** (azioni > Aggiungi cache).
4. Selezionare l'origine della cache come "pool di storage" o "SSD dedicati".
5. Fare clic su **(passa alla nuova esperienza)**.
6. Fare clic su **Storage > Tier** per verificare le dimensioni del nuovo aggregato.

## CLI

### Utilizzare la CLI per creare un pool di storage SSD

#### Fasi

1. Determinare i nomi degli SSD spare disponibili:

```
storage aggregate show-spare-disks -disk-type SSD
```

Gli SSD utilizzati in un pool di storage possono essere di proprietà di entrambi i nodi di una coppia ha.

2. Creare il pool di storage:

```
storage pool create -storage-pool sp_name -disk-list disk1,disk2,...
```



### 3. **Opzionale:** verificare il pool di storage appena creato:

```
storage pool show -storage-pool sp_name
```

#### **Risultati**

Una volta inseriti nel pool di storage, gli SSD non vengono più visualizzati come parti di ricambio nel cluster, anche se lo storage fornito dal pool di storage non è ancora stato allocato alle cache di Flash Pool. Non è possibile aggiungere SSD a un gruppo RAID come dischi discreti; il relativo storage può essere fornito solo utilizzando le unità di allocazione del pool di storage a cui appartengono.

#### **Creare un Tier locale Flash Pool (aggregato) utilizzando le unità di allocazione del pool di storage SSD**

È possibile configurare un Tier locale (aggregato) di Flash Pool aggiungendo una o più unità di allocazione da un pool di storage SSD a un Tier locale HDD esistente.

A partire da ONTAP 9.12.1, è possibile utilizzare il nuovo Gestore di sistema per creare un Tier locale di Flash Pool utilizzando le unità di allocazione del pool di storage.

#### **Di cosa hai bisogno**

- È necessario aver identificato un Tier locale valido composto da HDD per la conversione in un Tier locale di Flash Pool.
- È necessario aver determinato l'idoneità del caching in scrittura dei volumi associati al Tier locale e aver completato tutte le procedure necessarie per risolvere i problemi di idoneità.
- È necessario aver creato un pool di storage SSD per fornire la cache SSD a questo Tier locale di Flash Pool.

Tutte le unità di allocazione del pool di storage che si desidera utilizzare devono essere di proprietà dello stesso nodo proprietario del Tier locale di Flash Pool.

- È necessario determinare la quantità di cache che si desidera aggiungere al Tier locale.

La cache viene aggiunta al Tier locale in base alle unità di allocazione. È possibile aumentare le dimensioni delle unità di allocazione in un secondo momento aggiungendo SSD al pool di storage se c'è spazio.

- È necessario determinare il tipo di RAID che si desidera utilizzare per la cache SSD.

Dopo aver aggiunto una cache al Tier locale dai pool di storage SSD, non è possibile modificare il tipo RAID dei gruppi RAID della cache.

- È necessario determinare le dimensioni massime della cache per il sistema e determinare che l'aggiunta della cache SSD al Tier locale non causerà il superamento di tale dimensione.

È possibile visualizzare la quantità di cache che verrà aggiunta alle dimensioni totali della cache utilizzando `storage pool show` comando.

- È necessario aver acquisito dimestichezza con i requisiti di configurazione del Tier locale di Flash Pool.

#### **A proposito di questa attività**



Se si desidera che il tipo RAID della cache sia diverso da quello dei gruppi RAID HDD, è necessario specificare il tipo di cache RAID quando si aggiunge la capacità SSD. Dopo aver aggiunto la capacità SSD al Tier locale, non è più possibile modificare il tipo RAID della cache.

Dopo aver aggiunto una cache SSD a un Tier locale per creare un Tier locale di Flash Pool, non è possibile rimuovere la cache SSD per convertire di nuovo il Tier locale nella configurazione originale.

## System Manager

A partire da ONTAP 9.12.1, puoi utilizzare Gestione sistema per aggiungere SSD a un pool di storage SSD.

### Fasi

1. Fare clic su **Storage > Tier** e selezionare un Tier di storage HDD locale esistente.
2. Fare clic su  E selezionare **Add Flash Pool cache**.
3. Selezionare **Usa pool di storage**.
4. Selezionare un pool di storage.
5. Selezionare una dimensione della cache e una configurazione RAID.
6. Fare clic su **Save** (Salva).
7. Individuare nuovamente il Tier di storage e fare clic su .
8. Selezionare **More Details** (ulteriori dettagli) e verificare che Flash Pool sia visualizzato come **Enabled** (attivato).

### CLI

#### Fasi

1. Contrassegna l'aggregato come idoneo per diventare un aggregato di Flash Pool:

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

Se questo passaggio non riesce, determinare l'idoneità del caching in scrittura per l'aggregato di destinazione.

2. Mostrare le unità di allocazione del pool di storage SSD disponibili:

```
storage pool show-available-capacity
```

3. Aggiungere la capacità SSD all'aggregato:

```
storage aggregate add aggr_name -storage-pool sp_name -allocation-units  
number_of_units
```

Se si desidera che il tipo RAID della cache sia diverso da quello dei gruppi RAID HDD, è necessario modificarlo quando si inserisce questo comando utilizzando `raidtype` parametro.

Non è necessario specificare un nuovo gruppo RAID; ONTAP inserisce automaticamente la cache SSD in gruppi RAID separati dai gruppi RAID HDD.

Non è possibile impostare la dimensione del gruppo RAID della cache, in quanto è determinata dal numero di SSD nel pool di storage.

La cache viene aggiunta all'aggregato e l'aggregato è ora un aggregato di Flash Pool. Ogni unità di allocazione aggiunta all'aggregato diventa il proprio gruppo RAID.

4. Verificare la presenza e le dimensioni della cache SSD:

```
storage aggregate show aggregate_name
```

Le dimensioni della cache sono elencate in Total Hybrid Cache Size.

## Informazioni correlate

["Report tecnico di NetApp 4070: Guida alla progettazione e all'implementazione di Flash Pool"](#)

### Determinare l'impatto delle dimensioni della cache dell'aggiunta di SSD a un pool di storage SSD

Se l'aggiunta di SSD a un pool di storage causa il superamento del limite di cache del modello di piattaforma, ONTAP non assegna la capacità aggiunta di recente a alcun Tier locale di Flash Pool (aggregati). In questo modo, alcune o tutte le nuove capacità aggiunte potrebbero non essere disponibili per l'utilizzo.

#### A proposito di questa attività

Quando si aggiungono SSD a un pool di storage SSD con unità di allocazione già allocate ai Tier locali (aggregati) di Flash Pool, si aumentano le dimensioni della cache di ciascuno di questi Tier locali e la cache totale sul sistema. Se nessuna delle unità di allocazione del pool di storage è stata allocata, l'aggiunta di SSD a tale pool di storage non influisce sulle dimensioni della cache SSD fino a quando una o più unità di allocazione non vengono allocate in una cache.

#### Fasi

1. Determinare le dimensioni utilizzabili degli SSD che si stanno aggiungendo al pool di storage:

```
storage disk show disk_name -fields usable-size
```

2. Determinare quante unità di allocazione rimangono non allocate per il pool di storage:

```
storage pool show-available-capacity sp_name
```

Vengono visualizzate tutte le unità di allocazione non allocate nel pool di storage.

3. Calcolare la quantità di cache che verrà aggiunta applicando la seguente formula:

$(4 - \text{numero di unità di allocazione non allocate}) \times 25\% \times \text{dimensione utilizzabile} \times \text{numero di SSD}$

### Aggiungi SSD a un pool di storage SSD

Quando si aggiungono dischi a stato solido (SSD) a un pool di storage SSD, si aumentano le dimensioni fisiche e utilizzabili del pool di storage e le dimensioni dell'unità di allocazione. La dimensione dell'unità di allocazione maggiore influisce anche sulle unità di allocazione che sono già state allocate ai Tier locali (aggregati).

#### Di cosa hai bisogno

È necessario determinare che questa operazione non causerà il superamento del limite di cache per la coppia ha. ONTAP non impedisce di superare il limite di cache quando si aggiungono SSD a un pool di storage SSD, rendendo la capacità di storage aggiunta di recente non disponibile per l'utilizzo.

#### A proposito di questa attività


Quando si aggiungono SSD a un pool di storage SSD esistente, gli SSD devono essere di proprietà di un nodo o dell'altro della stessa coppia ha che possedeva già gli SSD esistenti nel pool di storage. È possibile aggiungere SSD di proprietà di entrambi i nodi della coppia ha.

L'SSD aggiunto al pool di storage deve avere le stesse dimensioni del disco attualmente utilizzato nel pool di storage.

**System Manager**

A partire da ONTAP 9.12.1, puoi utilizzare Gestione sistema per aggiungere SSD a un pool di storage SSD.

**Fasi**

- 1. Fare clic su **Storage > Tier** e individuare la sezione **Storage Pools**.
- 2. Individuare il pool di storage, fare clic su  e selezionare **Aggiungi dischi**.
- 3. Scegliere il tipo di disco e selezionare il numero di dischi.
- 4. Esaminare la dimensione stimata della cache.

**CLI**

**Fasi**

- 1. **Opzionale:** Visualizza le dimensioni correnti dell'unità di allocazione e lo storage disponibile per il pool di storage:

```
storage pool show -instance sp_name
```

- 2. Trova gli SSD disponibili:

```
storage disk show -container-type spare -type SSD
```

- 3. Aggiungere gli SSD al pool di storage:

```
storage pool add -storage-pool sp_name -disk-list disk1,disk2...
```

Il sistema visualizza le dimensioni degli aggregati di Flash Pool aumentate in base a questa operazione e alla quantità di dati e richiede di confermare l'operazione.

**Comandi per la gestione dei pool di storage SSD**

ONTAP offre `storage pool` Comando per la gestione dei pool di storage SSD.

Se si desidera...	Utilizzare questo comando...
Visualizzare la quantità di storage che un pool di storage fornisce a quali aggregati	<code>storage pool show-aggregate</code>
Visualizza la quantità di cache che verrà aggiunta alla capacità cache complessiva per entrambi i tipi RAID (dimensione dei dati dell'unità di allocazione)	<code>storage pool show -instance</code>
Visualizzare i dischi in un pool di storage	<code>storage pool show-disks</code>

Visualizzare le unità di allocazione non allocate per un pool di storage	<code>storage pool show-available-capacity</code>
Modificare la proprietà di una o più unità di allocazione di un pool di storage da un partner ha all'altro	<code>storage pool reassign</code>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

## Gestione dei livelli FabricPool

### Panoramica sulla gestione dei Tier FabricPool

È possibile utilizzare FabricPool per tierare automaticamente i dati in base alla frequenza di accesso.

FabricPool è una soluzione di storage ibrido che utilizza un aggregato all flash (all SSD) come Tier di performance e un archivio di oggetti come Tier di cloud. L'utilizzo di un FabricPool consente di ridurre i costi dello storage senza compromettere le performance, l'efficienza o la protezione.

Il livello cloud può essere localizzato su NetApp StorageGRID o ONTAP S3 (a partire da ONTAP 9.8) o su uno dei seguenti service provider:

- Cloud di Alibaba
- Amazon S3
- Amazon Commercial Cloud Services
- Google Cloud
- Cloud IBM
- Storage Blob Microsoft Azure



A partire da ONTAP 9,7, è possibile utilizzare altri provider di archivi di oggetti che supportano API S3 generiche selezionando il provider di archivi di oggetti S3\_Compatible.

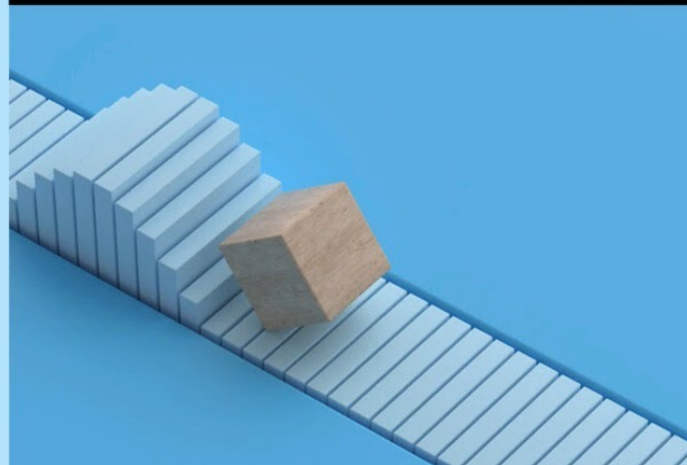
### Video sul caso di utilizzo di dati Tier e costi inferiori

# ONTAP FabricPool

Tier Data and Lower Costs

## Use Case

© 2020 NetApp, Inc. All rights reserved.



### Informazioni correlate

Vedere anche la ["Tiering cloud di NetApp"](#) documentazione.

### Vantaggi dei Tier di storage grazie a FabricPool

La configurazione di un aggregato per l'utilizzo di FabricPool consente di utilizzare i Tier di storage. Puoi bilanciare in modo efficiente le performance e i costi del tuo sistema storage, monitorare e ottimizzare l'utilizzo dello spazio ed eseguire lo spostamento dei dati basato su policy tra i Tier di storage.

- È possibile ottimizzare le performance dello storage e ridurre i costi dello storage memorizzando i dati in un Tier in base alla frequenza di accesso ai dati.

- I dati ad accesso frequente ("hot") vengono memorizzati nel *Tier di performance*.

Il Tier di performance utilizza uno storage primario dalle performance elevate, come un aggregato all flash (all SSD) del sistema storage.

- I dati ad accesso non frequente ("cold") vengono memorizzati nel *Tier cloud*, noto anche come *Tier di capacità*.

Il Tier cloud utilizza un archivio di oggetti meno costoso e che non richiede performance elevate.

- Hai la flessibilità di specificare il Tier in cui archiviare i dati.

È possibile specificare una delle opzioni dei criteri di tiering supportate a livello di volume. Le opzioni consentono di spostare in modo efficiente i dati tra i vari Tier man mano che i dati diventano caldi o freddi.

["Tipi di policy di tiering FabricPool"](#)

- Puoi scegliere uno degli archivi di oggetti supportati da utilizzare come Tier cloud per FabricPool.
- È possibile monitorare l'utilizzo dello spazio in un aggregato abilitato a FabricPool.
- È possibile visualizzare la quantità di dati inattivi in un volume utilizzando il reporting dei dati inattivi.
- È possibile ridurre l'impatto on-premise del sistema storage.

È possibile risparmiare spazio fisico quando si utilizza un archivio di oggetti basato sul cloud per il Tier cloud.

## Considerazioni e requisiti per l'utilizzo di FabricPool

È necessario acquisire familiarità con alcune considerazioni e requisiti relativi all'utilizzo di FabricPool.

### Considerazioni e requisiti generali

- Per utilizzare FabricPool, è necessario che ONTAP 9.2 sia in esecuzione almeno.
- È necessario eseguire ONTAP 9.4 o versioni successive per le seguenti funzionalità di FabricPool:
  - Il auto ["policy di tiering"](#)
  - Specifica del periodo di raffreddamento minimo di tiering
  - Report dei dati inattivi (IDR)
  - Utilizzo dello storage blob Microsoft Azure per il cloud come Tier cloud per FabricPool
  - Utilizzo di FabricPool con ONTAP Select
- È necessario eseguire ONTAP 9.5 o versioni successive per le seguenti funzionalità di FabricPool:
  - Specifica della soglia di tiering fullness
  - Utilizzo dello storage a oggetti cloud IBM come Tier cloud per FabricPool
  - NetApp Volume Encryption (NVE) del livello cloud, attivato per impostazione predefinita.
- È necessario eseguire ONTAP 9.6 o versioni successive per le seguenti funzionalità di FabricPool:
  - Il all policy di tiering
  - Report dei dati inattivi attivati manualmente sugli aggregati HDD
  - Report dei dati inattivi attivati automaticamente per gli aggregati SSD quando si esegue l'aggiornamento a ONTAP 9.6 e al momento della creazione dell'aggregato, ad eccezione dei sistemi di fascia bassa con meno di 4 CPU, meno di 6 GB di RAM o quando la dimensione della cache del buffer WAFL è inferiore a 3 GB.

ONTAP monitora il carico del sistema e, se il carico rimane elevato per 4 minuti continui, l'IDR viene disattivato e non viene attivato automaticamente. È possibile riabilitare l'IDR manualmente, tuttavia l'IDR abilitato manualmente non viene disattivato automaticamente.

  - Utilizzo dello storage a oggetti cloud di Alibaba come livello cloud per FabricPool
  - Utilizzo della piattaforma cloud di Google come Tier cloud per FabricPool
  - Spostamento del volume senza copia dei dati del Tier cloud
- È necessario eseguire ONTAP 9.7 o versioni successive per le seguenti funzionalità di FabricPool:
  - Proxy HTTP e HTTPS non trasparente per fornire l'accesso solo ai punti di accesso whitelist e per



fornire funzionalità di auditing e reporting.

- Mirroring FabricPool per il tiering dei dati cold in due archivi di oggetti contemporaneamente
- Mirroring di FabricPool sulle configurazioni MetroCluster
- Dump e ripristino NDMP attivati per impostazione predefinita negli aggregati FabricPool Attached.



Se l'applicazione di backup utilizza un protocollo diverso da NDMP, come NFS o SMB, tutti i dati di cui viene eseguito il backup nel Tier di performance diventano hot e possono influire sul tiering di tali dati nel Tier cloud. Le letture non NDMP possono causare la migrazione dei dati dal livello cloud al livello di performance.

#### "Supporto backup e ripristino NDMP per FabricPool"

- È necessario eseguire ONTAP 9.8 o versione successiva per le seguenti funzionalità di FabricPool:
  - Controllo della migrazione nel cloud per consentire l'override della policy di tiering predefinita
  - Promozione dei dati al Tier di performance
  - FabricPool con SnapLock Enterprise. FabricPool con SnapLock Enterprise richiede una richiesta di variazione del prodotto (FPVR). Per creare un FPVR, contatta il tuo team di vendita.
  - Periodo minimo di raffreddamento massimo di 183 giorni
  - Tagging degli oggetti mediante tag personalizzati creati dall'utente
  - FabricPools su piattaforme HDD e aggregati

I dischi HDD FabricPool sono supportati con dischi SAS, FSAS, BSAS e MSATA solo su sistemi con 6 o più core CPU, inclusi i seguenti modelli:

- FAS9000
- FAS8700
- FAS8300
- FAS8200
- FAS8080
- FAS8060
- FAS8040
- FAS2750
- FAS2720
- FAS2650
- FAS2620

Controllare ["Hardware Universe"](#) per i modelli più recenti supportati.

- FabricPool è supportato su tutte le piattaforme in grado di eseguire ONTAP 9.2, ad eccezione di:
  - FAS8020
  - FAS2554
  - FAS2552
  - FAS2520

- FabricPool supporta i seguenti tipi di aggregato:
  - Sui sistemi AFF, è possibile utilizzare solo tutti gli aggregati flash (tutti gli SSD) per FabricPool.
  - Sui sistemi FAS, è possibile utilizzare aggregati all-flash (all-SSD) o HDD per FabricPool.

Non è possibile utilizzare gli aggregati di Flash Pool, che contengono sia SSD che HDD.

- Su Cloud Volumes ONTAP e ONTAP Select, è possibile utilizzare aggregati SSD o HDD per FabricPool.

Tuttavia, si consiglia di utilizzare aggregati SSD.

- FabricPool supporta l'utilizzo dei seguenti archivi di oggetti come livello cloud:
  - NetApp StorageGRID 10.3 o versione successiva
  - NetApp ONTAP S3 (ONTAP 9.8 e versioni successive)
  - Alibaba Cloud Object Storage
  - Amazon Web Services Simple Storage Service (AWS S3)
  - Storage Google Cloud
  - Storage a oggetti IBM Cloud
  - Microsoft Azure Blob Storage per il cloud
- L'archivio di oggetti "bucket" (container) che intendi utilizzare deve essere già stato configurato, avere almeno 10 GB di spazio di storage e non deve essere rinominato.
- Le coppie HA che utilizzano FabricPool richiedono le LIF intercluster per comunicare con l'archivio di oggetti.
- Non è possibile scollegare un Tier cloud da un Tier locale dopo il collegamento; tuttavia, è possibile utilizzarlo ["Specchio FabricPool"](#) per collegare un tier locale a un tier cloud diverso.
- Se si utilizza il throughput floors (QoS min), la policy di tiering sui volumi deve essere impostata su `none` Prima che l'aggregato possa essere collegato a FabricPool.

Altri criteri di tiering impediscono l'associazione dell'aggregato a FabricPool. Una policy di QoS non applicherà i piani di throughput quando FabricPool è attivato.

- Seguire le linee guida delle Best practice per l'utilizzo di FabricPool in scenari specifici.

["Report tecnico di NetApp 4598: Best Practice FabricPool in ONTAP 9"](#)

## Considerazioni aggiuntive sull'utilizzo di Cloud Volumes ONTAP

Cloud Volumes ONTAP non richiede una licenza FabricPool, indipendentemente dal provider dell'archivio di oggetti in uso.

## Considerazioni aggiuntive per il tiering dei dati a cui accedono i protocolli SAN

Quando si esegue il tiering dei dati a cui accedono i protocolli SAN, NetApp consiglia di utilizzare cloud privati, come StorageGRID, a causa di considerazioni sulla connettività.

## Importante

Quando si utilizza FabricPool in un ambiente SAN con un host Windows, se lo storage a oggetti non è più disponibile per un periodo di tempo prolungato durante il tiering dei dati nel cloud, i file sul LUN NetApp

sull'host Windows potrebbero diventare inaccessibili o scomparire. Consultare l'articolo della Knowledge base ["Durante l'archiviazione di oggetti FabricPool S3 non disponibile, l'host SAN di Windows ha segnalato un danneggiamento del file system"](#).

## Funzionalità o funzionalità non supportate da FabricPool

- Archivi di oggetti con WORM abilitato e versione degli oggetti abilitata.
- Policy ILM (Information Lifecycle Management) applicate ai bucket degli archivi di oggetti

FabricPool supporta le policy di gestione del ciclo di vita delle informazioni di StorageGRID solo per la replica dei dati e l'erasure coding per proteggere i dati del Tier cloud dai guasti. Tuttavia, FabricPool *non* supporta le regole ILM avanzate, come il filtraggio basato su tag o metadati dell'utente. ILM include in genere varie policy di spostamento ed eliminazione. Queste policy possono interrompere i dati nel livello cloud di FabricPool. L'utilizzo di FabricPool con policy ILM configurate sugli archivi di oggetti può causare la perdita di dati.

- Transizione dei dati in 7 modalità utilizzando i comandi CLI di ONTAP o lo strumento di transizione in 7 modalità
- Virtualizzazione FlexArray
- RAID SyncMirror, tranne in una configurazione MetroCluster
- Volumi SnapLock quando si utilizza ONTAP 9.7 e versioni precedenti
- Backup su nastro con SMTape per aggregati abilitati FabricPool
- La funzionalità di bilanciamento automatico
- Volumi che utilizzano una garanzia di spazio diversa da `none`

Ad eccezione dei volumi SVM root e dei volumi di staging dell'audit CIFS, FabricPool non supporta l'associazione di un Tier cloud a un aggregato che contiene volumi che utilizzano una garanzia di spazio diversa da `none`. Ad esempio, un volume che utilizza una garanzia di spazio di `volume (-space -guarantee volume)` non è supportato.

- Cluster con ["Licenza DP\\_Optimized"](#)
- Aggregati di Flash Pool

## Informazioni sulle policy di tiering FabricPool

Le policy di tiering di FabricPool ti consentono di spostare i dati in modo efficiente tra i vari livelli quando i dati diventano caldi o freddi. La comprensione delle policy di tiering ti aiuta a scegliere la policy più adatta alle tue esigenze di gestione dello storage.

### Tipi di policy di tiering FabricPool

Le policy di tiering FabricPool determinano quando o se i blocchi di dati utente di un volume in FabricPool vengono spostati nel Tier cloud, in base al volume "temperature" di hot (attivo) o cold (inattivo). Il volume "temperature" aumenta quando si accede frequentemente e diminuisce quando non lo è. Alcune policy di tiering prevedono un periodo di raffreddamento minimo di tiering, che imposta il tempo in cui i dati utente in un volume di FabricPool devono rimanere inattivi affinché i dati vengano considerati "cold" e spostati al livello cloud.

Dopo che un blocco è stato identificato come cold, viene contrassegnato come idoneo per essere tiered. Una scansione giornaliera di tiering in background cerca i blocchi freddi. Una volta raccolti un numero sufficiente di

blocchi da 4 KB dallo stesso volume, questi vengono concatenati in un oggetto da 4 MB e spostati nel Tier cloud in base alla policy di tiering del volume.



Dati nei volumi utilizzando `all` la policy di tiering viene immediatamente contrassegnata come cold e inizia il tiering al livello cloud il prima possibile. Non è necessario attendere l'esecuzione della scansione di tiering giornaliera.

È possibile utilizzare `volume object-store tiering show` Per visualizzare lo stato di tiering di un volume FabricPool. Per ulteriori informazioni, consultare ["Riferimento comando"](#).

Il criterio di tiering FabricPool viene specificato a livello di volume. Sono disponibili quattro opzioni:

- Il `snapshot-only` La policy di tiering (impostazione predefinita) sposta i blocchi di dati utente delle copie Snapshot del volume non associate al file system attivo nel Tier cloud.

Il periodo di raffreddamento minimo per il tiering è di 2 giorni. È possibile modificare l'impostazione predefinita per il periodo di raffreddamento minimo di tiering con `-tiering-minimum-cooling-days` nel livello di privilegio avanzato di `volume create` e `volume modify` comandi. I valori validi vanno da 2 a 183 giorni utilizzando ONTAP 9.8 e versioni successive. Se si utilizza una versione di ONTAP precedente alla 9.8, i valori validi sono compresi tra 2 e 63 giorni.

- Il `auto` La policy di tiering, supportata solo su ONTAP 9.4 e versioni successive, sposta i blocchi di dati utente cold nelle copie Snapshot e nel file system attivo nel Tier cloud.

Il periodo di raffreddamento minimo di tiering predefinito è di 31 giorni e si applica all'intero volume, sia per il file system attivo che per le copie Snapshot.

È possibile modificare l'impostazione predefinita per il periodo di raffreddamento minimo di tiering con `-tiering-minimum-cooling-days` nel livello di privilegio avanzato di `volume create` e `volume modify` comandi. I valori validi vanno da 2 a 183 giorni.

- Il `all` La policy di tiering, supportata solo con ONTAP 9.6 e versioni successive, sposta tutti i blocchi di dati utente nel file system attivo e nelle copie Snapshot nel Tier cloud. Sostituisce il `backup` policy di tiering.

Il `all` i criteri di tiering dei volumi non devono essere utilizzati su volumi di lettura/scrittura con traffico client normale.

Il periodo di raffreddamento minimo del tiering non si applica perché i dati si spostano al livello cloud non appena viene eseguita la scansione del tiering e non è possibile modificare l'impostazione.

- Il `none` la policy di tiering mantiene i dati di un volume nel tier di performance e non passa al tier cloud.

Impostazione del criterio di tiering su `none` impedisce il nuovo tiering. I dati del volume precedentemente spostati nel Tier cloud rimangono nel Tier cloud fino a quando non diventano hot e vengono automaticamente spostati di nuovo nel Tier locale.

Il periodo di raffreddamento minimo del tiering non si applica perché i dati non si spostano mai al livello cloud e non è possibile modificare l'impostazione.

Quando si blocca a freddo in un volume con una policy di tiering impostata su `none` vengono letti, vengono resi a caldo e scritti nel tier locale.

Il `volume show` l'output del comando mostra la policy di tiering di un volume. Un volume che non è mai stato

utilizzato con FabricPool mostra `none` policy di tiering nell'output.

## Cosa accade quando si modifica il criterio di tiering di un volume in FabricPool

È possibile modificare la policy di tiering di un volume eseguendo una `volume modify` operazione. Devi comprendere come la modifica della policy di tiering possa influire sul tempo necessario per far diventare i dati più freddi e spostarli nel Tier cloud.

- Modifica della policy di tiering da `snapshot-only` oppure `none` a `auto`. Fa sì che ONTAP invii blocchi di dati utente nel file system attivo che sono già cold al livello cloud, anche se tali blocchi di dati utente non erano precedentemente idonei per il livello cloud.
- Modifica della policy di tiering in `all`. Da un'altra policy deriva che ONTAP sposta al più presto nel cloud tutti i blocchi utente nel file system attivo e nelle copie Snapshot. Prima di ONTAP 9,8, i blocchi necessitavano di attendere l'esecuzione della scansione di tiering successiva.

Non è consentito spostare nuovamente i blocchi nel Tier di performance.

- Modifica della policy di tiering da `auto` a `snapshot-only` oppure `none` non fa sì che i blocchi di file system attivi già spostati nel tier cloud vengano spostati di nuovo nel tier di performance.

Le letture dei volumi sono necessarie per riportare i dati al Tier di performance.

- Ogni volta che si modifica il criterio di tiering su un volume, il periodo minimo di raffreddamento del tiering viene ripristinato al valore predefinito per il criterio.

## Cosa accade alla policy di tiering quando si sposta un volume

- A meno che non si specifichi esplicitamente un criterio di tiering diverso, un volume conserva la propria policy di tiering originale quando viene spostato all'interno e all'esterno di un aggregato abilitato a FabricPool.

Tuttavia, la policy di tiering ha effetto solo quando il volume si trova in un aggregato abilitato a FabricPool.

- Il valore esistente di `-tiering-minimum-cooling-days` parametro per lo spostamento di un volume con il volume a meno che non si specifichi un criterio di tiering diverso per la destinazione.

Se si specifica un criterio di tiering diverso, il volume utilizza il periodo di raffreddamento minimo di tiering predefinito per tale criterio. Questo è il caso se la destinazione è FabricPool o meno.

- È possibile spostare un volume tra gli aggregati e contemporaneamente modificare la policy di tiering.
- Prestare particolare attenzione quando un `volume move` operazione comprende `auto` policy di tiering.

Supponendo che sia l'origine che la destinazione siano aggregati abilitati per FabricPool, la seguente tabella riassume il risultato di a. `volume move` operazione che comporta modifiche dei criteri correlate a. `auto`:

Quando si sposta un volume con una policy di tiering di...	Inoltre, è possibile modificare la policy di tiering passando a...	Quindi, dopo lo spostamento del volume...
<code>all</code>	<code>auto</code>	Tutti i dati vengono spostati nel Tier di performance.

snapshot-only, none, o. auto	auto	I blocchi di dati vengono spostati nello stesso livello della destinazione in cui si trovavano in precedenza nell'origine.
auto oppure all	snapshot-only	Tutti i dati vengono spostati nel Tier di performance.
auto	all	Tutti i dati degli utenti vengono spostati nel livello cloud.
snapshot-only, auto oppure all	none	Tutti i dati vengono conservati al livello di performance.

### Cosa accade alla policy di tiering quando si clonano volumi

- A partire da ONTAP 9.8, un volume clone eredita sempre sia la policy di tiering che la policy di recupero del cloud dal volume padre.

Nelle release precedenti a ONTAP 9.8, un clone eredita la policy di tiering dall'origine, tranne quando l'origine dispone di all policy di tiering.

- Se il volume padre dispone di never cloud retrieval policy, il suo volume clone deve disporre di never policy di recupero del cloud o di all policy di tiering e policy di recupero del cloud corrispondenti default.
- Impossibile modificare la policy di recupero cloud del volume padre in never a meno che tutti i volumi cloni non dispongano di una policy di recupero cloud never.

Quando si clonano i volumi, tenere presenti le seguenti Best practice:

- Il -tiering-policy opzione e. tiering-minimum-cooling-days l'opzione del clone controlla solo il comportamento di tiering dei blocchi unici per il clone. Pertanto, si consiglia di utilizzare le impostazioni di tiering sul FlexVol padre che spostano la stessa quantità di dati o spostano una quantità inferiore di dati rispetto a uno qualsiasi dei cloni
- La policy di recupero del cloud sul FlexVol padre deve spostare la stessa quantità di dati o spostare più dati rispetto alla policy di recupero di uno qualsiasi dei cloni

### Come funzionano le policy di tiering con la migrazione del cloud

Il recupero dei dati nel cloud di FabricPool è controllato da policy di tiering che determinano il recupero dei dati dal Tier cloud al Tier di performance in base al modello di lettura. I modelli di lettura possono essere sequenziali o casuali.

La tabella seguente elenca le policy di tiering e le regole di recupero dei dati cloud per ogni policy.

Policy di tiering	Comportamento di recupero
nessuno	Lecture sequenziali e casuali

solo snapshot	Lecture sequenziali e casuali
automatico	Lecture casuali
tutto	Nessun recupero dei dati

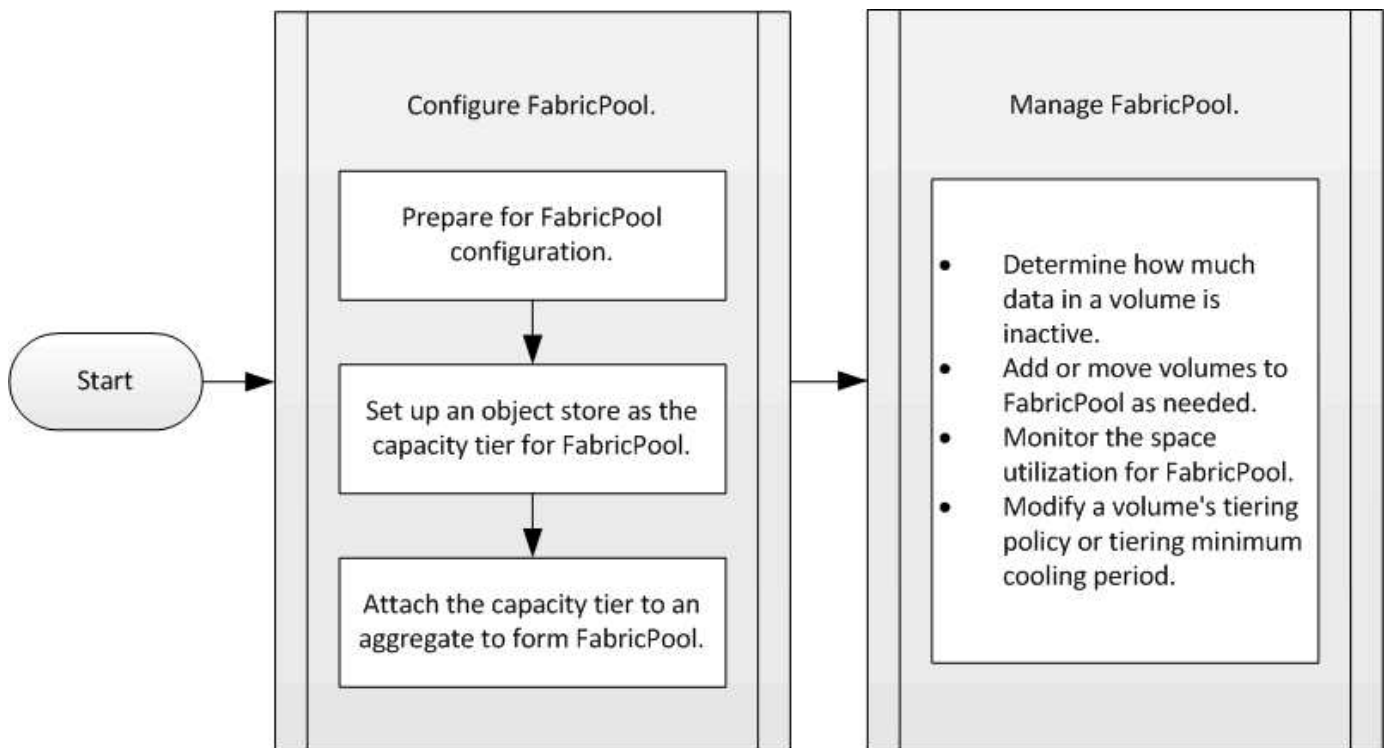
A partire da ONTAP 9.8, il controllo della migrazione nel cloud `cloud-retrieval-policy` l'opzione sovrascrive il comportamento predefinito di migrazione o recupero del cloud controllato dalla policy di tiering.

La seguente tabella elenca le policy di recupero cloud supportate e il loro comportamento di recupero.

Policy di recupero del cloud	Comportamento di recupero
predefinito	La policy di tiering decide quali dati devono essere ritirati, quindi non vi è alcuna modifica al recupero dei dati nel cloud con "default," <code>cloud-retrieval-policy</code> . Questo criterio è il valore predefinito per qualsiasi volume, indipendentemente dal tipo di aggregato ospitato.
a lettura	Tutti i dati letti dal client vengono estratti dal Tier cloud al Tier di performance.
mai	Nessun dato client-driven viene estratto dal Tier cloud al Tier di performance
promuovi	<ul style="list-style-type: none"> <li>• Per la policy di tiering "none", tutti i dati cloud vengono estratti dal Tier cloud al Tier di performance</li> <li>• Per la policy di tiering "snapshot-only," vengono estratti i dati AFS.</li> </ul>

## Workflow di gestione di FabricPool

È possibile utilizzare il diagramma del flusso di lavoro di FabricPool per pianificare le attività di configurazione e gestione.



## Configurare FabricPool

### Preparazione per la configurazione FabricPool

#### Preparazione per la panoramica della configurazione di FabricPool

La configurazione di FabricPool consente di gestire i dati del Tier di storage (il Tier di performance locale o il Tier cloud) da memorizzare in base all'accesso frequente ai dati.

La preparazione richiesta per la configurazione FabricPool dipende dall'archivio di oggetti utilizzato come livello cloud.

#### Aggiungi una connessione al cloud

A partire da ONTAP 9.9.0, è possibile utilizzare Gestione sistema per aggiungere una connessione al cloud.

Per iniziare, utilizza NetApp Cloud Insights per configurare un collector. Durante il processo di configurazione, si copia un codice di accoppiamento generato da Cloud Insights, quindi si accede a un cluster utilizzando Gestione sistema. In questo caso, è possibile aggiungere una connessione cloud utilizzando il codice di accoppiamento. Il resto del processo viene completato in Cloud Insights.



Se si sceglie l'opzione per utilizzare un server proxy quando si aggiunge una connessione da Cloud Volumes ONTAP al servizio Cloud Insights, è necessario assicurarsi che l'URL sia <https://example.com> è accessibile dal server proxy. Quando viene visualizzato il messaggio "la configurazione del proxy HTTP non è valida" <https://example.com> non è accessibile.

#### Fasi

1. In Cloud Insights, durante il processo di configurazione di un collector, copiare il codice di accoppiamento generato.



2. Utilizzando Gestione sistema con ONTAP 9.9.0 o versione successiva, accedere al cluster.
3. Selezionare **Cluster > Settings** (Cluster > Impostazioni).
4. Nella sezione connessioni cloud, selezionare **Aggiungi** per aggiungere una connessione.
5. Inserire un nome per la connessione e incollare il codice di accoppiamento nell'apposito spazio.
6. Selezionare **Aggiungi**.
7. Tornare a Cloud Insights per completare la configurazione del collector.

Per ulteriori informazioni su Cloud Insights, fare riferimento a. ["Documentazione Cloud Insights"](#).

#### Installare una licenza FabricPool

La licenza FabricPool utilizzata in passato sta cambiando e viene conservata solo per le configurazioni non supportate da BlueXP. A partire dal 21 agosto 2021, la licenza BYOL di Cloud Tiering è stata introdotta per le configurazioni di tiering che sono supportate in BlueXP utilizzando il servizio Cloud Tiering.

["Scopri di più sulla nuova licenza BYOL Cloud Tiering"](#).

Le configurazioni supportate da BlueXP devono utilizzare la pagina del portafoglio digitale in BlueXP per il tiering delle licenze per i cluster ONTAP. Ciò richiede la configurazione di un account BlueXP e la configurazione del tiering per il provider di storage a oggetti che si intende utilizzare. Attualmente BlueXP supporta il tiering per i seguenti storage a oggetti: Amazon S3, Azure Blob, Google Cloud Storage, S3-compatibile e StorageGRID.

["Scopri di più sul servizio di tiering cloud"](#).

È possibile scaricare e attivare una licenza FabricPool utilizzando Gestione sistema se si dispone di una delle configurazioni non supportate da BlueXP:

- Installazioni ONTAP in siti oscuri
- Cluster ONTAP che eseguono il tiering dei dati per lo storage a oggetti cloud IBM o Alibaba

La licenza FabricPool è una licenza a livello di cluster. Include un limite di utilizzo autorizzato acquistato per lo storage a oggetti associato a FabricPool nel cluster. L'utilizzo nel cluster non deve superare la capacità del limite di utilizzo autorizzato. Per aumentare il limite di utilizzo della licenza, contattare il rappresentante commerciale.



Le licenze FabricPool sono disponibili in formati perpetui o a termine, di 1 o 3 anni.

Una licenza FabricPool basata su termini con 10 TB di capacità libera è disponibile per i primi ordini FabricPool per le configurazioni di cluster esistenti non supportate in BlueXP. La capacità libera non è disponibile con licenze perpetue. Non è richiesta una licenza se si utilizza NetApp StorageGRID o ONTAP S3 per il livello cloud. Cloud Volumes ONTAP non richiede una licenza FabricPool, indipendentemente dal provider in uso.

Questa attività è supportata solo caricando il file di licenza nel cluster utilizzando System Manager.

#### Fasi

1. Scaricare il file di licenza NetApp (NLF) per la licenza FabricPool dal ["Sito di supporto NetApp"](#).
2. Eseguire le seguenti operazioni utilizzando Gestione di sistema per caricare la licenza FabricPool nel cluster:

- a. Nel riquadro **Cluster > Settings** (Cluster > Impostazioni), nella scheda **Licenses** (licenze), fare clic su .
- b. Nella pagina **License**, fare clic su  **Add**.
- c. Nella finestra di dialogo **Aggiungi licenza**, fare clic su **Sfoglia** per selezionare l'NLF scaricato, quindi fare clic su **Aggiungi** per caricare il file nel cluster.

#### Informazioni correlate

["Panoramica sulle licenze ONTAP FabricPool \(FP\)"](#)

["Ricerca licenze software NetApp"](#)

["TechComm TV di NetApp: Elenco di riproduzione FabricPool"](#)

#### Installare un certificato CA se si utilizza StorageGRID

A meno che non si preveda di disattivare il controllo dei certificati per StorageGRID, è necessario installare un certificato CA StorageGRID sul cluster in modo che ONTAP possa autenticare con StorageGRID come archivio di oggetti per FabricPool.

#### A proposito di questa attività

ONTAP 9.4 e versioni successive consentono di disattivare il controllo dei certificati per StorageGRID.

#### Fasi

1. Contattare l'amministratore di StorageGRID per ottenere il certificato CA del sistema StorageGRID.
2. Utilizzare `security certificate install` con il `-type server-ca` Parametro per installare il certificato CA StorageGRID sul cluster.

Il nome di dominio completo (FQDN) immesso deve corrispondere al nome comune personalizzato sul certificato CA di StorageGRID.

#### Aggiornare un certificato scaduto

Per aggiornare un certificato scaduto, è consigliabile utilizzare una CA attendibile per generare il nuovo certificato del server. Inoltre, è necessario assicurarsi che il certificato venga aggiornato contemporaneamente sul server StorageGRID e sul cluster ONTAP per ridurre al minimo i tempi di inattività.

#### Informazioni correlate

["Risorse StorageGRID"](#)

#### Installare un certificato CA se si utilizza ONTAP S3

A meno che non si preveda di disattivare il controllo dei certificati per ONTAP S3, è necessario installare un certificato CA ONTAP S3 sul cluster in modo che ONTAP possa autenticare con ONTAP S3 come archivio di oggetti per FabricPool.

#### Fasi

1. Ottenere il certificato CA del sistema ONTAP S3.
2. Utilizzare `security certificate install` con il `-type server-ca` Parametro per installare il certificato CA ONTAP S3 sul cluster.

Il nome di dominio completo (FQDN) immesso deve corrispondere al nome comune personalizzato sul certificato CA di ONTAP S3.

## Aggiornare un certificato scaduto

Per aggiornare un certificato scaduto, è consigliabile utilizzare una CA attendibile per generare il nuovo certificato del server. Inoltre, è necessario assicurarsi che il certificato venga aggiornato contemporaneamente sul server ONTAP S3 e sul cluster ONTAP per ridurre al minimo i tempi di inattività.

## Informazioni correlate

["Configurazione S3"](#)

## Impostare un archivio di oggetti come livello cloud per FabricPool

### Imposta un archivio di oggetti come livello cloud per la panoramica di FabricPool

La configurazione di FabricPool implica la specifica delle informazioni di configurazione dell'archivio di oggetti (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, Amazon S3, Google Cloud Storage, IBM Cloud Object Storage o Microsoft Azure Blob Storage per il cloud) che si intende utilizzare come livello cloud per FabricPool.

## Configura StorageGRID come Tier cloud

Se utilizzi ONTAP 9.2 o versioni successive, puoi impostare StorageGRID come livello cloud per FabricPool. Quando si esegue il tiering dei dati a cui accedono i protocolli SAN, NetApp consiglia di utilizzare cloud privati, come StorageGRID, a causa di considerazioni sulla connettività.

## Considerazioni sull'utilizzo di StorageGRID con FabricPool

- È necessario installare un certificato CA per StorageGRID, a meno che non si disabiliti esplicitamente il controllo dei certificati.
- Non è necessario attivare la versione degli oggetti StorageGRID nel bucket dell'archivio di oggetti.
- Non è richiesta una licenza FabricPool.
- Se un nodo StorageGRID viene implementato in una macchina virtuale con storage assegnato da un sistema NetApp AFF, verificare che il volume non abbia una policy di tiering FabricPool attivata.

La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.



Non utilizzare mai FabricPool per eseguire il tiering dei dati relativi a StorageGRID su StorageGRID. Il tiering dei dati StorageGRID su StorageGRID aumenta la risoluzione dei problemi e la complessità operativa.

## A proposito di questa attività

Il bilanciamento del carico è abilitato per StorageGRID in ONTAP 9.8 e versioni successive. Quando il nome host del server viene risolto in più indirizzi IP, ONTAP stabilisce connessioni client con tutti gli indirizzi IP restituiti (fino a un massimo di 16 indirizzi IP). Gli indirizzi IP vengono raccolti con un metodo round-robin quando vengono stabilite le connessioni.

## Procedure

Puoi impostare StorageGRID come livello cloud per FabricPool con Gestione di sistema ONTAP o l'interfaccia utente di ONTAP.

### System Manager

1. Fare clic su **Storage > Tier > Add Cloud Tier** e selezionare StorageGRID come provider dell'archivio di oggetti.
2. Completare le informazioni richieste.
3. Se si desidera creare un mirror cloud, fare clic su **Aggiungi come mirror FabricPool**.

Un mirror FabricPool offre un metodo per sostituire perfettamente un archivio di dati e garantisce che i dati siano disponibili in caso di disastro.

### CLI

1. Specificare le informazioni di configurazione StorageGRID utilizzando `storage aggregate object-store config create` con il `-provider-type SGWS` parametro.
  - Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere a StorageGRID con le informazioni fornite.
  - Si utilizza `-access-key` Parametro per specificare la chiave di accesso per autorizzare le richieste all'archivio di oggetti StorageGRID.
  - Si utilizza `-secret-password` Parametro per specificare la password (chiave di accesso segreta) per l'autenticazione delle richieste all'archivio di oggetti StorageGRID.
  - Se la password StorageGRID viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

In questo modo, ONTAP può accedere ai dati in StorageGRID senza interruzioni.

- Impostazione di `-is-certificate-validation-enabled` parametro a. `false` Disattiva il controllo dei certificati per StorageGRID.

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. Visualizzare e verificare le informazioni di configurazione StorageGRID utilizzando `storage aggregate object-store config show` comando.

Il `storage aggregate object-store config modify` Il comando consente di modificare le informazioni di configurazione StorageGRID per FabricPool.

## Imposta ONTAP S3 come Tier cloud

Se utilizzi ONTAP 9.8 o versioni successive, puoi impostare ONTAP S3 come livello cloud per FabricPool.

**Di cosa hai bisogno**

È necessario disporre del nome del server ONTAP S3 e dell'indirizzo IP dei relativi LIF associati sul cluster remoto.

Sul cluster locale devono essere presenti LIF intercluster.

**"Creazione di LIF intercluster per tiering FabricPool remoto"****A proposito di questa attività**

Il bilanciamento del carico è abilitato per i server ONTAP S3 in ONTAP 9.8 e versioni successive. Quando il nome host del server viene risolto in più indirizzi IP, ONTAP stabilisce connessioni client con tutti gli indirizzi IP restituiti (fino a un massimo di 16 indirizzi IP). Gli indirizzi IP vengono raccolti con un metodo round-robin quando vengono stabilite le connessioni.

**Procedure**

Puoi impostare ONTAP S3 come livello cloud per FabricPool con Gestione di sistema ONTAP o l'interfaccia utente di ONTAP.

## System Manager

1. Fare clic su **Storage > Tier > Add Cloud Tier** e selezionare ONTAP S3 come provider dell'archivio di oggetti.
2. Completare le informazioni richieste.
3. Se si desidera creare un mirror cloud, fare clic su **Aggiungi come mirror FabricPool**.

Un mirror FabricPool offre un metodo per sostituire perfettamente un archivio di dati e garantisce che i dati siano disponibili in caso di disastro.

## CLI

1. Aggiungere voci per il server S3 e i LIF al server DNS.

Opzione	Descrizione
<b>Se si utilizza un server DNS esterno</b>	Assegnare il nome del server S3 e gli indirizzi IP all'amministratore del server DNS.
<b>Se si utilizza la tabella degli host DNS del sistema locale</b>	Immettere il seguente comando:  <pre>dns host create -vserver svm_name -address ip_address -hostname s3_server_name</pre>

2. Specificare le informazioni di configurazione di ONTAP S3 utilizzando `storage aggregate object-store config create` con il `-provider-type ONTAP_S3` parametro.
  - Il `storage aggregate object-store config create` Il comando non riesce se il sistema ONTAP locale non riesce ad accedere al server ONTAP S3 con le informazioni fornite.
  - Si utilizza `-access-key` Parametro per specificare la chiave di accesso per l'autorizzazione delle richieste al server ONTAP S3.
  - Si utilizza `-secret-password` Parametro per specificare la password (chiave di accesso segreta) per l'autenticazione delle richieste al server ONTAP S3.
  - Se la password del server ONTAP S3 viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata nel sistema ONTAP locale.

In questo modo è possibile accedere ai dati nell'archivio di oggetti di ONTAP S3 senza interruzioni.

- Impostazione di `-is-certificate-validation-enabled` parametro a. `false` Disattiva il controllo dei certificati per ONTAP S3.

```
cluster1::> storage aggregate object-store config create  
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server  
-container-name myS3container -access-key myS3key  
-secret-password myS3pass
```

3. Visualizzare e verificare le informazioni di configurazione di ONTAP\_S3 utilizzando `storage`

aggregate object-store config show comando.

Il storage aggregate object-store config modify consente di modificare ONTAP\_S3 Informazioni di configurazione per FabricPool.

## Impostare Alibaba Cloud Object Storage come livello cloud

Se utilizzi ONTAP 9.6 o versioni successive, puoi impostare Alibaba Cloud Object Storage come livello cloud per FabricPool.

### Considerazioni sull'utilizzo dello storage a oggetti cloud di Alibaba con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.

I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool. Se ti serve capacità aggiuntiva su un sistema AFF, se utilizzi Alibaba Cloud Object Storage su un sistema non AFF, o se esegui l'upgrade da un cluster esistente, ti serve un ["Licenza FabricPool"](#).

- Nei sistemi AFF e FAS e in ONTAP Select, FabricPool supporta le seguenti classi di servizi di storage a oggetti Alibaba:
  - Alibaba Object Storage Service Standard
  - Alibaba Object Storage Service - accesso non frequente

["Alibaba Cloud: Introduzione alle classi di storage"](#)

Per informazioni sulle classi di storage non elencate, contattare il rappresentante commerciale NetApp.

### Fasi

1. Specificare le informazioni di configurazione di Alibaba Cloud Object Storage utilizzando storage aggregate object-store config create con il -provider-type AliCloud parametro.

- Il storage aggregate object-store config create Il comando non riesce se ONTAP non riesce ad accedere all'archivio di oggetti cloud Alibaba con le informazioni fornite.
- Si utilizza -access-key Parametro per specificare la chiave di accesso per autorizzare le richieste all'archivio di oggetti di Alibaba Cloud Object Storage.
- Se la password di Alibaba Cloud Object Storage viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

In questo modo, ONTAP può accedere ai dati nello storage a oggetti cloud di Alibaba senza interruzioni.

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Visualizzare e verificare le informazioni di configurazione di Alibaba Cloud Object Storage utilizzando storage aggregate object-store config show comando.

Il storage aggregate object-store config modify Il comando consente di modificare le

## Imposta Amazon S3 come Tier cloud

Se utilizzi ONTAP 9.2 o versioni successive, puoi impostare Amazon S3 come livello cloud per FabricPool. Se utilizzi ONTAP 9.5 o versioni successive, puoi configurare i servizi cloud commerciali Amazon (C2S) per FabricPool.

### Considerazioni sull'utilizzo di Amazon S3 con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.
    - I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool.
- Se ti serve capacità aggiuntiva in un sistema AFF, se utilizzi Amazon S3 su un sistema non AFF o se esegui l'upgrade da un cluster esistente, ti serve un ["Licenza FabricPool"](#).

Se si ordina FabricPool per la prima volta per un cluster esistente, è disponibile una licenza FabricPool con 10 TB di capacità libera.

- Si consiglia di utilizzare la LIF utilizzata da ONTAP per la connessione al server a oggetti Amazon S3 su una porta a 10 Gbps.
- Nei sistemi AFF e FAS e in ONTAP Select, FabricPool supporta le seguenti classi di storage Amazon S3:
  - Standard Amazon S3
  - Amazon S3 Standard - accesso non frequente (Standard - IA)
  - Amazon S3 One zone - accesso non frequente (una zona - IA)
  - Amazon S3 Intelligent-Tiering
  - Amazon Commercial Cloud Services
  - A partire da ONTAP 9.11.1, recupero immediato del ghiacciaio Amazon S3 (FabricPool non supporta il recupero flessibile del ghiacciaio o l'archiviazione profonda del ghiacciaio)

["Documentazione Amazon Web Services: Classi di storage Amazon S3"](#)

Per informazioni sulle classi di storage non elencate, contattare il rappresentante commerciale.

- Su Cloud Volumes ONTAP, FabricPool supporta il tiering da SSD General Purpose (gp2) e volumi HDD ottimizzati per il throughput (st1) di Amazon Elastic Block Store (EBS).

### Fasi

1. Specificare le informazioni di configurazione di Amazon S3 utilizzando `storage aggregate object-store config create` con il `-provider-type AWS_S3` parametro.
  - Si utilizza `-auth-type CAP` Parametro per ottenere le credenziali per l'accesso a C2S.

Quando si utilizza `-auth-type CAP` è necessario utilizzare il `-cap-url` Parametro per specificare l'URL completo per richiedere credenziali temporanee per l'accesso a C2S.

  - Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere ad Amazon S3 con le informazioni fornite.
  - Si utilizza `-access-key` Parametro per specificare la chiave di accesso per autorizzare le richieste



all'archivio di oggetti Amazon S3.

- Si utilizza `-secret-password` Parametro per specificare la password (chiave di accesso segreta) per l'autenticazione delle richieste all'archivio di oggetti Amazon S3.
- Se la password Amazon S3 viene modificata, devi aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

In questo modo, ONTAP può accedere ai dati in Amazon S3 senza interruzioni.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. Visualizzare e verificare le informazioni di configurazione di Amazon S3 utilizzando `storage aggregate object-store config show` comando.

Il `storage aggregate object-store config modify` Comando consente di modificare le informazioni di configurazione di Amazon S3 per FabricPool.

## Configura Google Cloud Storage come Tier cloud

Se utilizzi ONTAP 9.6 o versioni successive, puoi impostare Google Cloud Storage come livello cloud per FabricPool.

### Considerazioni aggiuntive sull'utilizzo dello storage cloud Google con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.

I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool. Se ti serve capacità aggiuntiva in un sistema AFF, se utilizzi Google Cloud Storage su un sistema non AFF, o se esegui l'upgrade da un cluster esistente, ti serve un [xref:./fabricpool/"Licenza FabricPool"](#).

- Si consiglia di utilizzare la LIF utilizzata da ONTAP per connettersi al server a oggetti di storage su Google Cloud su una porta a 10 Gbps.
- Sui sistemi AFF e FAS e su ONTAP Select, FabricPool supporta le seguenti classi di storage a oggetti di Google Cloud:
  - Google Cloud Multi-Regional
  - Google Cloud Regional
  - Google Cloud Nearline

- Google Cloud Coldline

### "Google Cloud: Classi di storage"

#### Fasi

1. Specificare le informazioni di configurazione di Google Cloud Storage utilizzando `storage aggregate object-store config create` con il `-provider-type GoogleCloud` parametro.
  - Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere a Google Cloud Storage con le informazioni fornite.
  - Si utilizza `-access-key` Parametro per specificare la chiave di accesso per autorizzare le richieste all'archivio di oggetti di Google Cloud Storage.
  - Se la password di Google Cloud Storage viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

In questo modo, ONTAP può accedere ai dati in Google Cloud Storage senza interruzioni.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. Visualizzare e verificare le informazioni di configurazione di Google Cloud Storage utilizzando `storage aggregate object-store config show` comando.

Il `storage aggregate object-store config modify` Il comando consente di modificare le informazioni di configurazione di Google Cloud Storage per FabricPool.

#### Configurare IBM Cloud Object Storage come Tier cloud

Se si utilizza ONTAP 9.5 o versione successiva, è possibile impostare lo storage a oggetti cloud IBM come livello cloud per FabricPool.

#### Considerazioni sull'utilizzo dello storage a oggetti cloud IBM con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.

I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool. Se ti serve capacità aggiuntiva su un sistema AFF, se utilizzi IBM Cloud Object Storage su un sistema non AFF o se esegui l'upgrade da un cluster esistente, ti serve un ["Licenza FabricPool"](#).

Se si ordina FabricPool per la prima volta per un cluster esistente, è disponibile una licenza FabricPool con 10 TB di capacità libera.

- Si consiglia di utilizzare la LIF utilizzata da ONTAP per la connessione al server a oggetti cloud IBM su una porta a 10 Gbps.

#### Fasi

1. Specificare le informazioni di configurazione di IBM Cloud Object Storage utilizzando `storage aggregate object-store config create` con il `-provider-type IBM_COS` parametro.

- Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere all'archivio di oggetti cloud IBM con le informazioni fornite.
- Si utilizza `-access-key` Parametro per specificare la chiave di accesso per autorizzare le richieste all'archivio di oggetti di IBM Cloud Object Storage.
- Si utilizza `-secret-password` Parametro per specificare la password (chiave di accesso segreta) per l'autenticazione delle richieste all'archivio di oggetti di IBM Cloud Object Storage.
- Se la password di IBM Cloud Object Storage viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

In questo modo, ONTAP può accedere ai dati nello storage a oggetti cloud IBM senza interruzioni.

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Visualizzare e verificare le informazioni di configurazione di IBM Cloud Object Storage utilizzando `storage aggregate object-store config show` comando.

Il `storage aggregate object-store config modify` Il comando consente di modificare le informazioni di configurazione di IBM Cloud Object Storage per FabricPool.

## Configura Azure Blob Storage per il cloud come Tier cloud

Se utilizzi ONTAP 9.4 o versioni successive, puoi configurare Azure Blob Storage per il cloud come Tier cloud per FabricPool.

### Considerazioni sull'utilizzo dello storage Blob di Microsoft Azure con FabricPool

- Potrebbe essere necessaria una licenza FabricPool.

I nuovi sistemi AFF ordinati sono dotati di 10 TB di capacità libera per l'utilizzo di FabricPool. Se ti serve capacità aggiuntiva in un sistema AFF, se utilizzi l'archiviazione BLOB di Azure su un sistema non AFF o se esegui l'upgrade da un cluster esistente, hai bisogno di un xref:./fabricpool/"[Licenza FabricPool](#)".

Se si ordina FabricPool per la prima volta per un cluster esistente, è disponibile una licenza FabricPool con 10 TB di capacità libera.

- Non è richiesta una licenza FabricPool se si utilizza Azure Blob Storage con Cloud Volumes ONTAP.
- Si consiglia di utilizzare la LIF utilizzata da ONTAP per la connessione al server a oggetti dello storage Blob Azure su una porta a 10 Gbps.
- FabricPool attualmente non supporta Azure Stack, ovvero servizi Azure on-premise.
- A livello di account in Microsoft Azure Blob Storage, FabricPool supporta solo livelli di storage hot e cool.

FabricPool non supporta il tiering a livello di blob. Inoltre, non supporta il tiering del Tier di storage di archivio di Azure.

### A proposito di questa attività

FabricPool attualmente non supporta Azure Stack, ovvero servizi Azure on-premise.

## Fasi

1. Specificare le informazioni di configurazione di Azure Blob Storage utilizzando `storage aggregate object-store config create` con il `-provider-type Azure_Cloud` parametro.
  - Il `storage aggregate object-store config create` Il comando non riesce se ONTAP non riesce ad accedere all'archivio Azure Blob con le informazioni fornite.
  - Si utilizza `-azure-account` Parametro per specificare l'account Azure Blob Storage.
  - Si utilizza `-azure-private-key` Parametro per specificare la chiave di accesso per l'autenticazione delle richieste a Azure Blob Storage.
  - Se la password di Azure Blob Storage viene modificata, è necessario aggiornare immediatamente la password corrispondente memorizzata in ONTAP.

In questo modo, ONTAP può accedere ai dati nello storage di Azure Blob senza interruzioni.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. Visualizzare e verificare le informazioni di configurazione di Azure Blob Storage utilizzando `storage aggregate object-store config show` comando.

Il `storage aggregate object-store config modify` Il comando consente di modificare le informazioni di configurazione dello storage di Azure Blob per FabricPool.

## Impostare gli archivi di oggetti per FabricPool in una configurazione MetroCluster

Se si esegue ONTAP 9.7 o versione successiva, è possibile impostare un FabricPool mirrorato su una configurazione MetroCluster per eseguire il Tier dei dati cold in archivi di oggetti in due diverse zone di errore.

### A proposito di questa attività

- FabricPool in MetroCluster richiede che l'aggregato mirrorato sottostante e la configurazione dell'archivio di oggetti associata siano di proprietà della stessa configurazione di MetroCluster.
- Non è possibile associare un aggregato a un archivio di oggetti creato nel sito MetroCluster remoto.
- È necessario creare configurazioni dell'archivio di oggetti sulla configurazione MetroCluster proprietaria dell'aggregato.

### Prima di iniziare

- La configurazione di MetroCluster è impostata e configurata correttamente.
- Nei siti MetroCluster appropriati vengono impostati due archivi di oggetti.
- I container sono configurati su ciascuno degli archivi di oggetti.
- Gli spazi IP vengono creati o identificati nelle due configurazioni MetroCluster e i relativi nomi corrispondono.

## Fase

1. Specificare le informazioni di configurazione dell'archivio di oggetti su ciascun sito MetroCluster utilizzando `storage object-store config create` comando.

In questo esempio, FabricPool è richiesto su un solo cluster nella configurazione MetroCluster. Per quel cluster vengono create due configurazioni di archivio di oggetti, una per ogni bucket di archivio di oggetti.

```
storage aggregate
  object-store config create -object-store-name mcc1-ostore-config-s1
  -provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mcc1-
ostore-config-s2
  -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
  <true|false> -provider <provider-type>
  -is-ssl-enabled <true|false> ipspace <IPSpace>
```

Questo esempio imposta FabricPool sul secondo cluster nella configurazione MetroCluster.

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s1
  -provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s2
  -provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

## Verificare le performance di throughput dell'archivio di oggetti prima di collegarlo a un Tier locale

Prima di collegare un archivio di oggetti a un livello locale, è possibile verificare le prestazioni di latenza e throughput dell'archivio di oggetti utilizzando il profiler dell'archivio di oggetti.

### Prima di essere

- È necessario aggiungere il livello cloud a ONTAP prima di poterlo utilizzare con il profiler dell'archivio di oggetti.
- È necessario essere in modalità privilegio avanzato CLI ONTAP.

### Fasi

1. Avviare il profiler dell'archivio oggetti:

```
storage aggregate object-store profiler start -object-store-name <name> -node <name>
```

2. Visualizzare i risultati:

```
storage aggregate object-store profiler show
```

## Collegare il Tier cloud a un Tier locale (aggregato)

Dopo aver configurato un archivio di oggetti come Tier cloud, specificare il Tier locale (aggregato) da utilizzare allegandolo a FabricPool. In ONTAP 9.5 e versioni successive, è anche possibile collegare Tier locali (aggregati) che contengono componenti di volume FlexGroup qualificati.

### A proposito di questa attività

Allegare un Tier cloud a un Tier locale è un'azione permanente. Non è possibile scollegare un Tier cloud da un Tier locale dopo il collegamento. Tuttavia, è possibile utilizzare "[Specchio FabricPool](#)" per collegare un tier locale a un tier cloud diverso.

### Prima di iniziare

Quando si utilizza l'interfaccia utente di ONTAP per impostare un aggregato per FabricPool, l'aggregato deve già esistere.




Quando si utilizza Gestione sistema per impostare un livello locale per FabricPool, è possibile creare il livello locale e configurarlo per l'utilizzo di FabricPool contemporaneamente.

### Fasi

È possibile collegare un Tier locale (aggregato) a un archivio di oggetti FabricPool con Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

## System Manager

1. Accedere a **Storage > Tier**, selezionare un livello cloud, quindi fare clic su .
2. Selezionare **Allega livelli locali**.
3. In **Add as Primary** (Aggiungi come principale), verificare che i volumi siano idonei per il collegamento.
4. Se necessario, selezionare **Converti volumi in thin provisioning**.
5. Fare clic su **Save** (Salva).

## CLI

### Per associare un archivio di oggetti a un aggregato con la CLI:

1. **Opzionale:** Per verificare la quantità di dati inattivi in un volume, seguire la procedura descritta in ["Determinare la quantità di dati inattivi in un volume utilizzando il reporting dei dati inattivi"](#).

La visualizzazione della quantità di dati inattivi in un volume può aiutare a decidere quale aggregato utilizzare per FabricPool.

2. Collegare l'archivio di oggetti a un aggregato utilizzando `storage aggregate object-store attach` comando.

Se l'aggregato non è mai stato utilizzato con FabricPool e contiene volumi esistenti, ai volumi viene assegnato il valore predefinito `snapshot-only` policy di tiering.

```
cluster1::> storage aggregate object-store attach -aggregate myaggr
-object-store-name Amazon01B1
```

È possibile utilizzare `allow-flexgroup true` Possibilità di collegare aggregati che contengono componenti del volume FlexGroup.

3. Visualizzare le informazioni sull'archivio di oggetti e verificare che l'archivio di oggetti collegato sia disponibile utilizzando `storage aggregate object-store show` comando.

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability State
-----	-----	-----
myaggr	Amazon01B1	available

## Dati di Tier al bucket locale


A partire da ONTAP 9.8, è possibile eseguire il tiering dei dati sullo storage a oggetti locale utilizzando ONTAP S3.

Il tiering dei dati in un bucket locale offre una semplice alternativa allo spostamento dei dati in un altro Tier locale. Questa procedura utilizza un bucket esistente sul cluster locale oppure è possibile consentire a ONTAP di creare automaticamente una nuova VM di storage e un nuovo bucket.

Tenere presente che una volta collegato a un Tier locale (aggregato), il Tier cloud non può essere disconnesso.

Per questo flusso di lavoro è necessaria una licenza S3, che crea un nuovo server S3 e un nuovo bucket, oppure utilizza quelli esistenti. Questa licenza è inclusa in "ONTAP uno". Per questo flusso di lavoro non è richiesta una licenza FabricPool.

### Fase

1. Tier data to a local bucket: Fare clic su **Tier**, selezionare un Tier, quindi fare clic su .
2. Se necessario, abilitare il thin provisioning.
3. Scegliere un livello esistente o crearne uno nuovo.
4. Se necessario, modificare il criterio di tiering esistente.

## Gestire FabricPool

### Panoramica di Manage FabricPool

Per soddisfare le esigenze di tiering dello storage, ONTAP consente di visualizzare la quantità di dati inattivi in un volume, aggiungere o spostare volumi in FabricPool, monitorare l'utilizzo dello spazio per FabricPool o modificare la policy di tiering di un volume o il periodo di raffreddamento minimo di tiering.

### Determinare la quantità di dati inattivi in un volume utilizzando il reporting dei dati inattivi

La visualizzazione della quantità di dati inattivi in un volume consente di utilizzare correttamente i Tier di storage. Le informazioni nel reporting dei dati inattivi consentono di decidere quale aggregato utilizzare per FabricPool, se spostare un volume in FabricPool o da esso o se modificare il criterio di tiering di un volume.

### Di cosa hai bisogno

Per utilizzare la funzionalità di reporting dei dati inattivi, è necessario eseguire ONTAP 9.4 o versioni successive.

### A proposito di questa attività

- Alcuni aggregati non supportano il reporting dei dati inattivi.

Non è possibile attivare la funzione di reporting dei dati inattivi quando non è possibile attivare FabricPool, incluse le seguenti istanze:

- Aggregati root
- Aggregati MetroCluster con versioni di ONTAP precedenti alla 9.7
- Flash Pool (aggregati ibridi o aggregati SnapLock)
- Il reporting dei dati inattivi è attivato per impostazione predefinita sugli aggregati in cui è attivata la compressione adattiva per tutti i volumi.
- Per impostazione predefinita, il reporting dei dati inattivi è attivato su tutti gli aggregati SSD in ONTAP 9.6.
- Per impostazione predefinita, la funzione di reporting dei dati inattivi è attivata nell'aggregato FabricPool in ONTAP 9.4 e ONTAP 9.5.




- È possibile abilitare la creazione di report dei dati inattivi su aggregati non FabricPool utilizzando l'interfaccia CLI di ONTAP, inclusi gli aggregati di dischi rigidi, a partire da ONTAP 9.6.

#### **Procedura**

È possibile determinare la quantità di dati inattivi con Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

## System Manager

### 1. Scegliere una delle seguenti opzioni:

- Una volta esistenti aggregati HDD, selezionare **Storage > Tier** e fare clic su  per l'aggregato su cui si desidera attivare il reporting dei dati inattivi.
- Se non sono configurati Tier cloud, accedere a **Dashboard** e fare clic sul collegamento **Enable inactive data reporting** sotto **Capacity**.

## CLI

### Per attivare la creazione di report dei dati inattivi con la CLI:

1. Se l'aggregato per il quale si desidera visualizzare il reporting dei dati inattivi non viene utilizzato in FabricPool, attivare il reporting dei dati inattivi per l'aggregato utilizzando `storage aggregate modify` con il `-is-inactive-data-reporting-enabled true` parametro.

```
cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
-data-reporting-enabled true
```

È necessario attivare esplicitamente la funzionalità di reporting dei dati inattivi su un aggregato non utilizzato per FabricPool.

Non è possibile e non è necessario attivare il reporting dei dati inattivi su un aggregato abilitato a FabricPool perché l'aggregato è già dotato di report dei dati inattivi. Il `-is-inactive-data-reporting-enabled` Il parametro non funziona sugli aggregati abilitati per FabricPool.

Il `-fields is-inactive-data-reporting-enabled` del parametro `storage aggregate show` il comando indica se il reporting dei dati inattivi è attivato su un aggregato.

2. Per visualizzare la quantità di dati inattivi su un volume, utilizzare `volume show` con il `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parametro.

```
cluster1::> volume show -fields performance-tier-inactive-user-
data,performance-tier-inactive-user-data-percent

vserver volume performance-tier-inactive-user-data performance-tier-
inactive-user-data-percent
-----
-----
vsim1    vol0    0B                                0%
vs1      vs1rv1  0B                                0%
vs1      vv1     10.34MB                             0%
vs1      vv2     10.38MB                             0%
4 entries were displayed.
```

- Il `performance-tier-inactive-user-data` campo visualizza la quantità di dati utente memorizzati nell'aggregato non attivi.

- Il `performance-tier-inactive-user-data-percent` Visualizza la percentuale di dati inattivi nel file system attivo e nelle copie Snapshot.
- Per un aggregato non utilizzato per FabricPool, il reporting dei dati inattivi utilizza la policy di tiering per stabilire la quantità di dati da riportare come cold.
  - Per `none` policy di tiering, 31 giorni.
  - Per `snapshot-only` e `auto`, utilizza il reporting dei dati inattivi `tiering-minimum-cooling-days`.
  - Per `ALL` policy, il reporting dei dati inattivi presuppone che i dati verranno tier entro un giorno.

Fino al raggiungimento del punto, l'output mostra “-” per la quantità di dati inattivi invece di un valore.
- Su un volume che fa parte di FabricPool, i report di ONTAP come inattivi dipendono dal criterio di tiering impostato su un volume.
  - Per `none` Policy di tiering, ONTAP riporta la quantità di volume intero che è inattivo per almeno 31 giorni. Non è possibile utilizzare `-tiering-minimum-cooling-days` con il `none` policy di tiering.
  - Per `ALL`, `snapshot-only`, e `auto` policy di tiering, il reporting dei dati inattivi non è supportato.

## Gestire i volumi per FabricPool

### Creare un volume per FabricPool

È possibile aggiungere volumi a FabricPool creando nuovi volumi direttamente nell'aggregato abilitato a FabricPool o spostando i volumi esistenti da un altro aggregato all'aggregato abilitato a FabricPool.

Quando si crea un volume per FabricPool, è possibile specificare un criterio di tiering. Se non viene specificato alcun criterio di tiering, il volume creato utilizza l'impostazione predefinita `snapshot-only` policy di tiering. Per un volume con `snapshot-only` oppure `auto` policy di tiering, è anche possibile specificare il periodo minimo di raffreddamento del tiering.

### Di cosa hai bisogno

- Impostazione di un volume per l'utilizzo di `auto` La policy di tiering o la specifica del periodo di raffreddamento minimo di tiering richiede ONTAP 9.4 o versione successiva.
- L'utilizzo di FlexGroup Volumes richiede ONTAP 9.5 o versione successiva.
- Impostazione di un volume per l'utilizzo di `all` I criteri di tiering richiedono ONTAP 9.6 o versione successiva.
- Impostazione di un volume per l'utilizzo di `-cloud-retrieval-policy` Il parametro richiede ONTAP 9.8 o versione successiva.

### Fasi

1. Creare un nuovo volume per FabricPool utilizzando `volume create` comando.
  - Il `-tiering-policy` il parametro opzionale consente di specificare il criterio di tiering per il volume.

È possibile specificare uno dei seguenti criteri di tiering:

- `snapshot-only` (impostazione predefinita)
- `auto`
- `all`
- `backup` (obsoleto)
- `none`

#### "Tipi di policy di tiering FabricPool"

- Il `-cloud-retrieval-policy` il parametro opzionale consente agli amministratori del cluster con il livello di privilegio avanzato di eseguire l'override del comportamento predefinito di recupero o migrazione del cloud controllato dalla policy di tiering.

È possibile specificare una delle seguenti policy di recupero del cloud:

- `default`

La policy di tiering determina quali dati vengono recuperati, quindi non vi è alcuna modifica al recupero dei dati nel cloud `default` policy-recupero-cloud. Questo significa che il comportamento è lo stesso delle release precedenti a ONTAP 9.8:

- Se la policy di tiering è `none` oppure `snapshot-only`, quindi "default" significa che qualsiasi lettura dei dati basata su client viene estratta dal tier cloud al tier di performance.
- Se la policy di tiering è `auto`, quindi viene estratta qualsiasi lettura casuale basata su client, ma non letture sequenziali.
- Se la policy di tiering è `all` quindi, nessun dato client-driven viene estratto dal tier cloud.

- `on-read`

Tutte le letture dei dati basate su client vengono estratte dal Tier cloud al Tier di performance.

- `never`

Nessun dato client-driven viene estratto dal Tier cloud al Tier di performance

- `promote`

- Per la policy di tiering `none`, tutti i dati del cloud vengono estratti dal livello cloud al livello di performance
- Per la policy di tiering `snapshot-only`, tutti i dati del file system attivi vengono estratti dal livello cloud al livello di performance.

- Il `-tiering-minimum-cooling-days` il parametro opzionale nel livello di privilegio avanzato consente di specificare il periodo minimo di raffreddamento del tiering per un volume che utilizza `snapshot-only` oppure `auto` policy di tiering.

A partire da ONTAP 9.8, è possibile specificare un valore compreso tra 2 e 183 per i giorni di raffreddamento minimi di tiering. Se si utilizza una versione di ONTAP precedente alla 9.8, è possibile specificare un valore compreso tra 2 e 63 per i giorni di raffreddamento minimi di tiering.

## Esempio di creazione di un volume per FabricPool

Nell'esempio seguente viene creato un volume denominato "myvol1" nell'aggregato abilitato a FabricPool "myFabricPool". La policy di tiering è impostata su `auto` e il periodo minimo di raffreddamento del tiering è impostato su 45 giorni:

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool  
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

## Informazioni correlate

["Gestione dei volumi FlexGroup"](#)

## Spostare un volume su FabricPool

Quando si sposta un volume in FabricPool, è possibile specificare o modificare il criterio di tiering per il volume durante lo spostamento. A partire da ONTAP 9.8, quando si sposta un volume non FabricPool con la funzione di reporting dei dati inattivi attivata, FabricPool utilizza una mappa termica per leggere i blocchi tierable e sposta i dati cold nel Tier di capacità sulla destinazione FabricPool.

## Di cosa hai bisogno

Devi comprendere come la modifica della policy di tiering possa influire sul tempo necessario per far diventare i dati più freddi e spostarli nel Tier cloud.

["Cosa accade alla policy di tiering quando si sposta un volume"](#)

## A proposito di questa attività

Se un volume non FabricPool ha attivato la funzione di reporting dei dati inattivi, quando si sposta un volume con policy di tiering `auto` oppure `snapshot-only` In un FabricPool, FabricPool legge i blocchi di temperatura da un file di mappa termica e utilizza tale temperatura per spostare i dati Cold direttamente nel Tier di capacità sulla destinazione FabricPool.

Non utilizzare `-tiering-policy` Opzione di spostamento del volume se si utilizza ONTAP 9.8 e si desidera che FabricPools utilizzi le informazioni di reporting dei dati inattive per spostare i dati direttamente nel livello di capacità. L'utilizzo di questa opzione fa sì che FabricPools ignori i dati relativi alla temperatura e segua invece il comportamento di spostamento delle release precedenti a ONTAP 9.8.

## Fase

1. Utilizzare `volume move start` Comando per spostare un volume in FabricPool.

Il `-tiering-policy` il parametro opzionale consente di specificare il criterio di tiering per il volume.

È possibile specificare uno dei seguenti criteri di tiering:

- `snapshot-only` (impostazione predefinita)
- `auto`
- `all`
- `none` ["Tipi di policy di tiering FabricPool"](#)

## Esempio di spostamento di un volume in FabricPool

Nell'esempio riportato di seguito viene spostato un volume denominato "myvol2" della SVM "vs1" nell'aggregato abilitato a FabricPool "dest\_FabricPool". Il volume viene esplicitamente impostato per l'utilizzo di none policy di tiering:

```
cluster1::> volume move start -vserver vs1 -volume myvol2  
-destination-aggregate dest_FabricPool -tiering-policy none
```

## Attiva e disattiva i volumi da scrivere direttamente nel cloud

A partire da ONTAP 9.14.1, puoi abilitare e disabilitare la scrittura direttamente nel cloud su un volume nuovo o esistente in una FabricPool, per consentire ai client NFS di scrivere dati direttamente nel cloud senza attendere le scansioni di tiering. I client SMB continuano a scrivere nel Tier di performance in un volume abilitato per la scrittura nel cloud. La modalità cloud-write è disattivata per impostazione predefinita.

Avere la possibilità di scrivere direttamente nel cloud è utile per casi come le migrazioni, ad esempio, dove grandi quantità di dati vengono trasferite in un cluster rispetto a quanto il cluster può supportare nel Tier locale. Senza la modalità cloud-write, durante la migrazione, vengono trasferite piccole quantità di dati, quindi trasferite e di nuovo in tiering, fino al completamento della migrazione. Utilizzando la modalità cloud-write, questo tipo di gestione non è più necessario, perché i dati non vengono mai trasferiti nel Tier locale.

### Prima di iniziare

- Dovresti essere un amministratore di cluster o SVM.
- È necessario essere al livello di privilegi avanzati.
- Il volume deve essere di tipo lettura-scrittura.
- Il volume deve disporre di TUTTA LA policy di tiering.

## Attiva la scrittura direttamente nel cloud durante la creazione del volume

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Creazione di un volume e abilitazione della modalità cloud-write:

```
volume create -volume <volume name> -is-cloud-write-enabled <true|false>  
-aggregate <local tier name>
```

L'esempio seguente crea un volume denominato vol1 con Cloud Write abilitato nel Tier locale FabricPool (aggr1):

```
volume create -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
```

## Consenti la scrittura diretta nel cloud di un volume esistente

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Modifica di un volume per abilitare la modalità cloud-write:

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>  
-aggregate <local tier name>
```

Il seguente esempio modifica un volume chiamato vol1 con scrittura cloud abilitata nel Tier locale FabricPool (aggr1):

```
volume modify -volume vol1 -is-cloud-write-enabled true -aggregate aggr1
```

## Disattivare la scrittura direttamente nel cloud su un volume

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Disattiva modalità cloud-write:

```
volume modify -volume <volume name> -is-cloud-write-enabled <true|false>  
-aggregate <aggregate name>
```

L'esempio seguente crea un volume denominato vol1 con Cloud Write abilitato:

```
volume modify -volume vol1 -is-cloud-write-enabled false -aggregate  
aggr1
```

## Attiva e disattiva la modalità aggressiva di Read-ahead

A partire da ONTAP 9.14.1, puoi abilitare e disabilitare la modalità aggressiva Read-ahead sui volumi in FabricPool che offrono supporto per media e intrattenimento, come ad esempio i workload in streaming dei film. Una aggressiva modalità di Read-ahead è disponibile in ONTAP 9.14.1 su tutte le piattaforme on-premise che supportano FabricPool. La funzione è disattivata per impostazione predefinita.

## A proposito di questa attività

Il `aggressive-readahead-mode` il comando ha due opzioni:

- `none`: la funzione `read-ahead` è disattivata.
- `file_prefetch`: il sistema legge l'intero file in memoria prima dell'applicazione client.

## Prima di iniziare

- Dovresti essere un amministratore di cluster o SVM.
- È necessario essere al livello di privilegi avanzati.

## Attiva la modalità Read-ahead aggressiva durante la creazione del volume

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Creazione di un volume e abilitazione della modalità aggressiva di Read-ahead:

```
volume create -volume <volume name> -aggressive-readahead-mode  
<none|file_prefetch>
```

Nell'esempio seguente viene creato un volume denominato `vol1` con la funzione di Read-ahead aggressiva abilitata con l'opzione `file_prefetch`:

```
volume create -volume vol1 -aggressive-readahead-mode file_prefetch
```

## Disattiva la modalità aggressiva di lettura anticipata

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Disattivare la modalità aggressiva di Read-ahead:

```
volume modify -volume <volume name> -aggressive-readahead-mode none
```

Nell'esempio seguente viene modificato un volume denominato `vol1` per disattivare la modalità aggressiva di Read-ahead:



```
volume modify -volume voll -aggressive-readahead-mode none
```

## Visualizzazione di una modalità di Read-ahead aggressiva su un volume

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Visualizza la modalità di lettura aggressiva:

```
volume show -fields aggressive-readahead-mode
```

## Tagging degli oggetti mediante tag personalizzati creati dall'utente

### Tagging degli oggetti mediante panoramica dei tag personalizzati creati dall'utente

A partire da ONTAP 9.8, FabricPool supporta il tagging degli oggetti utilizzando tag personalizzati creati dall'utente per consentire la classificazione e l'ordinamento degli oggetti per una gestione più semplice. Se si è un utente con il livello di privilegio admin, è possibile creare nuovi tag di oggetto e modificare, eliminare e visualizzare i tag esistenti.

### Assegnare un nuovo tag durante la creazione del volume

È possibile creare un nuovo tag di oggetto quando si desidera assegnare uno o più tag a nuovi oggetti a più livelli da un nuovo volume creato. È possibile utilizzare i tag per classificare e ordinare gli oggetti di tiering per semplificare la gestione dei dati. A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per creare tag di oggetto.

### A proposito di questa attività

È possibile impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Questi tag vengono conservati durante lo spostamento di un volume.

- È consentito un massimo di 4 tag per volume
- Nella CLI, ogni tag di oggetto deve essere una coppia chiave-valore separata da un segno uguale ("")
- Nella CLI, più tag devono essere separati da una virgola (",")
- Ogni valore di tag può contenere un massimo di 127 caratteri
- Ogni tag deve iniziare con un carattere alfabetico o con un carattere di sottolineatura.

Le chiavi devono contenere solo caratteri alfanumerici e caratteri di sottolineatura, mentre il numero massimo consentito è 127.

## Procedura

È possibile assegnare tag di oggetto con Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

### System Manager

1. Selezionare **Storage > Tier**.
2. Individuare un Tier di storage con i volumi che si desidera etichettare.
3. Fare clic sulla scheda **Volumes** (volumi).
4. Individuare il volume da contrassegnare e nella colonna **Tag oggetto** selezionare **fare clic per inserire i tag**.
5. Inserire una chiave e un valore.
6. Fare clic su **Apply** (Applica).

### CLI

1. Utilizzare `volume create` con il `-tiering-object-tags` opzione per creare un nuovo volume con i tag specificati. È possibile specificare più tag in coppie separate da virgole:

```
volume create [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1> [
    ,<key2=value2>,<key3=value3>,<key4=value4> ]
```

Nell'esempio seguente viene creato un volume denominato `fp_volume1` con tre tag di oggetto.

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

### Modificare un tag esistente

È possibile modificare il nome di un tag, sostituire tag su oggetti esistenti nell'archivio di oggetti o aggiungere un tag diverso a nuovi oggetti che si intende aggiungere in seguito.

### A proposito di questa attività

Utilizzando il `volume modify` con il `-tiering-object-tags` l'opzione sostituisce i tag esistenti con il nuovo valore fornito.

## Procedura

## System Manager

1. Selezionare **Storage > Tier**.
2. Individuare un Tier di storage con volumi contenenti tag che si desidera modificare.
3. Fare clic sulla scheda **Volumes** (volumi).
4. Individuare il volume con i tag che si desidera modificare e nella colonna **Tag oggetto** fare clic sul nome del tag.
5. Modificare il tag.
6. Fare clic su **Apply** (Applica).

## CLI

1. Utilizzare `volume modify` con il `-tiering-object-tags` opzione per modificare un tag esistente.

```
volume modify [ -vserver <vserver name> ] -volume <volume_name>  
-tiering-object-tags <key1=value1> [ ,<key2=value2>,  
<key3=value3>,<key4=value4> ]
```

Nell'esempio seguente viene modificato il nome del tag esistente `type=abc` in `type=xyz`.

```
vol create -volume fp_volumel -vserver vs0 -tiering-object-tags  
project=fabricpool,type=xyz,content=data
```

## Eliminare un tag

È possibile eliminare i tag di oggetto quando non si desidera che vengano impostati su un volume o su oggetti nell'archivio di oggetti.

## Procedura

È possibile eliminare i tag degli oggetti con Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

## System Manager

1. Selezionare **Storage > Tier**.
2. Individuare un Tier di storage con volumi contenenti tag che si desidera eliminare.
3. Fare clic sulla scheda **Volumes** (volumi).
4. Individuare il volume con i tag che si desidera eliminare e nella colonna **Tag oggetto** fare clic sul nome del tag.
5. Per eliminare il tag, fare clic sull'icona del cestino.
6. Fare clic su **Apply** (Applica).

## CLI

1. Utilizzare `volume modify` con il `-tiering-object-tags` seguito da un valore vuoto ("" ) per eliminare un tag esistente.

Nell'esempio seguente vengono cancellati i tag esistenti su `fp_volume1`.

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
```

## Visualizzare i tag esistenti su un volume

È possibile visualizzare i tag esistenti su un volume per visualizzare i tag disponibili prima di aggiungere nuovi tag all'elenco.

### Fase

1. Utilizzare `volume show` con il `-tiering-object-tags` opzione per visualizzare i tag esistenti su un volume.

```
volume show [ -vserver <vserver name> ] -volume <volume_name> -fields  
-tiering-object-tags
```

## Controllare lo stato di tagging degli oggetti sui volumi FabricPool

È possibile verificare se il tagging è completo su uno o più volumi FabricPool.

### Fase

1. Utilizzare `vol show` con il `-fieldsneeds-object-retagging` opzione per verificare se l'etichettatura è in corso, se è stata completata o se l'etichettatura non è stata impostata.

```
vol show -fields needs-object-retagging [ -instance | -volume <volume  
name>]
```

Viene visualizzato uno dei seguenti valori:

- `true` — lo scanner di tag degli oggetti non deve ancora essere eseguito o deve essere eseguito nuovamente per questo volume
- `false` — lo scanner di tagging degli oggetti ha completato la tagging per questo volume
- `<->` — lo scanner di tag degli oggetti non è applicabile a questo volume. Questo accade per i volumi che non risiedono su FabricPools.

## Monitorare l'utilizzo dello spazio per FabricPool

Devi sapere quanti dati sono memorizzati nei livelli di performance e cloud per FabricPool. Tali informazioni consentono di determinare se è necessario modificare la policy di tiering di un volume, aumentare il limite di utilizzo della licenza FabricPool o aumentare lo spazio di storage del Tier cloud.

### Fasi

1. Monitorare l'utilizzo dello spazio per gli aggregati abilitati a FabricPool utilizzando uno dei seguenti comandi per visualizzare le informazioni:

Se si desidera visualizzare...	Quindi utilizzare questo comando:
La dimensione utilizzata del Tier cloud in un aggregato	<code>storage aggregate show con -instance parametro</code>
Dettagli sull'utilizzo dello spazio all'interno di un aggregato, inclusa la capacità di riferimento dell'archivio di oggetti	<code>storage aggregate show-space con -instance parametro</code>
Utilizzo dello spazio degli archivi di oggetti collegati agli aggregati, inclusa la quantità di spazio di licenza utilizzata	<code>storage aggregate object-store show-space</code>
Un elenco di volumi in un aggregato e le impronte dei dati e dei metadati	<code>volume show-footprint</code>

Oltre a utilizzare i comandi CLI, è possibile utilizzare Active IQ Unified Manager (precedentemente noto come gestore unificato di OnCommand), insieme a FabricPool Advisor, supportato su cluster ONTAP 9.4 e versioni successive, o System Manager per monitorare l'utilizzo dello spazio.

Nell'esempio seguente vengono illustrati i modi per visualizzare l'utilizzo dello spazio e le informazioni correlate per FabricPool:

```
cluster1::> storage aggregate show-space -instance
```

```

Aggregate: MyFabricPool
...
Aggregate Display Name:
MyFabricPool
...
Total Object Store Logical Referenced
Capacity: -
Object Store Logical Referenced Capacity
Percentage: -
...
Object Store
Size: -
Object Store Space Saved by Storage
Efficiency: -
Object Store Space Saved by Storage Efficiency
Percentage: -
Total Logical Used
Size: -
Logical Used
Percentage: -
Logical Unreferenced
Capacity: -
Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance
```

```

Aggregate: MyFabricPool
...
Composite: true
Capacity Tier Used Size:
...
```

```
cluster1::> volume show-footprint
```

```
Vserver : vs1
```

```
Volume : rootvol
```

Feature	Used	Used%
Volume Footprint	KB	%
Volume Guarantee	MB	%
Flexible Volume Metadata	KB	%
Delayed Frees	KB	%
Total Footprint	MB	%

```
Vserver : vs1
```

```
Volume : vol
```

Feature	Used	Used%
Volume Footprint	KB	%
Footprint in Performance Tier	KB	%
Footprint in Amazon01	KB	%
Flexible Volume Metadata	MB	%
Delayed Frees	KB	%
Total Footprint	MB	%
...		

2. Eseguire una delle seguenti operazioni in base alle necessità:

Se si desidera...	Quindi...
Modificare la policy di tiering di un volume	Seguire la procedura descritta in <a href="#">"Gestione del tiering dello storage modificando la policy di tiering di un volume o il periodo minimo di raffreddamento del tiering"</a> .
Aumentare il limite di utilizzo della licenza FabricPool	Contattare il rappresentante commerciale NetApp o del partner.  <a href="#">"Supporto NetApp"</a>
Aumentare lo spazio di storage del Tier cloud	Contattare il provider dell'archivio di oggetti utilizzato per il livello cloud.

## Gestire il tiering dello storage modificando la policy di tiering di un volume o il periodo minimo di raffreddamento del tiering

È possibile modificare la policy di tiering di un volume per controllare se i dati vengono spostati nel Tier cloud quando diventano inattivi (*cold*). Per un volume con `snapshot-only` oppure `auto` policy di tiering, puoi anche specificare il periodo minimo di raffreddamento del tiering in base al quale i dati dell'utente devono rimanere inattivi prima di essere spostati nel tier cloud.

### Di cosa hai bisogno

Modifica di un volume in `auto` La policy di tiering o la modifica del periodo di raffreddamento minimo di tiering richiede ONTAP 9.4 o versione successiva.

### A proposito di questa attività

La modifica della policy di tiering di un volume modifica solo il successivo comportamento di tiering del volume. Non sposta retroattivamente i dati nel Tier cloud.

La modifica della policy di tiering potrebbe influire sul tempo necessario affinché i dati diventino freddi e vengano spostati al livello cloud.

["Cosa accade quando si modifica il criterio di tiering di un volume in FabricPool"](#)

### Fasi

1. Modificare il criterio di tiering per un volume esistente utilizzando `volume modify` con il `-tiering-policy` parametro:

È possibile specificare uno dei seguenti criteri di tiering:

- `snapshot-only` (impostazione predefinita)
- `auto`
- `all`
- `none`

["Tipi di policy di tiering FabricPool"](#)

2. Se il volume utilizza `snapshot-only` oppure `auto` policy di tiering e si desidera modificare il periodo di raffreddamento minimo di tiering, utilizzare `volume modify` con il `-tiering-minimum-cooling-days` parametro facoltativo nel livello di privilegio avanzato.

È possibile specificare un valore compreso tra 2 e 183 per i giorni di raffreddamento minimi di tiering. Se si utilizza una versione di ONTAP precedente alla 9.8, è possibile specificare un valore compreso tra 2 e 63 per i giorni di raffreddamento minimi di tiering.

### Esempio di modifica della policy di tiering e del periodo minimo di raffreddamento di tiering di un volume

Nell'esempio seguente viene modificata la policy di tiering del volume "myvol" in SVM "vs1" in `auto` e il periodo di raffreddamento minimo di tiering fino a 45 giorni:



```
cluster1::> volume modify -vserver vs1 -volume myvol  
-tiering-policy auto -tiering-minimum-cooling-days 45
```

## Archiviazione di volumi con FabricPool (video)

Questo video mostra una rapida panoramica sull'utilizzo di Gestione sistema per archiviare un volume su un livello cloud con FabricPool.

["Video NetApp: Archiviazione dei volumi con FabricPool \(backup + spostamento del volume\)"](#)

### Informazioni correlate

["TechComm TV di NetApp: Elenco di riproduzione FabricPool"](#)

## Utilizza i controlli di migrazione del cloud per ignorare la policy di tiering predefinita di un volume

È possibile modificare la policy di tiering predefinita di un volume per controllare il recupero dei dati utente dal livello cloud al livello di performance utilizzando `-cloud-retrieval-policy` Opzione introdotta in ONTAP 9.8.

### Di cosa hai bisogno

- Modifica di un volume mediante `-cloud-retrieval-policy` L'opzione richiede ONTAP 9.8 o versione successiva.
- Per eseguire questa operazione, è necessario disporre del livello di privilegio avanzato.
- È necessario comprendere il comportamento delle policy di tiering con `-cloud-retrieval-policy`.

["Come funzionano le policy di tiering con la migrazione del cloud"](#)

### Fase

1. Modificare il comportamento dei criteri di tiering per un volume esistente utilizzando `volume modify` con il `-cloud-retrieval-policy` opzione:

```
volume create -volume <volume_name> -vserver <vserver_name> - tiering-  
policy <policy_name> -cloud-retrieval-policy
```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy  
promote
```

## Promuovi i dati al Tier di performance

### Promuovi i dati nella panoramica del Tier di performance

A partire da ONTAP 9.8, se sei un amministratore del cluster a livello di privilegi avanzati, puoi promuovere in modo proattivo i dati al livello di performance dal livello cloud

utilizzando una combinazione di `tiering-policy` e `a. cloud-retrieval-policy` impostazione.

### A proposito di questa attività

Questa operazione può essere eseguita se si desidera interrompere l'utilizzo di FabricPool su un volume o se si dispone di `snapshot-only` Tiering policy e vuoi riportare i dati di copia Snapshot ripristinati al Tier di performance.

#### Promuovi tutti i dati da un volume FabricPool al Tier di performance

Puoi recuperare in modo proattivo tutti i dati su un volume FabricPool nel cloud e promuoverli al livello di performance.

#### Fase

1. Utilizzare `volume modify` comando da impostare `tiering-policy` a. `none` e `cloud-retrieval-policy` a. `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

#### Promuovere i dati del file system al livello di performance

È possibile recuperare in modo proattivo i dati del file system attivi da una copia Snapshot ripristinata nel Tier cloud e promuoverli nel Tier di performance.

#### Fase

1. Utilizzare `volume modify` comando da impostare `tiering-policy` a. `snapshot-only` e `cloud-retrieval-policy` a. `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

#### Verifica lo stato di una promozione per i Tier di performance

È possibile controllare lo stato della promozione del Tier di performance per determinare quando l'operazione è completa.

#### Fase

1. Utilizzare il volume `object-store` con il `tiering` opzione per controllare lo stato della promozione del tier di performance.

```

volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name

```

```

volume object-store tiering show v1 -instance

Vserver: vs1
Volume: v1
Node Name: node1
Volume DSID: 1023
Aggregate Name: a1
State: ready
Previous Run Status: completed
Aborted Exception Status: -
Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
Scanner Percent Complete: -
Scanner Current VBN: -
Scanner Max VBNs: -
Time Waiting Scan will be scheduled: -
Tiering Policy: snapshot-only
Estimated Space Needed for Promotion: -
Time Scan Started: -
Estimated Time Remaining for scan to complete: -
Cloud Retrieve Policy: promote

```

#### Attivare la migrazione pianificata e il tiering

A partire da ONTAP 9.8, è possibile attivare una richiesta di scansione a più livelli in qualsiasi momento quando si preferisce non attendere la scansione a più livelli predefinita.

#### Fase

1. Utilizzare `volume object-store` con il `trigger` opzione per richiedere migrazione e tiering.

```

volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name

```

## Gestire i mirror FabricPool

## Panoramica di Manage FabricPool Mirrors

Per garantire che i dati siano accessibili negli archivi dati in caso di disastro e per consentire la sostituzione di un archivio dati, è possibile configurare un mirror FabricPool aggiungendo un secondo archivio dati per il Tier sincrono dei dati a due archivi dati. È possibile aggiungere un secondo archivio dati a configurazioni FabricPool nuove o esistenti, monitorare lo stato del mirror, visualizzare i dettagli del mirror FabricPool, promuovere un mirror e rimuovere un mirror. È necessario eseguire ONTAP 9.7 o versione successiva.

### Creare un mirror FabricPool

Per creare un mirror FabricPool, si allegano due archivi di oggetti a un singolo FabricPool. È possibile creare un mirror FabricPool allegando un secondo archivio di oggetti a una configurazione FabricPool esistente di un singolo archivio di oggetti oppure creare una nuova configurazione FabricPool di un singolo archivio di oggetti e quindi allegarvi un secondo archivio di oggetti. È inoltre possibile creare mirror FabricPool sulle configurazioni MetroCluster.

#### Di cosa hai bisogno

- È necessario aver già creato i due archivi di oggetti utilizzando `storage aggregate object-store config` comando.
- Se si creano mirror FabricPool su configurazioni MetroCluster:
  - È necessario aver già configurato e configurato MetroCluster
  - È necessario aver creato le configurazioni dell'archivio di oggetti sul cluster selezionato.

Se si creano mirror FabricPool su entrambi i cluster in una configurazione MetroCluster, è necessario aver creato le configurazioni dell'archivio di oggetti su entrambi i cluster.

- Se non si utilizzano archivi di oggetti on-premise per le configurazioni MetroCluster, è necessario verificare che esista uno dei seguenti scenari:
  - Gli archivi di oggetti si trovano in diverse zone di disponibilità
  - Gli archivi di oggetti sono configurati per conservare copie di oggetti in più zone di disponibilità

["Impostazione degli archivi di oggetti per FabricPool in una configurazione MetroCluster"](#)

#### A proposito di questa attività

L'archivio di oggetti utilizzato per il mirror FabricPool deve essere diverso dall'archivio di oggetti primario.

La procedura per la creazione di un mirror FabricPool è la stessa per le configurazioni MetroCluster e non MetroCluster.

#### Fasi

1. Se non si utilizza una configurazione FabricPool esistente, crearne una nuova allegando un archivio di oggetti a un aggregato utilizzando `storage aggregate object-store attach` comando.

Questo esempio crea un nuovo FabricPool allegando un archivio di oggetti a un aggregato.

```
cluster1::> storage aggregate object-store attach -aggregate aggr1 -name my-store-1
```

2. Collegare un secondo archivio di oggetti all'aggregato utilizzando `storage aggregate object-store mirror` comando.

In questo esempio viene collegato un secondo archivio di oggetti a un aggregato per creare un mirror FabricPool.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name my-store-2
```

### Monitorare lo stato di risincronizzazione del mirror FabricPool

Quando si sostituisce un archivio di oggetti primario con un mirror, potrebbe essere necessario attendere la risincronizzazione del mirror con l'archivio di dati primario.

#### A proposito di questa attività

Se il mirror FabricPool è sincronizzato, non viene visualizzata alcuna voce.

#### Fase

1. Monitorare lo stato di risincronizzazione del mirror utilizzando `storage aggregate object-store show-resync-status` comando.

```
aggregate1::> storage aggregate object-store show-resync-status -aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
-----	-----	-----	-----
aggr1	my-store-1	my-store-2	40%

### Visualizza i dettagli del mirror FabricPool

È possibile visualizzare i dettagli di un mirror FabricPool per visualizzare gli archivi di oggetti presenti nella configurazione e se il mirror dell'archivio di oggetti è sincronizzato con l'archivio di oggetti primario.

#### Fase

1. Visualizzare le informazioni su un mirror FabricPool utilizzando `storage aggregate object-store show` comando.

In questo esempio vengono visualizzati i dettagli relativi agli archivi di oggetti primari e mirror in un mirror

FabricPool.

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability	Mirror Type
aggr1	my-store-1	available	primary
	my-store-2	available	mirror

Questo esempio mostra i dettagli sul mirror FabricPool, incluso se il mirror è degradato a causa di un'operazione di risincronizzazione.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-store-1	primary	-
	my-store-2	mirror	false

### Promuovere un mirror FabricPool

È possibile riassegnare il mirror dell'archivio di oggetti come archivio di oggetti primario promuovendolo. Quando il mirror dell'archivio di oggetti diventa il principale, il principale originale diventa automaticamente il mirror.

#### Di cosa hai bisogno

- Il mirror FabricPool deve essere sincronizzato
- L'archivio di oggetti deve essere operativo

#### A proposito di questa attività

È possibile sostituire l'archivio di oggetti originale con un archivio di oggetti di un altro provider cloud. Ad esempio, il mirror originale potrebbe essere un archivio di oggetti AWS, ma è possibile sostituirlo con un archivio di oggetti Azure.

#### Fase

1. Promuovere un mirror dell'archivio di oggetti utilizzando `storage aggregate object-store modify -aggregate` comando.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name my-store-2 -mirror-type primary
```

## Rimuovere un mirror FabricPool

È possibile rimuovere un mirror FabricPool se non è più necessario replicare un archivio di oggetti.

### Di cosa hai bisogno

L'archivio di oggetti primario deve essere operativo, altrimenti il comando non riesce.

### Fase

1. Rimuovere un mirror dell'archivio di oggetti in un FabricPool utilizzando `storage aggregate object-store unmirror -aggregate` comando.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

## Sostituire un archivio di oggetti esistente utilizzando un mirror FabricPool

È possibile utilizzare la tecnologia mirror FabricPool per sostituire un archivio di oggetti con un altro. Il nuovo archivio di oggetti non deve utilizzare lo stesso provider cloud dell'archivio di oggetti originale.

### A proposito di questa attività

È possibile sostituire l'archivio di oggetti originale con un archivio di oggetti che utilizza un provider cloud diverso. Ad esempio, l'archivio di oggetti originale potrebbe utilizzare AWS come provider cloud, ma è possibile sostituirlo con un archivio di oggetti che utilizza Azure come provider cloud e viceversa. Tuttavia, il nuovo archivio di oggetti deve conservare le stesse dimensioni dell'oggetto originale.

### Fasi

1. Creare un mirror FabricPool aggiungendo un nuovo archivio di oggetti a un FabricPool esistente utilizzando `storage aggregate object-store mirror -aggregate` comando.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name my-AZURE-store
```

2. Monitorare lo stato di risincronizzazione del mirror utilizzando `storage aggregate object-store show-resync-status` comando.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
-----	-----	-----	-----
aggr1	my-AWS-store	my-AZURE-store	40%

3. Verificare che il mirror sia sincronizzato utilizzando `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded` comando.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-AWS-store	primary	-
	my-AZURE-store	mirror	false

4. Sostituire l'archivio di oggetti primario con l'archivio di oggetti mirror utilizzando `storage aggregate object-store modify` comando.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name my-AZURE-store -mirror-type primary
```

5. Visualizzare i dettagli relativi al mirror FabricPool utilizzando `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` comando.

In questo esempio vengono visualizzate le informazioni relative al mirror FabricPool, incluso se il mirror è danneggiato (non sincronizzato).

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-AZURE-store	primary	-
	my-AWS-store	mirror	false

6. Rimuovere il mirror FabricPool utilizzando `storage aggregate object-store unmirror` comando.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. Verificare che FabricPool sia di nuovo in una configurazione di archivio oggetti singolo utilizzando `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` comando.



```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-AZURE-store	primary	-

## Sostituire un mirror FabricPool in una configurazione MetroCluster

Se uno degli archivi di oggetti in un mirror FabricPool viene distrutto o diventa permanentemente non disponibile in una configurazione MetroCluster, è possibile rendere l'archivio di oggetti il mirror se non è già il mirror, rimuovere l'archivio di oggetti danneggiato dal mirror FabricPool, Quindi aggiungere un nuovo mirror dell'archivio di oggetti a FabricPool.

### Fasi

1. Se l'archivio di oggetti danneggiato non è già il mirror, fare in modo che l'oggetto memorizzi il mirror con `storage aggregate object-store modify` comando.

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01  
-name mccl_ostore1 -mirror-type mirror
```

2. Rimuovere il mirror dell'archivio di oggetti da FabricPool utilizzando `storage aggregate object-store unmirror` comando.

```
storage aggregate object-store unmirror -aggregate <aggregate name>  
-name mccl_ostore1
```

3. È possibile forzare il ripristino del tiering nell'archivio dati principale dopo aver rimosso l'archivio dati mirror utilizzando `storage aggregate object-store modify` con `-force-tiering-on-metrocluster true` opzione.

L'assenza di un mirror interferisce con i requisiti di replica di una configurazione MetroCluster.

```
storage aggregate object-store modify -aggregate <aggregate name> -name  
mccl_ostore1 -force-tiering-on-metrocluster true
```

4. Creare un archivio di oggetti sostitutivo utilizzando `storage aggregate object-store config create` comando.

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. Aggiungere il mirror dell'archivio di oggetti al mirror FabricPool utilizzando `storage aggregate object-store mirror` comando.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. Visualizzare le informazioni sull'archivio di oggetti utilizzando `storage aggregate object-store show` comando.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	mcc1_ostore1-mc	primary	-
	mcc1_ostore3-mc	mirror	true

7. Monitorare lo stato di risincronizzazione del mirror utilizzando `storage aggregate object-store show-resync-status` comando.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
aggr1	mcc1_ostore1-mc	mcc1_ostore3-mc	40%

## Comandi per la gestione degli aggregati con FabricPool

Si utilizza `storage aggregate object-store` Comandi per gestire gli archivi di oggetti per FabricPool. Si utilizza `storage aggregate` Comandi per gestire gli aggregati per FabricPool. Si utilizza `volume` Comandi per gestire i volumi per FabricPool.

Se si desidera...	Utilizzare questo comando:
Definire la configurazione per un archivio di oggetti in modo che ONTAP possa accedervi	<code>storage aggregate object-store config create</code>
Modificare gli attributi di configurazione dell'archivio di oggetti	<code>storage aggregate object-store config modify</code>
Rinominare una configurazione dell'archivio di oggetti esistente	<code>storage aggregate object-store config rename</code>
Eliminare la configurazione di un archivio di oggetti	<code>storage aggregate object-store config delete</code>
Visualizzare un elenco di configurazioni dell'archivio di oggetti	<code>storage aggregate object-store config show</code>
Collegare un secondo archivio di oggetti a un FabricPool nuovo o esistente come mirror	<code>storage aggregate object-store mirror</code> con <code>-aggregate</code> e <code>-name</code> nel livello di privilegio <b>admin</b>
Rimuovere un mirror dell'archivio di oggetti da un mirror FabricPool esistente	<code>storage aggregate object-store unmirror</code> con <code>-aggregate</code> e <code>-name</code> nel livello di privilegio <b>admin</b>
Monitorare lo stato di risincronizzazione del mirror FabricPool	<code>storage aggregate object-store show-resync-status</code>
Visualizza i dettagli del mirror FabricPool	<code>storage aggregate object-store show</code>
Promuovere un mirror dell'archivio di oggetti per sostituire un archivio di oggetti primario in una configurazione mirror FabricPool	<code>storage aggregate object-store modify</code> con <code>-aggregate</code> nel livello di privilegio <b>admin</b>
Verificare la latenza e le performance di un archivio di oggetti senza collegare l'archivio di oggetti a un aggregato	<code>storage aggregate object-store profiler start</code> con <code>-object-store-name</code> e <code>-node</code> nel livello di privilegio <b>avanzato</b>
Monitorare lo stato del profiler dell'archivio di oggetti	<code>storage aggregate object-store profiler show</code> con <code>-object-store-name</code> e <code>-node</code> nel livello di privilegio <b>avanzato</b>
Interrompere il profiler dell'archivio di oggetti quando è in esecuzione	<code>storage aggregate object-store profiler abort</code> con <code>-object-store-name</code> e <code>-node</code> nel livello di privilegio <b>avanzato</b>

Collegare un archivio di oggetti a un aggregato per utilizzare FabricPool	<code>storage aggregate object-store attach</code>
Collegare un archivio di oggetti a un aggregato che contiene un volume FlexGroup per l'utilizzo di FabricPool	<code>storage aggregate object-store attach</code> <code>con allow-flexgroup true</code>
Visualizza i dettagli degli archivi di oggetti collegati agli aggregati abilitati per FabricPool	<code>storage aggregate object-store show</code>
Visualizza la soglia di fullness aggregata utilizzata dalla scansione di tiering	<code>storage aggregate object-store show</code> <b>con</b> <code>-fields tiering-fullness-threshold</code> <b>nel</b> <b>livello di privilegio avanzato</b>
Visualizza l'utilizzo dello spazio degli archivi di oggetti collegati agli aggregati abilitati per FabricPool	<code>storage aggregate object-store show-</code> <code>space</code>
Attiva la creazione di report dei dati inattivi su un aggregato non utilizzato per FabricPool	<code>storage aggregate modify</code> <b>con</b> <code>-is-inactive-</code> <code>-data-reporting-enabled true</code> <b>parametro</b>
Visualizza se il reporting dei dati inattivi è attivato su un aggregato	<code>storage aggregate show</code> <b>con</b> <code>-fields is-</code> <code>inactive-data-reporting-enabled</code> <b>parametro</b>
Visualizza le informazioni sulla quantità di dati utente a freddo all'interno di un aggregato	<code>storage aggregate show-space</code> <b>con</b> <code>-fields</code> <code>performance-tier-inactive-user-</code> <code>data,performance-tier-inactive-user-</code> <code>data-percent</code> <b>parametro</b>
Creare un volume per FabricPool, specificando quanto segue: <ul style="list-style-type: none"> <li>• La policy di tiering</li> <li>• Il periodo di raffreddamento minimo di tiering (per <code>snapshot-only</code> oppure <code>auto policy di tiering</code>)</li> </ul>	<code>volume create</code> <ul style="list-style-type: none"> <li>• Si utilizza <code>-tiering-policy</code> parametro per specificare il criterio di tiering.</li> <li>• Si utilizza <code>-tiering-minimum-cooling-days</code> nel livello di privilegio avanzato per specificare il periodo minimo di raffreddamento del tiering.</li> </ul>
Modificare un volume per FabricPool, modificando quanto segue: <ul style="list-style-type: none"> <li>• La policy di tiering</li> <li>• Il periodo di raffreddamento minimo di tiering (per <code>snapshot-only</code> oppure <code>auto policy di tiering</code>)</li> </ul>	<code>volume modify</code> <ul style="list-style-type: none"> <li>• Si utilizza <code>-tiering-policy</code> parametro per specificare il criterio di tiering.</li> <li>• Si utilizza <code>-tiering-minimum-cooling-days</code> nel livello di privilegio avanzato per specificare il periodo minimo di raffreddamento del tiering.</li> </ul>

Visualizzare le informazioni FabricPool relative a un volume, tra cui: <ul style="list-style-type: none"> <li>• Il periodo di raffreddamento minimo di tiering</li> <li>• Quanti dati utente sono cold</li> </ul>	<p><code>volume show</code></p> <ul style="list-style-type: none"> <li>• Si utilizza <code>-fields tiering-minimum-cooling-days</code> nel livello di privilegio avanzato per visualizzare il periodo minimo di raffreddamento del tiering.</li> <li>• Si utilizza <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> parametro per visualizzare la quantità di dati utente a freddo.</li> </ul>
Consente di spostare un volume in entrata o in uscita da FabricPool	<p><code>volume move start</code> Si utilizza <code>-tiering-policy</code> parametro facoltativo per specificare il criterio di tiering per il volume.</p>
Modificare la soglia per recuperare lo spazio senza riferimento (la soglia di deframmentazione) per FabricPool	<p><code>storage aggregate object-store modify</code> con <code>-unreclaimed-space-threshold</code> nel livello di privilegio avanzato</p>
<p>Modificare la soglia per la percentuale di pieno che l'aggregato diventa prima che la scansione del tiering inizi a tiering dei dati per FabricPool</p> <p>FabricPool continua a eseguire il tiering dei dati cold su un Tier cloud fino a quando il Tier locale non raggiunge il 98% della capacità.</p>	<p><code>storage aggregate object-store modify</code> con <code>-tiering-fullness-threshold</code> nel livello di privilegio avanzato</p>
Visualizza la soglia per il recupero dello spazio senza riferimento per FabricPool	<p><code>storage aggregate object-store show</code> oppure <code>storage aggregate object-store show-space</code> con il <code>-unreclaimed-space-threshold</code> nel livello di privilegio avanzato</p>

## Mobilità dei dati SVM

### Panoramica sulla mobilità dei dati SVM

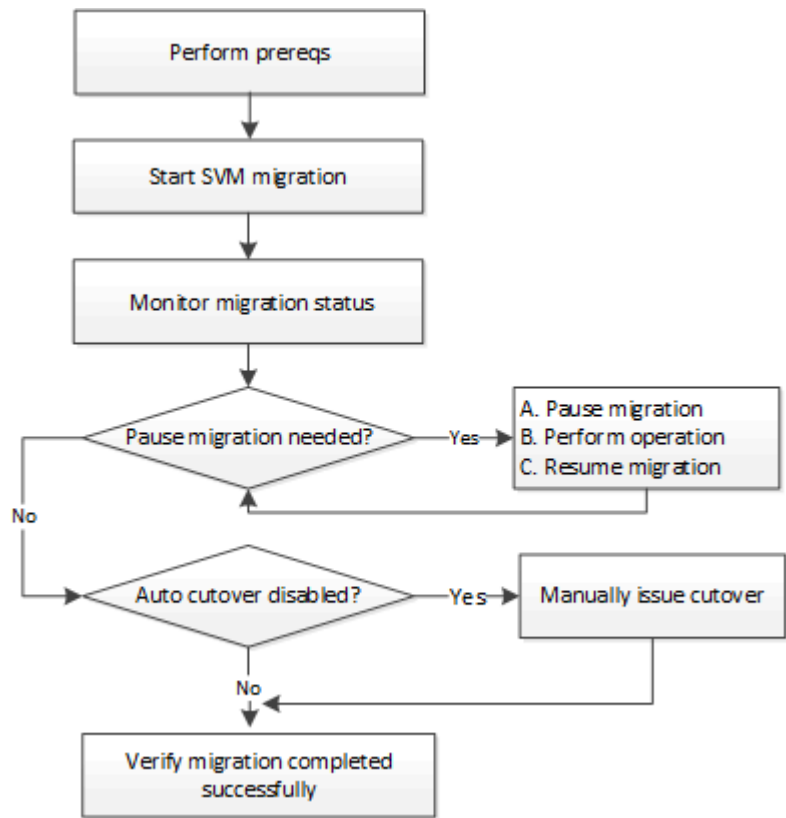
A partire da ONTAP 9.10.1, gli amministratori del cluster possono spostare senza interruzioni una SVM da un cluster di origine a un cluster di destinazione per gestire il bilanciamento della capacità e del carico, oppure per abilitare gli aggiornamenti delle apparecchiature o il consolidamento del data center utilizzando la CLI ONTAP.

Questa funzionalità di trasferimento SVM senza interruzioni è supportata sulle piattaforme AFF in ONTAP 9.10.1 e 9.11.1. A partire da ONTAP 9.12.1, questa funzionalità è supportata su piattaforme FAS e AFF e su aggregati ibridi.

Il nome e l'UUID di SVM rimangono invariati dopo la migrazione, oltre al nome LIF dei dati, all'indirizzo IP e ai nomi degli oggetti, come il nome del volume. L'UUID degli oggetti nella SVM sarà diverso.

Workflow di migrazione SVM

Il diagramma illustra il tipico flusso di lavoro per una migrazione SVM. Viene avviata una migrazione SVM dal cluster di destinazione. È possibile monitorare la migrazione dall'origine o dalla destinazione. È possibile eseguire un cutover manuale o automatico. Per impostazione predefinita viene eseguito un cutover automatico.



Supporto della piattaforma di migrazione SVM

Famiglia di controller	Versioni di ONTAP supportate
AFF serie A.	ONTAP 9.10.1 e versioni successive
AFF serie C.	ONTAP 9.12.1 patch 4 e versioni successive
FAS	ONTAP 9.12.1 e versioni successive



Durante la migrazione da un cluster AFF a un cluster FAS con aggregati ibridi, il posizionamento automatico del volume tenderà di eseguire una corrispondenza simile a quella degli aggregati. Ad esempio, se il cluster di origine ha 60 volumi, il posizionamento del volume tenderà di trovare un aggregato AFF sulla destinazione per posizionare i volumi. In mancanza di spazio sufficiente sugli aggregati AFF, i volumi verranno collocati negli aggregati con dischi non flash.

Supporto della scalabilità tramite la versione di ONTAP

Versione di ONTAP	COPPIE HA in origine e destinazione
ONTAP 9.14.1	12
ONTAP 9.13.1	6

ONTAP 9.11.1	3
ONTAP 9.10.1	1

### Requisiti di performance dell'infrastruttura di rete per il tempo di round trip TCP (RTT) tra il cluster di origine e di destinazione

A seconda della versione di ONTAP installata sul cluster, la rete che collega i cluster di origine e di destinazione deve avere un tempo massimo di andata e ritorno, come indicato di seguito:

Versione di ONTAP	RTT massimo
ONTAP 9.12.1 e versioni successive	10 ms.
ONTAP 9.11.1 e versioni precedenti	2 ms.

### Volumi massimi supportati per SVM

Origine	Destinazione	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1 e versioni precedenti
AFF	AFF	400	200	100	100
FAS	FAS	80	80	80	N/A.
FAS	AFF	80	80	80	N/A.
AFF	FAS	80	80	80	N/A.

### Prerequisiti

Prima di iniziare una migrazione SVM, è necessario soddisfare i seguenti prerequisiti:

- Devi essere un amministratore del cluster.
- ["I cluster di origine e di destinazione devono essere connessi in peering l'uno all'altro"](#).
- I cluster di destinazione e di origine devono avere SnapMirror sincrono ["licenza installata"](#). Questa licenza è inclusa con ["ONTAP uno"](#).
- Tutti i nodi nel cluster di origine devono eseguire ONTAP 9.10.1 o versione successiva. Per informazioni sul supporto specifico dei controller di array ONTAP, vedere ["Hardware Universe"](#).
- Tutti i nodi nel cluster di origine devono eseguire la stessa versione di ONTAP.
- Tutti i nodi nel cluster di destinazione devono eseguire la stessa versione di ONTAP.
- Il cluster di destinazione deve essere uguale o non più di due importanti versioni effettive del cluster (ECV) del cluster di origine.
- I cluster di origine e di destinazione devono supportare la stessa subnet IP per l'accesso ai dati LIF.
- La SVM di origine deve contenere meno di [numero massimo di volumi di dati supportati per la release](#).
- Sulla destinazione deve essere disponibile uno spazio sufficiente per il posizionamento del volume
- Onboard Key Manager deve essere configurato sulla destinazione se la SVM di origine ha volumi crittografati

## Best practice

Durante la migrazione delle SVM, è consigliabile lasciare il 30% di spazio a disposizione della CPU sia sul cluster di origine che su quello di destinazione per consentire l'esecuzione del workload della CPU.

## Operazioni SVM

È necessario controllare le operazioni che possono entrare in conflitto con una migrazione SVM:


- Non sono in corso operazioni di failover
- WAFLIRON non può essere in esecuzione
- Impronta digitale non in corso
- Vol move, rehosting, cloning, create, convert o analytics non sono in esecuzione


## Funzioni supportate e non supportate

La tabella indica le funzionalità di ONTAP supportate dalla mobilità dei dati SVM e le release di ONTAP in cui è disponibile il supporto.

Funzione	Release supportata per la prima volta	Commenti
Protezione ransomware autonoma	ONTAP 9.12.1	
Cloud Volumes ONTAP	Non supportato	
Gestore delle chiavi esterno	ONTAP 9.11.1	
FabricPool	ONTAP 9.11.1	Scopri di più <a href="#">Supporto FabricPool</a> .
Relazione fanout (l'origine della migrazione ha un volume di origine SnapMirror con più di una destinazione)	ONTAP 9.11.1	
SAN FC	Non supportato	
Flash Pool	ONTAP 9.12.1	
Volumi FlexCache	Non supportato	
FlexGroup	Non supportato	
Criteri IPsec	Non supportato	
LIF IPv6	Non supportato	



SAN iSCSI	Non supportato	
Replica della pianificazione del processo	ONTAP 9.11.1	In ONTAP 9.10.1, le pianificazioni dei processi non vengono replicate durante la migrazione e devono essere create manualmente sulla destinazione. A partire da ONTAP 9.11.1, le pianificazioni dei processi utilizzate dall'origine vengono replicate automaticamente durante la migrazione.
Mirror per la condivisione del carico	Non supportato	
SVM MetroCluster	Non supportato	Sebbene la migrazione SVM non supporti la migrazione MetroCluster SVM, potrebbe essere possibile utilizzare la replica asincrona SnapMirror in <a href="#">"Migrare una SVM in una configurazione MetroCluster"</a> . Tenere presente che il processo descritto per la migrazione di una SVM in una configurazione MetroCluster è <i>non</i> un metodo senza interruzioni.
NetApp aggregate Encryption (NAE)	Non supportato	La migrazione non è supportata da un'origine non crittografata a una destinazione crittografata.
Configurazioni NDMP	Non supportato	
NetApp Volume Encryption (NVE)	ONTAP 9.10.1	
Registri di audit NFS e SMB	ONTAP 9.13.1	<div>  <p>Il reindirizzamento dei log di audit è disponibile solo in modalità cloud. Per la migrazione delle SVM on-premise con audit abilitato, devi disabilitare l'audit sulla SVM di origine ed eseguire la migrazione.</p> </div> <p>Prima della migrazione SVM:</p> <ul style="list-style-type: none"> <li>• <a href="#">"Il reindirizzamento del log di audit deve essere abilitato sul cluster di destinazione"</a>.</li> <li>• <a href="#">"Occorre creare il percorso di destinazione dell'audit log dalla SVM di origine nel cluster di destinazione"</a>.</li> </ul>
NFS v3, NFS v4.1 e NFS v4.2	ONTAP 9.10.1	
NFS v4.0	ONTAP 9.12.1	
NFSv4,1 con pNFS	ONTAP 9.14.1	
NVMe su fabric	Non supportato	

Onboard Key Manager (OKM) con la modalità Common Criteria attivata sul cluster di origine	Non supportato	
Qtree	ONTAP 9.14.1	
Quote	ONTAP 9.14.1	
S3	Non supportato	
Protocollo SMB	ONTAP 9.12.1	Le migrazioni SMB sono un'interruzione e richiedono un refresh del client dopo la migrazione.
Relazioni di SnapMirror Cloud	ONTAP 9.12.1	A partire da ONTAP 9.12.1, per migrare una SVM con relazioni SnapMirror Cloud, il cluster di destinazione deve disporre di " <a href="#">Licenza SnapMirror Cloud</a> " installato e deve avere sufficiente capacità a disposizione per supportare lo spostamento della capacità nei volumi su cui viene eseguito il mirroring nel cloud.
Destinazione asincrona di SnapMirror	ONTAP 9.12.1	
Fonte asincrona di SnapMirror	ONTAP 9.11.1	<ul style="list-style-type: none"> <li>• I trasferimenti possono continuare normalmente sulle relazioni di FlexVol SnapMirror durante la maggior parte della migrazione.</li> <li>• Eventuali trasferimenti in corso vengono annullati durante il cutover e i nuovi trasferimenti falliscono durante il cutover e non possono essere riavviati fino al completamento della migrazione.</li> <li>• I trasferimenti pianificati che sono stati annullati o persi durante la migrazione non vengono avviati automaticamente al termine della migrazione.</li> </ul> <div>  <p>Al momento della migrazione di un'origine SnapMirror, ONTAP non impedisce la cancellazione del volume dopo la migrazione fino all'esecuzione dell'aggiornamento di SnapMirror. Questo si verifica perché le informazioni relative a SnapMirror per i volumi di origine di SnapMirror migrati sono disponibili solo al termine della migrazione e dopo il primo aggiornamento.</p> </div>
Impostazioni SMTape	Non supportato	
SnapLock	Non supportato	

Continuità aziendale di SnapMirror	Non supportato	
Relazioni peer di SnapMirror SVM	ONTAP 9.12.1	
Disaster recovery di SnapMirror SVM	Non supportato	
SnapMirror sincrono	Non supportato	
Copia Snapshot	ONTAP 9.10.1	
Blocco delle copie Snapshot a prova di manomissione	ONTAP 9.14.1	Il blocco delle copie Snapshot a prova di manomissione non è equivalente a SnapLock. SnapLock rimane non supportato.
LIF IP/BGP virtuali	Non supportato	
Virtual Storage Console 7.0 e versioni successive	Non supportato	VSC fa parte di <a href="#">"Strumenti ONTAP per appliance virtuali VMware vSphere"</a> A partire da VSC 7.0.
Cloni di volume	Non supportato	
VStorage	Non supportato	

### Supporto FabricPool

La migrazione SVM è supportata con i volumi su FabricPools per le seguenti piattaforme:

- Piattaforma Azure NetApp Files. Sono supportati tutti i criteri di tiering (solo snapshot, automatico, tutti e nessuno).
- Piattaforma on-premise. È supportato solo il criterio di tiering del volume "nessuno".

### Operazioni supportate durante la migrazione

La seguente tabella indica le operazioni di volume supportate nella SVM in migrazione in base allo stato di migrazione:

Funzionamento del volume	Stato di migrazione SVM		
	In corso	In pausa	Cutover
Creare	Non consentito	Consentito	Non supportato
Eliminare	Non consentito	Consentito	Non supportato
Disattivazione di file System Analytics	Consentito	Consentito	Non supportato
Attivazione di file System Analytics	Non consentito	Consentito	Non supportato
Modificare	Consentito	Consentito	Non supportato
Offline/Online	Non consentito	Consentito	Non supportato

Spostare/eseguire nuovamente l'host	Non consentito	Consentito	Non supportato
Creazione/modifica qtree	Non consentito	Consentito	Non supportato
Creazione/modifica quota	Non consentito	Consentito	Non supportato
Rinominare	Non consentito	Consentito	Non supportato
Ridimensionare	Consentito	Consentito	Non supportato
Limitare	Non consentito	Consentito	Non supportato
Modifica degli attributi della copia Snapshot	Consentito	Consentito	Non supportato
Modifica dell'eliminazione automatica della copia Snapshot	Consentito	Consentito	Non supportato
Creazione della copia Snapshot	Consentito	Consentito	Non supportato
Eliminazione della copia Snapshot	Consentito	Consentito	Non supportato
Ripristinare il file dalla copia Snapshot	Consentito	Consentito	Non supportato

## Migrare una SVM

Al termine di una migrazione SVM, i client vengono tagliati automaticamente nel cluster di destinazione e la SVM non necessaria viene rimossa dal cluster di origine. Il cutover automatico e il cleanup automatico della sorgente sono attivati per impostazione predefinita. Se necessario, è possibile disattivare il cutover automatico del client per sospendere la migrazione prima che si verifichi il cutover ed è anche possibile disattivare il cleanup SVM di origine automatico.

- È possibile utilizzare `-auto-cutover false` opzione per sospendere la migrazione quando normalmente si verifica il cutover automatico del client e quindi eseguire manualmente il cutover in un secondo momento.

### Cutover manuale dei client dopo la migrazione SVM

- È possibile utilizzare il privilegio Advance `-auto-source-cleanup false` Opzione per disattivare la rimozione della SVM di origine dopo il cutover e quindi attivare manualmente la pulitura della sorgente in un secondo momento, dopo il cutover.

### Rimuovere manualmente la SVM di origine dopo il cutover

## Migrare una SVM con il cutover automatico attivato

Per impostazione predefinita, i client vengono tagliati automaticamente nel cluster di destinazione al termine della migrazione e la SVM non necessaria viene rimossa dal cluster di origine.

### Fasi

1. Dal cluster di destinazione, eseguire i controlli preliminari per la migrazione:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster
cluster_name -check-only true
```

2. Dal cluster di destinazione, avviare la migrazione SVM:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster cluster_name
```

3. Controllare lo stato della migrazione:

```
dest_cluster> vserver migrate show
```

Lo stato visualizza Migrate-complete (migrazione completata) al termine della migrazione SVM.

### Migrare una SVM con il cutover automatico del client disattivato

È possibile utilizzare l'opzione `-auto-cutover false` per sospendere la migrazione quando si verifica normalmente un cutover automatico del client e quindi eseguire manualmente il cutover in un secondo momento. Vedere [Cutover manuale dei client dopo la migrazione SVM](#).

#### Fasi

1. Dal cluster di destinazione, eseguire i controlli preliminari per la migrazione:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster cluster_name -check-only true
```

2. Dal cluster di destinazione, avviare la migrazione SVM:

```
dest_cluster> vserver migrate start -vserver SVM_name -source-cluster cluster_name -auto-cutover false
```

3. Controllare lo stato della migrazione:

```
`dest_cluster> vserver migrate show`
```

Lo stato visualizza Ready-for-cutover quando la migrazione SVM completa i trasferimenti di dati asincroni ed è pronta per l'operazione di cutover.

### Migrazione di una SVM con pulitura origine disattivata

È possibile utilizzare l'opzione `Advance Privilege -auto-source-cleanup false` per disattivare la rimozione della SVM di origine dopo il cutover e quindi attivare manualmente la pulitura della sorgente in un secondo momento, dopo il cutover. Vedere [Rimuovere manualmente SVM di origine](#).

#### Fasi

1. Dal cluster di destinazione, eseguire i controlli preliminari per la migrazione:

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster cluster_name -check-only true
```

2. Dal cluster di destinazione, avviare la migrazione SVM:

```
dest_cluster*> vserver migrate start -vserver SVM_name -source-cluster cluster_name -auto-source-cleanup false
```

3. Controllare lo stato della migrazione:

```
dest_cluster*> vserver migrate show
```

Lo stato visualizza Ready-for-source-cleanup quando la migrazione SVM è completa ed è pronto per rimuovere SVM sul cluster di origine.

## Monitorare la migrazione dei volumi

Oltre a monitorare la migrazione SVM complessiva con `vserver migrate show` È possibile monitorare lo stato di migrazione dei volumi contenuti nella SVM.

### Fasi

1. Controllare lo stato della migrazione del volume:

```
dest_clust> vserver migrate show-volume
```

## Sospendere e riprendere la migrazione SVM

Potrebbe essere necessario sospendere una migrazione SVM prima dell'inizio del cutover della migrazione. È possibile sospendere una migrazione SVM utilizzando `vserver migrate pause` comando.

### Sospendere la migrazione

È possibile sospendere una migrazione SVM prima dell'avvio del cutover del client utilizzando `vserver migrate pause` comando.

Alcune modifiche alla configurazione sono limitate quando è in corso un'operazione di migrazione; tuttavia, a partire da ONTAP 9.12.1, è possibile sospendere una migrazione per correggere alcune configurazioni limitate e alcuni stati non riusciti, in modo da risolvere i problemi di configurazione che potrebbero aver causato l'errore. Alcuni degli stati di errore che è possibile correggere quando si interrompe la migrazione SVM includono:

- setup-configuration-failed. (configurazione non riuscita.
- migrazione non riuscita

### Fasi

1. Dal cluster di destinazione, sospendere la migrazione:

```
dest_cluster> vserver migrate pause -vserver <vserver name>
```

### Riprendere le migrazioni

Quando si è pronti a riprendere una migrazione SVM in pausa o quando una migrazione SVM non è riuscita, è possibile utilizzare `vserver migrate resume` comando.

### Fase

1. Riprendere la migrazione SVM:

```
dest_cluster> vserver migrate resume
```

2. Verificare che la migrazione SVM sia stata ripresa e monitorare l'avanzamento:

```
dest_cluster> vserver migrate show
```

## Annullare una migrazione SVM

Se è necessario annullare una migrazione SVM prima del completamento, è possibile utilizzare `vserver migrate abort` comando. È possibile annullare una migrazione SVM solo quando l'operazione è in stato di pausa o non riuscita. Non è possibile annullare una migrazione SVM quando lo stato è "cutover-started" (cutover avviato) o dopo il completamento del cutover. Non è possibile utilizzare `abort` Opzione quando è in corso una migrazione SVM.

### Fasi

1. Controllare lo stato della migrazione:

```
dest_cluster> vserver migrate show -vserver <vserver name>
```

2. Annullare la migrazione:

```
dest_cluster> vserver migrate abort -vserver <vserver name>
```

3. Verificare l'avanzamento dell'operazione di annullamento:

```
dest_cluster> vserver migrate show
```

Lo stato della migrazione mostra l'interruzione della migrazione mentre l'operazione di annullamento è in corso. Al termine dell'operazione di annullamento, lo stato della migrazione non mostra nulla.

## Tagliare manualmente i client

Per impostazione predefinita, il cutover del client al cluster di destinazione viene eseguito automaticamente quando la migrazione SVM raggiunge lo stato "ready-for-cutover". Se si sceglie di disattivare il cutover automatico del client, è necessario eseguire manualmente il cutover del client.

### Fasi

1. Eseguire manualmente il cutover del client:

```
dest_cluster> vserver migrate cutover -vserver <vserver name>
```

2. Controllare lo stato dell'operazione di cutover:

```
dest_cluster> vserver migrate show
```

## Rimuovere manualmente la SVM di origine dopo il cutover del client

Se è stata eseguita la migrazione SVM con la pulitura del codice sorgente disattivata, è possibile rimuovere manualmente la SVM di origine al termine del cutover del client.

### Fasi

1. Verificare che lo stato sia pronto per la pulizia della sorgente:

```
dest_cluster> vsserver migrate show
```

2. Pulire la fonte:

```
dest_cluster> vsserver migrate source-cleanup -vsserver <vsserver_name>
```

## Gestione delle coppie HA

### Panoramica sulla gestione delle coppie HA

I nodi del cluster sono configurati in coppie ad alta disponibilità (ha) per la fault tolerance e le operazioni senza interruzioni. Se un nodo si guasta o se è necessario interrompere un nodo per la manutenzione ordinaria, il partner può assumere il controllo dello storage e continuare a fornire i dati da esso. Il partner restituisce lo storage quando il nodo viene riportato on-line.

La configurazione del Pair Controller ha è costituita da una coppia di storage controller FAS/AFF corrispondenti (nodo locale e nodo partner). Ciascuno di questi nodi è collegato agli shelf di dischi dell'altro. Quando un nodo di una coppia ha rileva un errore e interrompe l'elaborazione dei dati, il partner rileva lo stato di errore del partner e rileva tutte le elaborazioni dei dati da quel controller.

*Takeover* è il processo in cui un nodo assume il controllo dello storage del partner.

*Giveback* è il processo in cui lo storage viene restituito al partner.

Per impostazione predefinita, i takeover si verificano automaticamente in una delle seguenti situazioni:

- Si verifica un errore di software o di sistema su un nodo che porta a un panico. I controller di coppia ha eseguono automaticamente il failover nel nodo partner. Una volta che il partner si è ripristinato dal panico e si è avviato, il nodo esegue automaticamente un giveback, riportando il partner al normale funzionamento.
- Si verifica un errore di sistema su un nodo e il nodo non può essere riavviato. Ad esempio, quando un nodo si guasta a causa di una perdita di alimentazione, i controller di coppia ha eseguono automaticamente il failover nel nodo partner e distribuiscono i dati dal controller di storage sopravvissuto.



Se anche lo storage di un nodo perde alimentazione contemporaneamente, non è possibile eseguire un takeover standard.

- I messaggi heartbeat non vengono ricevuti dal partner del nodo. Ciò potrebbe verificarsi se il partner ha riscontrato un errore hardware o software (ad esempio, un errore di interconnessione) che non ha causato panico ma ha comunque impedito il corretto funzionamento.
- Arrestare uno dei nodi senza utilizzare `-f` oppure `-inhibit-takeover true` parametro.



In un cluster a due nodi con cluster ha attivato, arrestare o riavviare un nodo utilizzando `-inhibit-takeover true` Il parametro causa l'interruzione della fornitura dei dati da parte di entrambi i nodi, a meno che non venga prima disattivata la disponibilità del cluster e quindi assegnata l'epsilon al nodo che si desidera mantenere in linea.

- Riavviare uno dei nodi senza utilizzare `-inhibit-takeover true` parametro. (Il `-onboot` del parametro



`storage failover` il comando è attivato per impostazione predefinita).

- Il dispositivo di gestione remota (Service Processor) rileva un errore del nodo partner. Questa opzione non è applicabile se si disattiva il Takeover assistito dall'hardware.

È inoltre possibile avviare manualmente le operazioni di takeover con `storage failover takeover` comando.

## Resilienza del cluster e miglioramenti diagnostici

A partire da ONTAP 9,9.1, le seguenti aggiunte di resilienza e diagnostica migliorano il funzionamento del cluster:

- **Monitoraggio ed esclusione delle porte:** Nelle configurazioni cluster senza switch a due nodi, il sistema evita le porte che subiscono la perdita totale dei pacchetti (perdita di connettività). In ONTAP 9.8.1 e versioni precedenti, questa funzionalità era disponibile solo nelle configurazioni con switch.
- **Failover automatico dei nodi:** Se un nodo non è in grado di fornire dati attraverso la rete cluster, tale nodo non deve possedere alcun disco. Il partner ha dovrebbe invece assumere il controllo, se il partner è in buona salute.
- **Comandi per analizzare i problemi di connettività:** Utilizzare il seguente comando per visualizzare i percorsi del cluster in cui si verificano perdite di pacchetti: `network interface check cluster-connectivity show`

## Come funziona il Takeover assistito dall'hardware

Attivata per impostazione predefinita, la funzione di Takeover assistita dall'hardware può accelerare il processo di Takeover utilizzando il dispositivo di gestione remota di un nodo (Service Processor).

Quando il dispositivo di gestione remota rileva un guasto, avvia rapidamente il rilevamento piuttosto che attendere che ONTAP riconosca che il battito cardiaco del partner si è arrestato. Se si verifica un errore senza che questa funzione sia attivata, il partner attende fino a quando non rileva che il nodo non sta più dando un heartbeat, conferma la perdita di heartbeat, quindi avvia il takeover.

La funzionalità di Takeover assistita dall'hardware utilizza il seguente processo per evitare tale attesa:

1. Il dispositivo di gestione remota monitora il sistema locale per rilevare determinati tipi di guasti.
2. Se viene rilevato un errore, il dispositivo di gestione remota invia immediatamente un avviso al nodo partner.
3. Una volta ricevuto l'avviso, il partner avvia la presa in consegna.

## Eventi di sistema che attivano il Takeover assistito dall'hardware

Il nodo partner potrebbe generare un Takeover a seconda del tipo di avviso ricevuto dal dispositivo di gestione remota (Service Processor).

Avviso	Acquisizione avviata al ricevimento?	Descrizione
<code>abnormal_reboot</code>	No	Si è verificato un riavvio anomalo del nodo.

l2_watchdog_reset	Sì	L'hardware del watchdog di sistema ha rilevato un ripristino L2. Il dispositivo di gestione remota ha rilevato una mancanza di risposta dalla CPU di sistema e ha ripristinato il sistema.
perdita di heartbeat	No	Il dispositivo di gestione remota non riceve più il messaggio heartbeat dal nodo. Questo avviso non fa riferimento ai messaggi heartbeat tra i nodi della coppia; si riferisce al heartbeat tra il nodo e il dispositivo di gestione remota locale.
messaggio_periodico	No	Viene inviato un messaggio periodico durante una normale operazione di Takeover assistita dall'hardware.
power_cycle_via_sp	Sì	Il dispositivo di gestione remota ha spento e riaccessato il sistema.
power_loss	Sì	Si è verificata una perdita di alimentazione nel nodo. Il dispositivo di gestione remota dispone di un alimentatore che mantiene l'alimentazione per un breve periodo dopo un'interruzione dell'alimentazione, consentendo di segnalare al partner l'interruzione dell'alimentazione.
power_off_via_sp	Sì	Il dispositivo di gestione remota ha spento il sistema.
reset_via_sp	Sì	Il dispositivo di gestione remota ripristina il sistema.
test	No	Viene inviato un messaggio di test per verificare un'operazione di Takeover assistita dall'hardware.

## Come funziona il Takeover e il giveback automatico

Le operazioni automatiche di Takeover e giveback possono lavorare insieme per ridurre ed evitare le interruzioni dei client.

Per impostazione predefinita, se un nodo della coppia ha eseguito il panic, il riavvio o l'arresto, il nodo partner assume automaticamente il controllo e restituisce lo storage al riavvio del nodo interessato. La coppia ha ripreso quindi uno stato operativo normale.

Le acquisizioni automatiche possono verificarsi anche se uno dei nodi non risponde.

Il giveback automatico viene eseguito per impostazione predefinita. Se si desidera controllare l'impatto del giveback sui client, è possibile disattivare il giveback automatico e utilizzare `storage failover modify -auto-giveback false -node <node>` comando. Prima di eseguire il giveback automatico (indipendentemente da ciò che lo ha attivato), il nodo partner attende un periodo di tempo fisso, come controllato da `-delay- seconds` del parametro `storage failover modify` comando. Il ritardo predefinito è di 600 secondi. Ritardando il giveback, il processo si traduce in due brevi interruzioni: Una durante il takeover e una durante il giveback.

Questo processo evita un singolo e prolungato disservizio che include il tempo necessario per:

- Operazione di Takeover
- Il nodo preso in consegna per l'avvio fino al punto in cui è pronto per il giveback

- L'operazione di giveback

Se il giveback automatico non riesce per uno qualsiasi degli aggregati non root, il sistema effettua automaticamente due tentativi aggiuntivi per completare il giveback.



Durante il processo di takeover, il processo di giveback automatico inizia prima che il nodo partner sia pronto per il giveback. Quando il limite di tempo del processo di giveback automatico scade e il nodo partner non è ancora pronto, il timer viene riavviato. Di conseguenza, il tempo che intercorre tra il nodo partner pronto e l'effettivo giveback eseguito potrebbe essere inferiore al tempo di giveback automatico.

## Cosa succede durante il takeover

Quando un nodo assume il controllo del proprio partner, continua a fornire e aggiornare i dati negli aggregati e nei volumi del partner.

Durante il processo di Takeover si verificano le seguenti fasi:

1. Se il Takeover negoziato è avviato dall'utente, i dati aggregati vengono spostati dal nodo partner al nodo che sta eseguendo il Takeover. Una breve interruzione si verifica quando il proprietario corrente di ciascun aggregato (ad eccezione dell'aggregato root) passa al nodo di Takeover. Questa interruzione è più breve di un'interruzione che si verifica durante un'acquisizione senza ricollocazione aggregata.



Un takeover negoziato durante il panico non può verificarsi in caso di panico. Un takeover può derivare da un errore non associato a un panico. Si verifica un errore quando la comunicazione tra un nodo e il suo partner viene persa, chiamata anche perdita heartbeat. In caso di takeover a causa di un guasto, l'interruzione potrebbe essere più lunga poiché il nodo partner ha bisogno di tempo per rilevare la perdita di heartbeat.

- È possibile monitorare l'avanzamento utilizzando `storage failover show-takeover` comando.
- È possibile evitare il trasferimento dell'aggregato durante questa istanza di Takeover utilizzando `-bypass-optimization` con il `storage failover takeover` comando.

Gli aggregati vengono ricollocati in modo seriale durante le operazioni di Takeover pianificate per ridurre l'interruzione del servizio del client. Se il trasferimento aggregato viene ignorato, si verifica un'interruzione più lunga del client durante gli eventi di acquisizione pianificati.

2. Se il Takeover avviato dall'utente è un Takeover negoziato, il nodo di destinazione si spegne senza problemi, seguito dal Takeover dell'aggregato root del nodo di destinazione e degli aggregati che non sono stati ricollocati nella fase 1.
3. Le interfacce logiche (LIF) dei dati migrano dal nodo di destinazione al nodo di takeover o a qualsiasi altro nodo del cluster in base alle regole di failover della LIF. È possibile evitare la migrazione LIF utilizzando `-skip-lif-migration` con il `storage failover takeover` comando. In caso di takeover avviato dall'utente, le LIF dati vengono migrate prima dell'inizio del takeover dello storage. In caso di panico o guasto, le LIF dati e lo storage vengono migrati insieme.
4. Le sessioni SMB esistenti vengono disconnesse quando si verifica il takeover.



A causa della natura del protocollo SMB, tutte le sessioni SMB vengono interrotte (ad eccezione delle sessioni SMB 3.0 connesse alle condivisioni con il set di proprietà Continuous Availability). Le sessioni SMB 1.0 e SMB 2.x non possono riconnettersi dopo un evento di Takeover; pertanto, il Takeover è un'interruzione e potrebbe verificarsi una perdita di dati.

5. Le sessioni SMB 3.0 stabilite per le condivisioni con la proprietà disponibilità continua attivata possono riconnettersi alle condivisioni disconnesse dopo un evento di Takeover. Se il sito utilizza connessioni SMB 3.0 a Microsoft Hyper-V e la proprietà disponibilità continua è attivata sulle condivisioni associate, le acquisizioni non sono disruptive per tali sessioni.

#### **Cosa succede se un nodo che esegue una panoramica di Takeover**

Se il nodo che esegue il takeover esegue il panic entro 60 secondi dall'inizio del takeover, si verificano i seguenti eventi:

- Il nodo che ha avviato il panico si riavvia.
- Dopo il riavvio, il nodo esegue le operazioni di ripristino automatico e non è più in modalità Takeover.
- Il failover è disattivato.
- Se il nodo possiede ancora alcuni aggregati del partner, dopo aver attivato il failover dello storage, restituire questi aggregati al partner utilizzando `storage failover giveback` comando.

#### **Cosa succede durante il giveback**

Il nodo locale restituisce la proprietà al nodo partner quando i problemi vengono risolti, quando il nodo partner si avvia o quando viene avviato il giveback.

Il seguente processo viene eseguito in una normale operazione di giveback. In questa discussione, il nodo A ha assunto il controllo del nodo B. Tutti i problemi sul nodo B sono stati risolti ed è pronto per riprendere la fornitura dei dati.

1. Tutti i problemi sul nodo B vengono risolti e viene visualizzato il seguente messaggio: `Waiting for giveback`
2. Il giveback viene avviato da `storage failover giveback` o tramite giveback automatico se il sistema è configurato per esso. Questo avvia il processo di restituzione della proprietà degli aggregati e dei volumi del nodo B dal nodo A al nodo B.
3. Il nodo A restituisce prima il controllo dell'aggregato root.
4. Il nodo B completa il processo di avvio fino al suo normale stato operativo.
5. Non appena il nodo B raggiunge il punto del processo di boot in cui può accettare gli aggregati non root, il nodo A restituisce la proprietà degli altri aggregati, uno alla volta, fino al completamento del giveback. È possibile monitorare l'avanzamento del giveback utilizzando `storage failover show-giveback` comando.



Il `storage failover show-giveback command` non visualizza (né intende) informazioni su tutte le operazioni che si verificano durante l'operazione di giveback di failover dello storage. È possibile utilizzare `storage failover show` per visualizzare ulteriori dettagli sullo stato di failover corrente del nodo, ad esempio se il nodo è completamente funzionante, è possibile eseguire il takeover e il giveback è completo.

I/o riprende per ciascun aggregato dopo il completamento del giveback per quell'aggregato, riducendo così

la finestra generale di interruzione.

## Ha e il suo effetto sull'acquisizione e sul giveback

ONTAP assegna automaticamente a un aggregato una policy ha di CFO (failover del controller) e SFO (failover dello storage). Questo criterio determina il modo in cui avvengono le operazioni di failover dello storage per l'aggregato e i suoi volumi.

Le due opzioni, CFO e SFO, determinano la sequenza di controllo aggregata utilizzata da ONTAP durante le operazioni di giveback e failover dello storage.

Sebbene i termini CFO e SFO siano talvolta utilizzati in modo informale per fare riferimento alle operazioni di failover dello storage (takeover e giveback), essi rappresentano effettivamente la policy ha assegnata agli aggregati. Ad esempio, i termini aggregato SFO o aggregato CFO si riferiscono semplicemente all'assegnazione dei criteri ha dell'aggregato.

Le policy DI HA influiscono sulle operazioni di takeover e giveback come segue:

- Gli aggregati creati sui sistemi ONTAP (ad eccezione dell'aggregato root contenente il volume root) hanno una policy di ha di SFO. Il Takeover avviato manualmente è ottimizzato per le performance trasferendo gli aggregati SFO (non root) in modo seriale al partner prima del Takeover. Durante il processo di giveback, gli aggregati vengono restituiti in modo seriale dopo l'avvio del sistema acquisito e l'accesso alle applicazioni di gestione, consentendo al nodo di ricevere i propri aggregati.
- Poiché le operazioni di riposizionamento degli aggregati comportano la riassegnazione della proprietà dei dischi aggregati e lo spostamento del controllo da un nodo al suo partner, solo gli aggregati con una policy di ha di SFO sono idonei per il riposizionamento degli aggregati.
- L'aggregato root ha sempre una policy di ha di CFO e viene restituita all'inizio dell'operazione di giveback. Ciò è necessario per consentire l'avvio del sistema preso in consegna. Tutti gli altri aggregati vengono restituiti in modo seriale dopo che il sistema acquisito ha completato il processo di boot e le applicazioni di gestione sono online, consentendo al nodo di ricevere i propri aggregati.



La modifica della policy ha di un aggregato da SFO a CFO è un'operazione in modalità Maintenance. Non modificare questa impostazione a meno che non sia richiesto da un rappresentante dell'assistenza clienti.

## In che modo gli aggiornamenti in background influiscono su Takeover e giveback

Gli aggiornamenti in background del firmware del disco influiscono in modo diverso sulle operazioni di takeover, giveback e trasferimento degli aggregati della coppia ha, a seconda di come vengono avviate tali operazioni.

Il seguente elenco descrive come gli aggiornamenti del firmware dei dischi in background influiscono su Takeover, giveback e trasferimento degli aggregati:

- Se si verifica un aggiornamento del firmware del disco in background su un disco su uno dei nodi, le operazioni di Takeover avviate manualmente vengono ritardate fino al completamento dell'aggiornamento del firmware del disco su tale disco. Se l'aggiornamento del firmware del disco in background richiede più di 120 secondi, le operazioni di Takeover vengono interrotte e devono essere riavviate manualmente al termine dell'aggiornamento del firmware del disco. Se l'acquisizione è stata avviata con `-bypass -optimization` del parametro `storage failover takeover` comando impostato su `true`, l'aggiornamento del firmware del disco in background che si verifica sul nodo di destinazione non influisce sul takeover.

- Se si verifica un aggiornamento del firmware del disco in background su un disco nel nodo di origine (o Takeover) e il Takeover è stato avviato manualmente con `-options` del parametro `storage failover takeover` comando impostato su `immediate`, le operazioni di takeover iniziano immediatamente.
- Se si verifica un aggiornamento del firmware del disco in background su un disco di un nodo e si verifica una situazione di panico, l'acquisizione del nodo in pannello inizia immediatamente.
- Se si verifica un aggiornamento del firmware del disco in background su un disco su uno dei nodi, il giveback degli aggregati di dati viene ritardato fino al completamento dell'aggiornamento del firmware del disco su tale disco.
- Se l'aggiornamento del firmware del disco in background richiede più di 120 secondi, le operazioni di giveback vengono interrotte e devono essere riavviate manualmente al termine dell'aggiornamento del firmware del disco.
- Se si verifica un aggiornamento del firmware del disco in background su un disco di uno dei nodi, le operazioni di trasferimento aggregato vengono ritardate fino al completamento dell'aggiornamento del firmware del disco su tale disco. Se l'aggiornamento del firmware del disco in background richiede più di 120 secondi, le operazioni di trasferimento aggregato vengono interrotte e devono essere riavviate manualmente al termine dell'aggiornamento del firmware del disco. Se è stato avviato il trasferimento di aggregati con `-override-destination-checks` di `storage aggregate relocation` comando impostato su `true`, l'aggiornamento del firmware del disco in background che si verifica sul nodo di destinazione non influisce sul trasferimento dell'aggregato.

## Comandi di Takeover automatico

Il Takeover automatico è attivato per impostazione predefinita su tutte le piattaforme NetApp FAS, AFF e ASA supportate. Potrebbe essere necessario modificare il comportamento e il controllo predefiniti quando si verificano ripristini automatici quando il nodo partner si riavvia, esegue una panoramica o si arresta.

Se si desidera che l'acquisizione avvenga automaticamente quando il nodo partner...	Utilizzare questo comando...
Si riavvia o si arresta	<code>storage failover modify -node nodename -onreboot true</code>
Panoramica	<code>storage failover modify -node nodename -onpanic true</code>

## Attivare la notifica via email se la funzionalità di Takeover è disattivata

Per ricevere una notifica rapida in caso di disattivazione della funzionalità di Takeover, configurare il sistema in modo da abilitare la notifica automatica via email per i messaggi EMS "Takeover impossible":

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`

- `ha.takeoverImpNotDef`

## Comandi di giveback automatici

Per impostazione predefinita, il nodo partner take-over restituisce automaticamente lo storage quando il nodo off-line viene riportato in linea, ripristinando così la relazione di coppia ad alta disponibilità. Nella maggior parte dei casi, questo è il comportamento desiderato. Se è necessario disattivare il giveback automatico, ad esempio se si desidera esaminare la causa del takeover prima di restituirgli, è necessario essere consapevoli dell'interazione delle impostazioni non predefinite.

Se si desidera...	Utilizzare questo comando...
<p>Abilitare il giveback automatico in modo che il giveback avvenga non appena il nodo preso in consegna si avvia, raggiunga lo stato Waiting for Giveback (in attesa di giveback) e il periodo Delay before Auto Giveback (ritardo prima del giveback automatico) sia scaduto.</p> <p>L'impostazione predefinita è true.</p>	<pre>storage failover modify -node <i>nodename</i> -auto-giveback true</pre>
<p>Disattiva il giveback automatico. L'impostazione predefinita è true.</p> <p><b>Nota:</b> l'impostazione di questo parametro su false non disattiva il giveback automatico dopo il takeover in panic; il giveback automatico dopo il takeover in panic deve essere disattivato impostando il <code>-auto-giveback-after-panic</code> parametro su false.</p>	<pre>storage failover modify -node <i>nodename</i> -auto-giveback false</pre>
<p>Disattiva il giveback automatico dopo il takeover in panic (questa impostazione è attivata per impostazione predefinita).</p>	<pre>storage failover modify -node <i>nodename</i> -auto-giveback-after-panic false</pre>
<p>Ritarda il giveback automatico per un numero di secondi specificato (l'impostazione predefinita è 600). Questa opzione determina il tempo minimo in cui un nodo rimane in fase di Takeover prima di eseguire un giveback automatico.</p>	<pre>storage failover modify -node <i>nodename</i> -delay-seconds <i>seconds</i></pre>

### In che modo le variazioni del comando di modifica del failover dello storage influiscono sul giveback automatico

Il funzionamento del giveback automatico dipende dalla modalità di configurazione dei parametri del comando di modifica del failover dello storage.

La seguente tabella elenca le impostazioni predefinite per `storage failover modify` parametri di comando che si applicano agli eventi di takeover non causati da un panico.

Parametro	Impostazione predefinita
<code>-auto-giveback true</code>	<code>false</code>
<code>true</code>	<code>-delay-seconds integer (seconds)</code>
600	<code>-onreboot true</code>
<code>false</code>	<code>true</code>

La seguente tabella descrive le combinazioni di `-onreboot` e `-auto-giveback` i parametri influiscono sul giveback automatico per gli eventi di takeover non causati da un panico.

storage failover modify parametri utilizzati	Causa dell'acquisizione	Si verifica il giveback automatico?
<code>-onreboot true</code>  <code>-auto-giveback true</code>	comando reboot	Sì
Comando Halt (arresto) o operazione di spegnimento e riaccensione emessa dal Service Processor	Sì	<code>-onreboot true</code>  <code>-auto-giveback false</code>
comando reboot	Sì	Comando Halt (arresto) o operazione di spegnimento e riaccensione emessa dal Service Processor
No	<code>-onreboot false</code>  <code>-auto-giveback true</code>	comando reboot
N/D in questo caso, l'acquisizione non avviene	Comando Halt (arresto) o operazione di spegnimento e riaccensione emessa dal Service Processor	Sì
<code>-onreboot false</code>  <code>-auto-giveback false</code>	comando reboot	No

Il `-auto-giveback` i controlli dei parametri vengono ripristinati dopo il panic e tutti gli altri takeover automatici. Se il `-onreboot` il parametro è impostato su `true` e un takeover si verifica a causa di un riavvio, quindi viene sempre eseguito il giveback automatico, indipendentemente dal fatto che il `-auto-giveback` il parametro è impostato su `true`.

Il `-onreboot` Il parametro si applica ai comandi di riavvio e arresto emessi da ONTAP. Quando il `-onreboot` il parametro è impostato su `false`, non si verifica un takeover in caso di riavvio di un nodo. Pertanto, non è



possibile eseguire il giveback automatico, indipendentemente dal fatto che il `-auto-giveback` il parametro è impostato su `true`. Si verifica un'interruzione del client.

### Gli effetti delle combinazioni di parametri di giveback automatico che si applicano alle situazioni di panico.

La seguente tabella elenca `storage failover modify` parametri dei comandi applicabili alle situazioni di emergenza:

Parametro	Impostazione predefinita
<code>`-onpanic _true</code>	<code>false_`</code>
<code>true</code>	<code>`-auto-giveback-after-panic _true</code>
<code>false_`</code> (Privilegio: Avanzato)	<code>true</code>
<code>`-auto-giveback _true</code>	<code>false_`</code>

La seguente tabella descrive le combinazioni di parametri di `storage failover modify` il comando influisce sul giveback automatico in situazioni di panico.

<code>storage failover</code> parametri utilizzati	Il giveback automatico si verifica dopo il panico?
<code>-onpanic true</code> <code>-auto-giveback true</code> <code>-auto-giveback-after-panic true</code>	Sì
<code>-onpanic true</code> <code>-auto-giveback true</code> <code>-auto-giveback-after-panic false</code>	Sì
<code>-onpanic true</code> <code>-auto-giveback false</code> <code>-auto-giveback-after-panic true</code>	Sì
<code>-onpanic true</code> <code>-auto-giveback false</code> <code>-auto-giveback-after-panic false</code>	No
<code>-onpanic false`</code> Se <code>`-onpanic</code> è impostato su <code>false</code> , il takeover/giveback non si verifica, indipendentemente dal valore impostato per <code>-auto-giveback</code> oppure <code>-auto-giveback-after-panic</code>	No



Un takeover può derivare da un errore non associato a un panico. Si verifica un *guasto* quando la comunicazione tra un nodo e il suo partner viene persa, chiamata anche *perdita heartbeat*. Se si verifica un Takeover a causa di un guasto, il giveback viene controllato da `-onfailure` invece di `-auto-giveback-after-panic` parameter.



Quando un nodo viene preso in panica, invia un pacchetto panic al nodo partner. Se per qualsiasi motivo il pacchetto panic non viene ricevuto dal nodo partner, il panic può essere interpretato erroneamente come un errore. Senza la ricezione del pacchetto panic, il nodo partner sa solo che la comunicazione è stata persa e non sa che si è verificato un panico. In questo caso, il nodo partner elabora la perdita di comunicazione come un errore invece di un panico e il giveback è controllato da `-onfailure` (e non da `-auto-giveback-after-panic parameter`).

Per ulteriori informazioni su tutti `storage failover modify` per i parametri, vedere ["Pagine di manuale di ONTAP"](#).

## Comandi manuali di Takeover

È possibile eseguire un takeover manualmente quando è necessaria la manutenzione del partner e in altre situazioni simili. A seconda dello stato del partner, il comando utilizzato per eseguire il takeover varia.

Se si desidera...	Utilizzare questo comando...
Assumere il controllo del nodo partner	<code>storage failover takeover</code>
Monitorare l'avanzamento dell'acquisizione man mano che gli aggregati del partner vengono spostati nel nodo che esegue l'acquisizione	<code>storage failover show-takeover</code>
Visualizzare lo stato di failover dello storage per tutti i nodi del cluster	<code>storage failover show</code>
Assumere il controllo del nodo partner senza migrare i LIF	<code>storage failover takeover -skip-lif -migration-before-takeover true</code>
Assumere il controllo del nodo partner anche in caso di mancata corrispondenza del disco	<code>storage failover takeover -skip-lif -migration-before-takeover true</code>
Assumere il controllo del nodo partner anche in caso di mancata corrispondenza della versione di ONTAP <b>Nota:</b> questa opzione viene utilizzata solo durante il processo di aggiornamento di ONTAP senza interruzioni.	<code>storage failover takeover -option allow-version-mismatch</code>
Assumere il controllo del nodo partner senza eseguire il trasferimento dell'aggregato	<code>storage failover takeover -bypass -optimization true</code>
Assumere il controllo del nodo partner prima che il partner abbia il tempo di chiudere correttamente le proprie risorse di storage	<code>storage failover takeover -option immediate</code>

Prima di eseguire il comando di failover dello storage con l'opzione `immediate`, è necessario migrare i file LIF dei dati in un altro nodo utilizzando il seguente comando: `network interface migrate-all -node node`



Se si specifica `storage failover takeover -option immediate` Senza prima eseguire la migrazione dei dati LIF, la migrazione dei dati LIF dal nodo viene ritardata in modo significativo anche se `skip-lif-migration-before-takeover` opzione non specificata.

Analogamente, se si specifica l'opzione `immediata`, l'ottimizzazione del Takeover negoziato viene ignorata anche se l'opzione di ottimizzazione `bypass` è impostata su `false`.

## Spostamento di epsilon per alcuni takeover avviati manualmente

È consigliabile spostare epsilon se si prevede che eventuali operazioni di takeover avviate manualmente potrebbero causare un guasto inaspettato del nodo del sistema storage, lontano da una perdita di quorum a livello di cluster.

### A proposito di questa attività

Per eseguire la manutenzione pianificata, è necessario assumere il controllo di uno dei nodi di una coppia ha. È necessario mantenere il quorum a livello di cluster per evitare interruzioni non pianificate dei dati dei client per i nodi rimanenti. In alcuni casi, l'esecuzione del takeover può causare un cluster che rappresenta un guasto inaspettato del nodo a causa della perdita di quorum a livello di cluster.

Questo può verificarsi se il nodo che viene sostituito contiene epsilon o se il nodo con epsilon non è integro. Per mantenere un cluster più resiliente, è possibile trasferire epsilon a un nodo integro che non viene sostituito. In genere, questo sarebbe il partner ha.

Solo i nodi sani e idonei partecipano al voto del quorum. Per mantenere il quorum a livello di cluster, sono richiesti più di  $N/2$  voti (dove  $N$  rappresenta la somma dei nodi online sani e idonei). Nei cluster con un numero pari di nodi online, epsilon aggiunge ulteriore peso di voto per mantenere il quorum per il nodo a cui è assegnato.



Sebbene il voto di formazione del cluster possa essere modificato utilizzando `cluster modify -eligibility false` evitare questo problema, ad eccezione di situazioni come il ripristino della configurazione del nodo o la manutenzione prolungata del nodo. Se si imposta un nodo come non idoneo, questo interrompe la fornitura dei dati SAN fino a quando il nodo non viene reimpostato su idoneo e riavviato. Anche l'accesso ai dati NAS al nodo potrebbe essere compromesso quando il nodo non è idoneo.

## Fasi

1. Verificare lo stato del cluster e verificare che epsilon sia mantenuto da un nodo integro che non viene sostituito:
  - a. Passare al livello di privilegio avanzato, confermando che si desidera continuare quando viene visualizzato il prompt della modalità avanzata (`*>`):

```
set -privilege advanced
```

- b. Determinare quale nodo contiene epsilon:

```
cluster show
```

Nell'esempio seguente, Node1 contiene epsilon:

Nodo	Salute	Idoneità	Epsilon
Node1 Node2	vero vero	vero vero	vero falso

+

Se il nodo che si desidera sostituire non include epsilon, passare alla fase 4.

2. Rimuovere epsilon dal nodo che si desidera sostituire:

```
cluster modify -node Node1 -epsilon false
```

3. Assegnare epsilon al nodo partner (in questo esempio, Node2):

```
cluster modify -node Node2 -epsilon true
```

4. Eseguire l'operazione di takeover:

```
storage failover takeover -ofnode node_name
```

5. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Comandi manuali di giveback

È possibile eseguire un giveback normale, un giveback in cui si terminano i processi sul nodo partner o un giveback forzato.



Prima di eseguire un giveback, è necessario rimuovere i dischi guasti nel sistema preso in consegna come descritto in ["Gestione di dischi e aggregati"](#).

### In caso di interruzione del giveback

Se durante il processo di giveback si verifica un guasto o un'interruzione dell'alimentazione del nodo di Takeover, tale processo si interrompe e il nodo di Takeover torna in modalità Takeover fino a quando l'errore non viene riparato o l'alimentazione non viene ripristinata.

Tuttavia, ciò dipende dalla fase di giveback in cui si è verificato il guasto. Se il nodo ha riscontrato un guasto o un'interruzione dell'alimentazione durante lo stato di giveback parziale (dopo aver restituito l'aggregato root), non tornerà alla modalità Takeover. Il nodo torna invece alla modalità di parziale giveback. In tal caso, completare il processo ripetendo l'operazione di giveback.

### Se il giveback è veto

Se il giveback è vetoed, è necessario controllare i messaggi EMS per determinare la causa. A seconda del motivo o dei motivi, è possibile decidere se è possibile eseguire l'override dei veti in modo sicuro.

Il `storage failover show-giveback` il comando visualizza l'avanzamento del giveback e indica quale sottosistema ha posto il veto del giveback, se presente. I veti morbidi possono essere ignorati, mentre i veti difficili non possono essere, anche se forzati. Le seguenti tabelle riepilogano i file soft vetoes che non devono essere sovrascritti, insieme alle soluzioni consigliate.

È possibile rivedere i dettagli EMS per qualsiasi veto di giveback utilizzando il seguente comando:

```
event log show -node * -event gb*
```

### Giveback dell'aggregato root

Questi veti non si applicano alle operazioni di trasferimento degli aggregati:

Modulo del sottosistema di vetoing	Soluzione alternativa
vfiler_low_level	<p>Terminare le sessioni SMB che causano il veto o chiudere l'applicazione SMB che ha stabilito le sessioni aperte.</p> <p>L'override di questo veto potrebbe causare la disconnessione improvvisa dell'applicazione che utilizza SMB e la perdita di dati.</p>
Controllo disco	<p>Tutti i dischi guasti o bypassati devono essere rimossi prima di tentare il giveback. Se i dischi vengono disinfettati, attendere il completamento dell'operazione.</p> <p>L'override di questo veto potrebbe causare un'interruzione causata da aggregati o volumi che vanno fuori linea a causa di conflitti di prenotazione o dischi inaccessibili.</p>

### Giveback degli aggregati SFO

Questi veti non si applicano alle operazioni di trasferimento degli aggregati:

Modulo del sottosistema di vetoing	Soluzione alternativa
Gestione blocchi	<p>Arrestare correttamente le applicazioni SMB che hanno file aperti o spostare tali volumi in un aggregato diverso.</p> <p>L'override di questo veto comporta la perdita dello stato di blocco SMB, causando interruzioni e perdita di dati.</p>
Gestione blocchi NDO	<p>Attendere il mirroring dei blocchi.</p> <p>L'override di questo veto causa interruzioni alle macchine virtuali Microsoft Hyper-V.</p>

RAID	<p>Controllare i messaggi EMS per determinare la causa del veto:</p> <p>Se il veto è dovuto a nvfile, portare online i volumi offline e gli aggregati.</p> <p>Se sono in corso operazioni di aggiunta o riassegnazione della proprietà del disco, attendere il completamento.</p> <p>Se il veto è dovuto a un conflitto di nome aggregato o UUID, risolvere il problema.</p> <p>Se il veto è dovuto alla risincronizzazione del mirror, alla verifica del mirror o ai dischi offline, il veto può essere ignorato e l'operazione viene riavviata dopo il giveback.</p>
Inventario dei dischi	<p>Risolvere i problemi per identificare e risolvere la causa del problema.</p> <p>Il nodo di destinazione potrebbe non essere in grado di visualizzare i dischi appartenenti a un aggregato in fase di migrazione.</p> <p>I dischi inaccessibili possono causare aggregati o volumi inaccessibili.</p>
Operazione di spostamento del volume	<p>Risolvere i problemi per identificare e risolvere la causa del problema.</p> <p>Questo veto impedisce l'interruzione dell'operazione di spostamento del volume durante l'importante fase di cutover. Se il lavoro viene interrotto durante il cutover, il volume potrebbe diventare inaccessibile.</p>

#### Comandi per l'esecuzione di un giveback manuale

È possibile avviare manualmente un giveback su un nodo di una coppia ha per restituire lo storage al proprietario originale dopo aver completato la manutenzione o aver risolto eventuali problemi che hanno causato il takeover.

Se si desidera...	Utilizzare questo comando...
Restituire lo storage a un nodo partner	<code>storage failover giveback -ofnode <i>nodename</i></code>
Restituire lo storage anche se il partner non è in attesa della modalità di giveback	<code>storage failover giveback -ofnode <i>nodename</i></code> <code>-require-partner-waiting false</code>  <p>Non utilizzare questa opzione a meno che non sia accettabile un'interruzione più lunga del client.</p>

Restituire lo storage anche se i processi stanno vetoing l'operazione di giveback (forzare il giveback)	<pre>storage failover giveback -ofnode nodename -override-vetoes true</pre> <p>L'utilizzo di questa opzione può potenzialmente causare un'interruzione più lunga del servizio client o la mancata disponibilità di aggregati e volumi dopo il giveback.</p>
Restituire solo gli aggregati CFO (l'aggregato root)	<pre>storage failover giveback -ofnode nodename  -only-cfo-aggregates true</pre>
Monitorare l'avanzamento del giveback dopo aver eseguito il comando giveback	<pre>storage failover show-giveback</pre>

## Test di Takeover e giveback

Dopo aver configurato tutti gli aspetti della coppia ha, è necessario verificare che funzioni come previsto per mantenere l'accesso ininterrotto allo storage di entrambi i nodi durante le operazioni di takeover e giveback. Durante il processo di acquisizione, il nodo locale (o Takeover) deve continuare a fornire i dati normalmente forniti dal nodo partner. Durante il giveback, il controllo e la consegna dello storage del partner dovrebbero tornare al nodo partner.

### Fasi

1. Verificare che i cavi di interconnessione ha siano collegati correttamente.
2. Verificare che sia possibile creare e recuperare file su entrambi i nodi per ciascun protocollo concesso in licenza.
3. Immettere il seguente comando:

```
storage failover takeover -ofnode partnernode
```

Vedere la pagina man per i dettagli sui comandi.

4. Immettere uno dei seguenti comandi per confermare che si è verificato il Takeover:

```
storage failover show-takeover
```

```
storage failover show
```

Se si dispone di `storage failover` del comando `-auto-giveback` opzione attivata:

Nodo	Partner	Possibilità di acquisizione	Descrizione dello stato
nodo 1	nodo 2	-	In attesa di un giveback

nodo 2	nodo 1	falso	In fase di acquisizione, il giveback automatico verrà avviato in pochi secondi
--------	--------	-------	--

Se si dispone di `storage failover` del comando `-auto-giveback` opzione disattivata:

Nodo	Partner	Possibilità di acquisizione	Descrizione dello stato
nodo 1	nodo 2	-	In attesa di un giveback
nodo 2	nodo 1	falso	In fase di acquisizione

5. Visualizzare tutti i dischi appartenenti al nodo partner (Node2) che il nodo di Takeover (Node1) può rilevare:

```
storage disk show -home node2 -ownership
```

Il seguente comando visualizza tutti i dischi appartenenti a Node2 che Node1 può rilevare:

```
cluster::> storage disk show -home node2 -ownership
```

Disco	Aggregato	A casa	Proprietario	Dr. Casa	ID casa	ID proprietario	ID casa DR	Riservato re	Piscina
1.0.2	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0
1.0.3	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0

6. Verificare che il nodo di Takeover (Node1) controlli gli aggregati del nodo partner (Node2):

```
aggr show -fields home-id,home-name,is-home
```

aggregato	id abitazione	nome di casa	è a casa
aggr0_1	2014942045	node1	vero
aggr0_2	4078312453	node2	falso
aggr1_1	2014942045	node1	vero
aggr1_2	4078312453	node2	falso

Durante l'acquisizione, il valore "is-home" degli aggregati del nodo partner è falso.

7. Restituire il servizio dati del nodo partner dopo aver visualizzato il messaggio "Waiting for giveback":

```
storage failover giveback -ofnode partnernode
```

8. Immettere uno dei seguenti comandi per osservare l'avanzamento dell'operazione di giveback:



```
storage failover show-giveback
```

```
storage failover show
```

9. Procedere, a seconda che sia stato visualizzato il messaggio che indica che il giveback è stato completato correttamente:

In caso di acquisizione e giveback...	Quindi...
Sono stati completati correttamente	Ripetere i passaggi da 2 a 8 sul nodo partner.
Non riuscito	Correggere l'errore di takeover o giveback, quindi ripetere questa procedura.

## Comandi per il monitoraggio di una coppia ha

È possibile utilizzare i comandi ONTAP per monitorare lo stato della coppia ha. Se si verifica un Takeover, è anche possibile determinare la causa del Takeover.

Se si desidera controllare	Utilizzare questo comando
Se il failover è attivato o si è verificato, oppure perché il failover non è attualmente possibile	<code>storage failover show</code>
Consente di visualizzare i nodi su cui è abilitata l'impostazione ha-mode di failover dello storage. Devi impostare il valore su ha perché il nodo partecipi a una configurazione di failover dello storage (coppia ha).	<code>storage failover show -fields mode</code>
Se il Takeover assistito dall'hardware è attivato	<code>storage failover hwassist show</code>
La cronologia degli eventi di Takeover assistiti dall'hardware che si sono verificati	<code>storage failover hwassist stats show</code>
Lo stato di avanzamento di un'operazione di Takeover mentre gli aggregati del partner vengono spostati nel nodo che esegue il Takeover	<code>storage failover show-takeover</code>
Lo stato di avanzamento di un'operazione di giveback nella restituzione degli aggregati al nodo partner	<code>storage failover show-giveback</code>
Se un aggregato è a casa durante le operazioni di acquisizione o di giveback	<code>aggregate show -fields home-id,owner-id,home-name,owner-name,is-home</code>
Se l'ha del cluster è attivato (si applica solo ai cluster a due nodi)	<code>cluster ha show</code>
Lo stato ha dei componenti di una coppia ha (sui sistemi che utilizzano lo stato ha)	<code>'ha-config show'</code> Si tratta di un comando della modalità di manutenzione.

## stati dei nodi visualizzati dai comandi di tipo show di failover dello storage

L'elenco seguente descrive gli stati dei nodi in cui si trova `storage failover show` viene visualizzato il comando.

Stato del nodo	Descrizione
Connesso a partner_name, Takeover automatico disattivato.	L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. L'acquisizione automatica del partner è disattivata.
In attesa di nome_partner, giveback dei dischi di riserva del partner in sospeso.	<p>Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il giveback degli aggregati SFO per il partner viene eseguito, ma i dischi di riserva del partner sono ancora di proprietà del nodo locale.</p> <ul style="list-style-type: none"> <li>• Eseguire <code>storage failover show-giveback</code> per ulteriori informazioni.</li> </ul>
In attesa di nome_partner. In attesa della sincronizzazione del blocco partner.	Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha e attende che venga eseguita la sincronizzazione del blocco del partner.
In attesa di nome_partner. In attesa che le applicazioni cluster siano online sul nodo locale.	Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha e attende che le applicazioni del cluster siano online.
Takeover pianificato. Nodo di destinazione spostamento dei propri aggregati SFO in preparazione del Takeover.	L'elaborazione del takeover è iniziata. Il nodo di destinazione sta trasferendo la proprietà dei propri aggregati SFO in preparazione del takeover.
Takeover pianificato. Il nodo di destinazione ha riallocato i propri aggregati SFO in preparazione del Takeover.	L'elaborazione del takeover è iniziata. Il nodo di destinazione ha riallocato la proprietà dei propri aggregati SFO in preparazione del takeover.
Takeover pianificato. In attesa di disattivare gli aggiornamenti del firmware del disco in background sul nodo locale. È in corso un aggiornamento del firmware sul nodo.	L'elaborazione del takeover è iniziata. Il sistema è in attesa del completamento delle operazioni di aggiornamento del firmware del disco in background sul nodo locale.
Spostamento degli aggregati SFO nel nodo di acquisizione in preparazione del Takeover.	Il nodo locale sta trasferendo la proprietà dei propri aggregati SFO nel nodo di Taking-over in preparazione del Takeover.
Riallocare gli aggregati SFO per assumere il nodo. In attesa di acquisizione del nodo.	Il trasferimento della proprietà degli aggregati SFO dal nodo locale al nodo di acquisizione è stato completato. Il sistema è in attesa di essere assunto dal nodo di acquisizione.

<p>Spostamento degli aggregati SFO in nome_partner. In attesa di disattivare gli aggiornamenti del firmware del disco in background sul nodo locale. È in corso un aggiornamento del firmware sul nodo.</p>	<p>È in corso il trasferimento della proprietà degli aggregati SFO dal nodo locale al nodo di acquisizione. Il sistema è in attesa del completamento delle operazioni di aggiornamento del firmware del disco in background sul nodo locale.</p>
<p>Spostamento degli aggregati SFO in nome_partner. In attesa di disattivare gli aggiornamenti del firmware del disco in background su partner_name. È in corso un aggiornamento del firmware sul nodo.</p>	<p>È in corso il trasferimento della proprietà degli aggregati SFO dal nodo locale al nodo di acquisizione. Il sistema è in attesa del completamento delle operazioni di aggiornamento del firmware del disco in background sul nodo partner.</p>
<p>Connesso a partner_name. Il precedente tentativo di takeover è stato interrotto a causa del motivo. Il nodo locale possiede alcuni aggregati SFO del partner. Rimettere un'acquisizione del partner con <code>-bypass-optimization</code> parametro impostato su true per rilevare gli aggregati rimanenti o emettere un giveback del partner per restituire gli aggregati ricollocati.</p>	<p>L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il tentativo di acquisizione precedente è stato interrotto a causa del motivo visualizzato sotto Reason (motivo). Il nodo locale possiede alcuni aggregati SFO del partner.</p> <ul style="list-style-type: none"> <li>• Rimettere un takeover del nodo partner, impostando il parametro di ottimizzazione <code>-bypass-</code> su true per rilevare gli aggregati SFO rimanenti, oppure eseguire un giveback del partner per restituire gli aggregati ricollocati.</li> </ul>
<p>Connesso a partner_name. Il tentativo di acquisizione precedente è stato interrotto. Il nodo locale possiede alcuni aggregati SFO del partner. Rimettere un'acquisizione del partner con <code>-bypass-optimization</code> parametro impostato su true per rilevare gli aggregati rimanenti o emettere un giveback del partner per restituire gli aggregati ricollocati.</p>	<p>L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il tentativo di acquisizione precedente è stato interrotto. Il nodo locale possiede alcuni aggregati SFO del partner.</p> <ul style="list-style-type: none"> <li>• Rimettere un takeover del nodo partner, impostando il parametro di ottimizzazione <code>-bypass-</code> su true per rilevare gli aggregati SFO rimanenti, oppure eseguire un giveback del partner per restituire gli aggregati ricollocati.</li> </ul>
<p>In attesa di nome_partner. Il precedente tentativo di takeover è stato interrotto a causa del motivo. Il nodo locale possiede alcuni aggregati SFO del partner. Rimettere un'acquisizione del partner con il parametro <code>"-bypass-Optimization"</code> impostato su true per rilevare gli aggregati rimanenti o emettere un giveback del partner per restituire gli aggregati ricollocati.</p>	<p>Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il tentativo di acquisizione precedente è stato interrotto a causa del motivo visualizzato sotto Reason (motivo). Il nodo locale possiede alcuni aggregati SFO del partner.</p> <ul style="list-style-type: none"> <li>• Rimettere un takeover del nodo partner, impostando il parametro di ottimizzazione <code>-bypass-</code> su true per rilevare gli aggregati SFO rimanenti, oppure eseguire un giveback del partner per restituire gli aggregati ricollocati.</li> </ul>

In attesa di nome_partner. Il tentativo di acquisizione precedente è stato interrotto. Il nodo locale possiede alcuni aggregati SFO del partner. Rimettere un'acquisizione del partner con il parametro "-bypass-Optimization" impostato su true per rilevare gli aggregati rimanenti o emettere un giveback del partner per restituire gli aggregati ricollocati.	<p>Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il tentativo di acquisizione precedente è stato interrotto. Il nodo locale possiede alcuni aggregati SFO del partner.</p> <ul style="list-style-type: none"> <li>• Rimettere un takeover del nodo partner, impostando il parametro di ottimizzazione -bypass-su true per rilevare gli aggregati SFO rimanenti, oppure eseguire un giveback del partner per restituire gli aggregati ricollocati.</li> </ul>
Connesso a partner_name. Il precedente tentativo di takeover è stato interrotto perché non è stato possibile disattivare l'aggiornamento del firmware del disco in background (BDFU) sul nodo locale.	L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il tentativo di takeover precedente è stato interrotto perché l'aggiornamento del firmware del disco in background sul nodo locale non era stato disattivato.
Connesso a partner_name. Il precedente tentativo di takeover è stato interrotto a causa del motivo.	L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il tentativo di acquisizione precedente è stato interrotto a causa del motivo visualizzato sotto Reason (motivo).
In attesa di nome_partner. Il precedente tentativo di takeover è stato interrotto a causa del motivo.	Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il tentativo di acquisizione precedente è stato interrotto a causa del motivo visualizzato sotto Reason (motivo).
Connesso a partner_name. Il precedente tentativo di acquisizione da parte di partner_name è stato interrotto a causa del motivo.	L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il precedente tentativo di acquisizione da parte del nodo partner è stato interrotto a causa del motivo visualizzato sotto Reason.
Connesso a partner_name. Il precedente tentativo di acquisizione da parte di partner_name è stato interrotto.	L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il precedente tentativo di acquisizione da parte del nodo partner è stato interrotto.
In attesa di nome_partner. Il precedente tentativo di acquisizione da parte di partner_name è stato interrotto a causa del motivo.	Il nodo locale non può scambiare informazioni con il nodo partner tramite l'interconnessione ha. Il precedente tentativo di acquisizione da parte del nodo partner è stato interrotto a causa del motivo visualizzato sotto Reason.
Giveback precedente non riuscito nel modulo: Nome modulo. Il giveback automatico verrà avviato in pochi secondi.	<p>Il precedente tentativo di giveback non è riuscito nel modulo module_name. Il giveback automatico verrà avviato in pochi secondi.</p> <ul style="list-style-type: none"> <li>• Eseguire storage failover show-giveback per ulteriori informazioni.</li> </ul>

Node possiede gli aggregati del partner come parte della procedura di upgrade del controller senza interruzioni.	Il nodo possiede gli aggregati del partner a causa della procedura di aggiornamento del controller senza interruzioni attualmente in corso.
Connesso a partner_name. Il nodo possiede aggregati appartenenti a un altro nodo del cluster.	L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il nodo possiede aggregati appartenenti a un altro nodo del cluster.
Connesso a partner_name. In attesa della sincronizzazione del blocco partner.	L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il sistema è in attesa del completamento della sincronizzazione del blocco partner.
Connesso a partner_name. In attesa che le applicazioni cluster siano online sul nodo locale.	L'interconnessione ha è attiva e può trasmettere i dati al nodo partner. Il sistema è in attesa che le applicazioni del cluster siano online sul nodo locale.
Modalità non ha, riavviare per utilizzare la NVRAM completa.	Il failover dello storage non è possibile. L'opzione ha mode è configurata come non_ha.  • Riavviare il nodo per utilizzare tutta la NVRAM.
Modalità non ha. Riavviare il nodo per attivare ha.	Il failover dello storage non è possibile.  • Il nodo deve essere riavviato per abilitare la funzionalità ha.
Modalità non ha.	Il failover dello storage non è possibile. L'opzione ha mode è configurata come non_ha.  • È necessario eseguire <code>storage failover modify -mode ha -node nodename</code> Su entrambi i nodi della coppia ha, quindi riavviare i nodi per abilitare la funzionalità ha.

## Comandi per abilitare e disabilitare il failover dello storage

Utilizzare i seguenti comandi per attivare e disattivare la funzionalità di failover dello storage.

Se si desidera...	Utilizzare questo comando...
Abilitare il Takeover	<code>storage failover modify -enabled true -node nodename</code>
Disattiva il Takeover	<code>storage failover modify -enabled false -node nodename</code>



È necessario disattivare il failover dello storage solo se necessario come parte di una procedura di manutenzione.

## Arrestare o riavviare un nodo senza avviare il Takeover in un cluster a due nodi

Arrestare o riavviare un nodo in un cluster a due nodi senza avviare il Takeover quando si esegue una determinata manutenzione hardware su un nodo o uno shelf e si desidera limitare il tempo di inattività mantenendo il nodo partner attivo, oppure quando si verificano problemi che impediscono un takeover manuale e si desidera mantenere aggiornati gli aggregati del nodo partner e fornire i dati. Inoltre, se il supporto tecnico sta fornendo assistenza per la risoluzione dei problemi, potrebbe essere necessario eseguire questa procedura come parte di tali sforzi.

### A proposito di questa attività

- Prima di inibire il Takeover (utilizzando il `-inhibit-takeover true` Parametro), si disattiva il cluster ha.



- In un cluster a due nodi, il cluster ha garantisce che il guasto di un nodo non disabiliti il cluster. Tuttavia, se non si disattiva il cluster ha prima di utilizzare `-inhibit-takeover true` parametro, entrambi i nodi interrompono la fornitura dei dati.
- Se si tenta di arrestare o riavviare un nodo prima di disattivare il cluster ha, ONTAP emette un avviso e richiede di disattivare il cluster ha.

- La migrazione delle LIF (interfacce logiche) al nodo partner che si desidera mantenere in linea.
- Se sul nodo che si sta arrestando o riavviando sono presenti aggregati che si desidera mantenere, spostarli nel nodo che si desidera mantenere in linea.

### Fasi

1. Verificare che entrambi i nodi siano integri:

```
cluster show
```

Per entrambi i nodi, `true` viene visualizzato in Health colonna.

```
cluster::> cluster show
Node           Health  Eligibility
-----
node1          true    true
node2          true    true
```

2. Migrare tutte le LIF dal nodo che si desidera arrestare o riavviare al nodo partner:  
`network interface migrate-all -node node_name`
3. Se sul nodo si arresta o si riavvia ci sono aggregati che si desidera mantenere in linea quando il nodo è inattivo, trasferirli sul nodo partner; in caso contrario, passare alla fase successiva.
  - a. Mostrare gli aggregati sul nodo che si desidera arrestare o riavviare:  
`storage aggregates show -node node_name`

Ad esempio, `node1` è il nodo che verrà arrestato o riavviato:

```
cluster::> storage aggregates show -node node1
Aggregate Size Available Used% State #Vols Nodes RAID
Status
-----
-----
aggr0_node_1_0
744.9GB 32.68GB 96% online 2 node1 raid_dp,
normal
aggr1 2.91TB 2.62TB 10% online 8 node1 raid_dp,
normal
aggr2 4.36TB 3.74TB 14% online 12 node1 raid_dp,
normal
test2_aggr 2.18TB 2.18TB 0% online 7 node1 raid_dp,
normal
4 entries were displayed.
```

b. Spostare gli aggregati nel nodo partner:

```
storage aggregate relocation start -node node_name -destination node_name
-aggregate-list aggregate_name
```

Ad esempio, gli aggregati aggr1, aggr2 e test2\_aggr vengono spostati da node1 a node2:

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr1,aggr2,test2_aggr
```

4. Disattiva cluster ha:

```
cluster ha modify -configured false
```

L'output di ritorno conferma che ha è disattivato: Notice: HA is disabled



Questa operazione non disattiva il failover dello storage.

5. Arrestare o riavviare e inibire il takeover del nodo di destinazione, utilizzando il comando appropriato:

- ° `system node halt -node node_name -inhibit-takeover true`
- ° `system node reboot -node node_name -inhibit-takeover true`



Nell'output del comando, viene visualizzato un avviso che chiede se si desidera procedere, digitare *y*.

6. Verificare che il nodo ancora in linea sia in buono stato (mentre il partner non è attivo):

```
cluster show
```

Per il nodo online, `true` viene visualizzato in `Health` colonna.



Nell'output del comando, viene visualizzato un avviso che indica che il cluster ha non è configurato. È possibile ignorare l'avviso in questo momento.

7. Eseguire le azioni necessarie per arrestare o riavviare il nodo.

8. Avviare il nodo non allineato dal prompt DEL CARICATORE:

```
boot_ontap
```

9. Verificare che entrambi i nodi siano integri:

```
cluster show
```

Per entrambi i nodi, `true` viene visualizzato in `Health` colonna.



Nell'output del comando, viene visualizzato un avviso che indica che il cluster ha non è configurato. È possibile ignorare l'avviso in questo momento.

10. Riabilitare il cluster ha:

```
cluster ha modify -configured true
```

11. Se prima di questa procedura sono state spostate le aggregazioni nel nodo partner, spostarle di nuovo nel nodo principale; in caso contrario, passare alla fase successiva:

```
storage aggregate relocation start -node node_name -destination node_name  
-aggregate-list aggregate_name
```

Ad esempio, gli aggregati `aggr1`, `aggr2` e `test2_aggr` vengono spostati dal nodo `node2` al nodo `node1`:

```
storage aggregate relocation start -node node2 -destination node1 -aggregate  
-list aggr1,aggr2,test2_aggr
```

12. Ripristinare le LIF alle porte home:

a. Visualizza le LIF che non sono a casa:

```
network interface show -is-home false
```

b. Se esistono LIF non domestiche che non sono state migrate dal nodo DOWN, verificare che sia sicuro spostarle prima di eseguire il ripristino.

c. In caso di sicurezza, ripristinare tutte le LIF a casa.

```
network interface revert *
```

## Gestione delle API REST con System Manager

### Gestione delle API REST con System Manager

Il log delle API REST acquisisce le chiamate API che Gestione di sistema invia a ONTAP. È possibile utilizzare il log per comprendere la natura e la sequenza delle chiamate necessarie per eseguire le varie attività amministrative di ONTAP.

#### Come System Manager utilizza l'API REST e il log API

Esistono diversi modi in cui le chiamate REST API vengono inviate da Gestore di sistema a ONTAP.



## Quando System Manager effettua chiamate API

Di seguito sono riportati gli esempi più importanti di quando Gestione sistema esegue chiamate API REST ONTAP.

### Aggiornamento automatico della pagina

System Manager effettua automaticamente chiamate API in background per aggiornare le informazioni visualizzate, ad esempio nella pagina della dashboard.

### Azione di visualizzazione per utente

Una o più chiamate API vengono emesse quando si visualizza una risorsa di storage specifica o una raccolta di risorse dall'interfaccia utente di System Manager.

### Azione di aggiornamento da parte dell'utente

Una chiamata API viene eseguita quando si aggiunge, modifica o elimina una risorsa ONTAP dall'interfaccia utente di Gestione sistema.

### Rimissione di una chiamata API

È inoltre possibile eseguire manualmente una chiamata API facendo clic su una voce di registro. Visualizza l'output JSON raw della chiamata.


### Ulteriori informazioni

- ["Documentazione sull'automazione di ONTAP 9"](#)

## Accesso al log API REST

È possibile accedere al registro contenente un record delle chiamate API REST ONTAP effettuate da Gestore di sistema. Quando si visualizza il log, è possibile anche emettere nuovamente le chiamate API e rivedere l'output.

### Fasi

1. Nella parte superiore della pagina, fare clic su  Per visualizzare il log API REST.

Le voci più recenti vengono visualizzate nella parte inferiore della pagina.

2. A sinistra, fare clic su **DASHBOARD** e osservare le nuove voci create per le chiamate API emesse per aggiornare la pagina.
3. Fare clic su **STORAGE**, quindi su **Qtree**.

In questo modo System Manager esegue una chiamata API specifica per recuperare un elenco di Qtree.

4. Individuare la voce di registro che descrive la chiamata API che ha il modulo:

```
GET /api/storage/qtrees
```

Verranno visualizzati ulteriori parametri di query HTTP inclusi nella voce, ad esempio `max_records`.

5. Fare clic sulla voce di registro per emettere nuovamente la chiamata GET API e visualizzare l'output JSON raw.

#### Esempio

```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {
          "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-00a0986abd71/1"
        }
      }
    }
  ]
}
```

```
    }  
  },  
],  
"num_records": 1,  
"_links": {  
  "self": {  
    "href":  
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"  
  }  
}  
}
```

# Amministrazione dei volumi

## Gestione di volumi e LUN con System Manager

### Panoramica sull'amministrazione dei volumi con System Manager

A partire da ONTAP 9.7, è possibile utilizzare Gestione sistema per gestire lo storage logico, ad esempio FlexVol Volumes e LUN, qtree, efficienza dello storage e quote.

Se si utilizza la gestione di sistema classica (disponibile solo in ONTAP 9.7 e versioni precedenti), fare riferimento a. ["Gestione dello storage logico"](#)

### Gestire i volumi

#### Panoramica di Manage Volumes





Dopo aver visualizzato un elenco di volumi in System Manager, è possibile eseguire varie azioni per gestire i volumi.



#### Fasi

1. In System Manager, fare clic su **Storage > Volumes** (Storage > volumi).

Viene visualizzato l'elenco dei volumi.

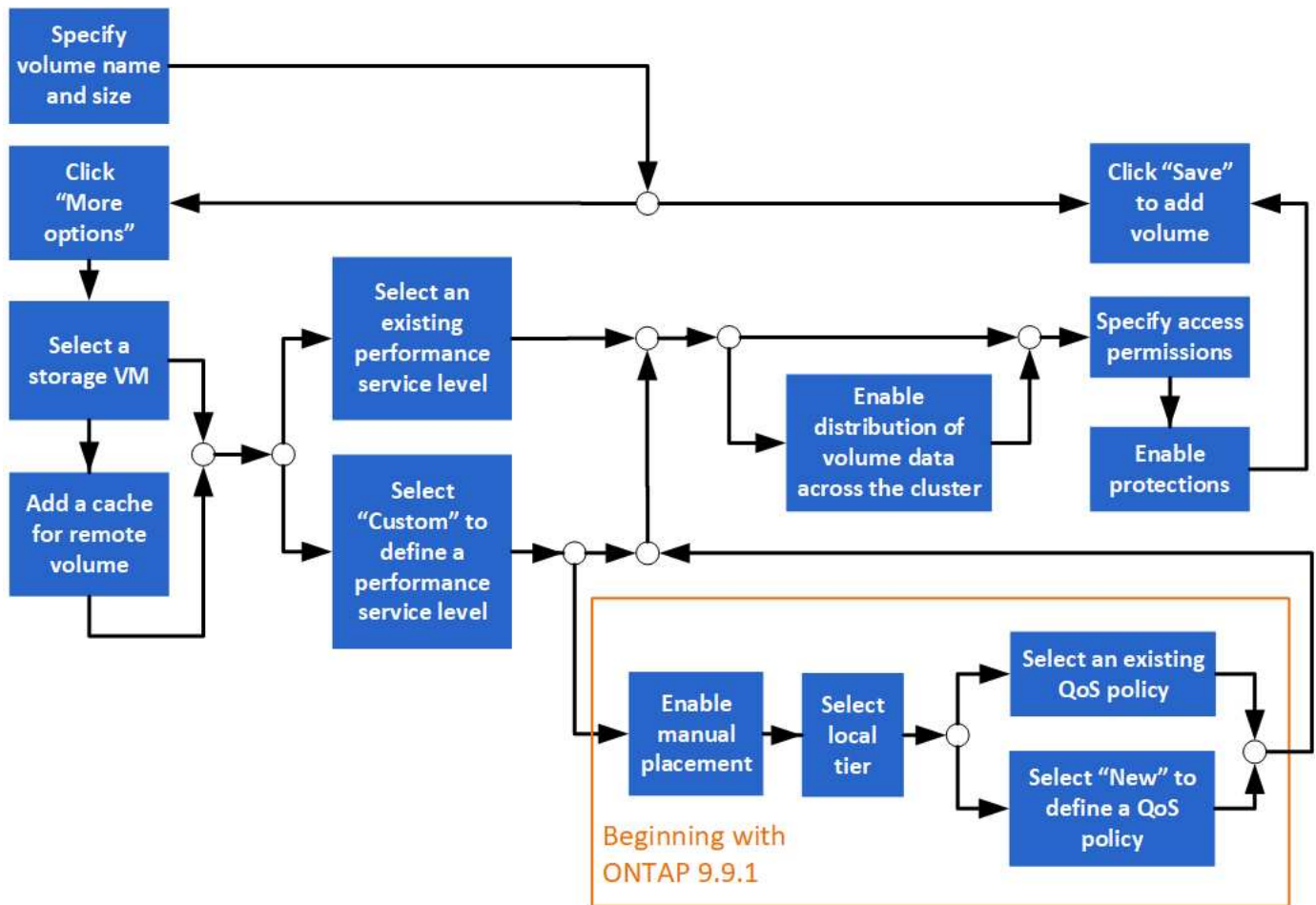
2. È possibile eseguire le seguenti operazioni:

Per eseguire questa attività...	Intraprendere queste azioni...
Aggiungere un volume	Fare clic su  <b>Add</b> . Vedere <a href="#">"Aggiungere un volume"</a> .
Gestire più volumi	<p>Selezionare le caselle accanto ai volumi.</p> <ul style="list-style-type: none"><li>• Fare clic su  <b>Delete</b> per eliminare i volumi selezionati.</li><li>• Fare clic su  <b>Protect</b> per assegnare un criterio di protezione ai volumi selezionati.</li><li>• Fare clic su  <b>More</b> per selezionare una delle seguenti azioni da eseguire per tutti i volumi selezionati:<ul style="list-style-type: none"><li>◦ Attiva quota</li><li>◦ Non in linea</li><li>◦ Sposta</li><li>◦ Mostra volumi cancellati</li></ul></li></ul>

Gestire un singolo volume	<p>Accanto al volume, fare clic su , quindi selezionare una delle seguenti azioni da eseguire:</p> <ul style="list-style-type: none"> <li>• Modifica</li> <li>• Ridimensionamento (a partire da ONTAP 9.10.1 e solo per volumi online e volumi DP FlexVol)</li> <li>• Eliminare</li> <li>• Clonare</li> <li>• Take Offline (o Bring Online)</li> <li>• Attiva quota (o Disattiva quota)</li> <li>• Modifica policy di esportazione</li> <li>• Modifica percorso di montaggio</li> <li>• Sposta</li> <li>• Modifica impostazioni livello cloud</li> <li>• Proteggere</li> </ul>
Rinominare un volume	<p>È possibile rinominare un volume dalla pagina di panoramica.</p> <p>Fare clic su  accanto al nome del volume, quindi modificare il nome del volume.</p>

### Aggiungere un volume

È possibile creare un volume e aggiungerlo a una VM di storage esistente configurata per il servizio NFS o SMB.



### Prima di iniziare

- Nel cluster dovrebbe essere presente una VM di storage configurata per il servizio NFS o SMB.
- A partire da ONTAP 9.13.1, puoi attivare l'analisi della capacità e il monitoraggio delle attività per impostazione predefinita sui nuovi volumi. In System Manager, è possibile gestire le impostazioni predefinite a livello di cluster o storage VM. Per ulteriori informazioni, vedere [Abilita analisi del file system](#).

### Fasi

1. Accedere a **Storage > Volumes** (Storage > volumi).
2. Selezionare **+ Add**.
3. Specificare un nome e una dimensione per il volume.
4. Eseguire una delle seguenti operazioni:

Selezionare questo pulsante...	Per eseguire questa azione...
<b>Salva</b>	Il volume viene creato e aggiunto utilizzando le impostazioni predefinite del sistema. Non sono necessari passaggi aggiuntivi.
<b>Altre opzioni</b>	Passare a. <a href="#">[step5]</a> consente di definire le specifiche del volume.

5. [\[\[fase 5,fase 5\]\]](#) il nome e le dimensioni del volume vengono visualizzati se precedentemente specificati. In caso contrario, inserire il nome e la dimensione.
6. Selezionare una VM di storage dall'elenco a discesa.

Vengono elencate solo le VM di storage configurate con il protocollo NFS. Se è disponibile una sola VM di

storage configurata con il protocollo NFS, il campo **Storage VM** non viene visualizzato.

7. Per aggiungere una cache per il volume remoto, selezionare **Aggiungi una cache per il volume remoto** e specificare i seguenti valori:

- Selezionare un cluster.
- Selezionare una VM di storage.
- Selezionare il volume che si desidera utilizzare come volume della cache.

8. Nella sezione **Storage and Optimization**, specificare i seguenti valori:

- La capacità del volume è già visualizzata, ma è possibile modificarla.
- Nel campo **Performance Service Level**, selezionare un livello di servizio:

Quando si seleziona questo livello di servizio...	Ciò si verifica...
Un livello di servizio esistente, ad esempio "Extreme", "Performance" o "Value".  Vengono visualizzati solo i livelli di servizio validi per la piattaforma di sistema (AFF, FAS o altri).	Vengono selezionati automaticamente uno o più Tier locali. Passare a. <a href="#">[step9]</a> .
Personalizzato	Passare a. <a href="#">[step8c]</a> per definire un nuovo livello di servizio.

- [[fase 8c, fase 8c]] a partire da ONTAP 9.9.1, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale su cui si desidera posizionare il volume da creare (se è stato selezionato il livello di servizio "personalizzato").



Questa opzione non è disponibile se si seleziona **Aggiungi come cache per un volume remoto** o **Distribuisci i dati del volume nel cluster** (vedere di seguito).

Quando fai questa scelta...	Eseguire questi passaggi...
<b>Posizionamento manuale</b>	Il posizionamento manuale è attivato. La selezione <b>Distribuisci i dati del volume nel cluster</b> è disattivata (vedere di seguito). Passare a. <a href="#">[step8d]</a> per completare il processo.
Nessuna selezione	Il posizionamento manuale non è abilitato. Il Tier locale viene selezionato automaticamente. Passare a. <a href="#">[step9]</a> .

- [[fase 8d, fase 8d]] selezionare un livello locale dal menu a discesa.
- Selezionare un criterio QoS.

Selezionare "esistente" per scegliere da un elenco di policy esistenti oppure selezionare "nuovo" per inserire le specifiche di una nuova policy.

9. [[fase 9, fase 9]] nella sezione **Opzioni di ottimizzazione**, determinare se si desidera distribuire i dati del volume nel cluster:

Quando fai questa scelta...	Ciò si verifica...
-----------------------------	--------------------

<b>Distribuire i dati dei volumi nel cluster</b>	Il volume che si sta aggiungendo diventa un volume FlexGroup. Questa opzione non è disponibile se in precedenza è stato selezionato <b>posizionamento manuale</b> .
Nessuna selezione	Per impostazione predefinita, il volume che si sta aggiungendo diventa un volume FlexVol.

10. Nella sezione **Access Permissions**, specificare le autorizzazioni di accesso per i protocolli per i quali è configurato il volume.

A partire da ONTAP 9.11.1, il nuovo volume non sarà condivisibile per impostazione predefinita. È possibile specificare le autorizzazioni di accesso predefinite verificando che siano selezionate le seguenti caselle di controllo:

- **Export via NGS:** Crea il volume con la policy di esportazione “default” che garantisce agli utenti l’accesso completo ai dati.
- **Share via SMB/CIFS:** Crea una condivisione con un nome generato automaticamente, che puoi modificare. L’accesso è concesso a “Everyone”. Inoltre, è possibile specificare il livello di autorizzazione.

11. Nella sezione **protezione**, specificare le protezioni per il volume.

- A partire da ONTAP 9.12.1, è possibile selezionare **attiva copie snapshot (locale)** e scegliere un criterio di copia snapshot piuttosto che utilizzare quello predefinito.
- Se si seleziona **Enable SnapMirror (Local or Remote)** (attiva SnapMirror (locale o remoto)), specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.

12. Selezionare **Salva**.

Il volume viene creato e aggiunto alla VM del cluster e dello storage.



Puoi anche salvare le specifiche di questo volume in un Ansible Playbook. Per ulteriori informazioni, visitare il sito Web all’indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

## Assegnare tag ai volumi

A partire da ONTAP 9.14.1, è possibile utilizzare Gestione sistema per assegnare tag ai volumi per identificare gli oggetti come appartenenti a una categoria, ad esempio progetti o centri di costo.

### A proposito di questa attività

È possibile assegnare un tag a un volume. Innanzitutto, è necessario definire e aggiungere il tag. Quindi, è anche possibile modificare o eliminare il tag.

È possibile aggiungere tag durante la creazione di un volume o aggiungerli in un secondo momento.

È possibile definire un tag specificando una chiave e associando un valore utilizzando il formato “key:value”. Ad esempio: “dept:engineering” o “location:san-jose”.

Quando si creano tag, è necessario tenere in considerazione quanto segue:



- Le chiavi hanno una lunghezza minima di un carattere e non possono essere nulle. I valori possono essere nulli.
- Una chiave può essere associata a più valori separando i valori con una virgola, ad esempio, "location:san-jose,toronto"
- I tag possono essere utilizzati per più risorse.
- I tag devono iniziare con una lettera minuscola.
- I tag assegnati ai volumi verranno eliminati quando viene eliminato il volume.
- I tag non vengono recuperati se un volume viene recuperato dalla coda di ripristino.
- I tag vengono conservati se il volume viene spostato o clonato.
- I tag assegnati alle macchine virtuali storage in una relazione di disaster recovery vengono replicati sul volume sul sito del partner.

## Fasi


Per gestire i tag, attenersi alla seguente procedura:

1. In System Manager, fare clic su **volumi**, quindi selezionare il volume a cui si desidera aggiungere un tag.

I tag sono elencati nella sezione **Tag**.

2. Fare clic su **Gestisci tag** per modificare i tag esistenti o aggiungerne di nuovi.

È possibile aggiungere, modificare o eliminare i tag.

Per eseguire questa azione...	Eseguire questa procedura...
Aggiungere un tag	<ol style="list-style-type: none"> <li>a. Fare clic su <b>Aggiungi tag</b>.</li> <li>b. Specificare una chiave e il suo valore o i suoi valori (separare più valori con virgole).</li> <li>c. Fare clic su <b>Save</b> (Salva).</li> </ol>
Modificare un tag	<ol style="list-style-type: none"> <li>a. Modificare il contenuto nei campi <b>chiave</b> e <b>valori (facoltativo)</b>.</li> <li>b. Fare clic su <b>Save</b> (Salva).</li> </ol>
Eliminare un tag	<ol style="list-style-type: none"> <li>a. Fare clic su  accanto al tag che si desidera eliminare.</li> </ol>

## Ripristinare i volumi cancellati

Se uno o più volumi FlexVol sono stati accidentalmente eliminati, è possibile utilizzare Gestione sistema per ripristinare tali volumi. A partire da ONTAP 9.8, è anche possibile utilizzare Gestione di sistema per ripristinare i volumi FlexGroup. È inoltre possibile eliminare i volumi in modo permanente eliminando i volumi.

Il tempo di conservazione del volume può essere impostato a livello di storage VM. Per impostazione predefinita, il tempo di conservazione del volume è impostato su 12 ore.

## Selezione dei volumi cancellati

### Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Fare clic su **Altro > Mostra volumi cancellati**.
3. Selezionare i volumi e fare clic sull'azione desiderata per ripristinarli o eliminarli definitivamente.

## Ripristino delle configurazioni del volume

L'eliminazione di un volume elimina le configurazioni associate del volume. Il ripristino di un volume non ripristina tutte le configurazioni. Eseguire le seguenti operazioni manualmente dopo il ripristino di un volume per riportarlo allo stato originale:

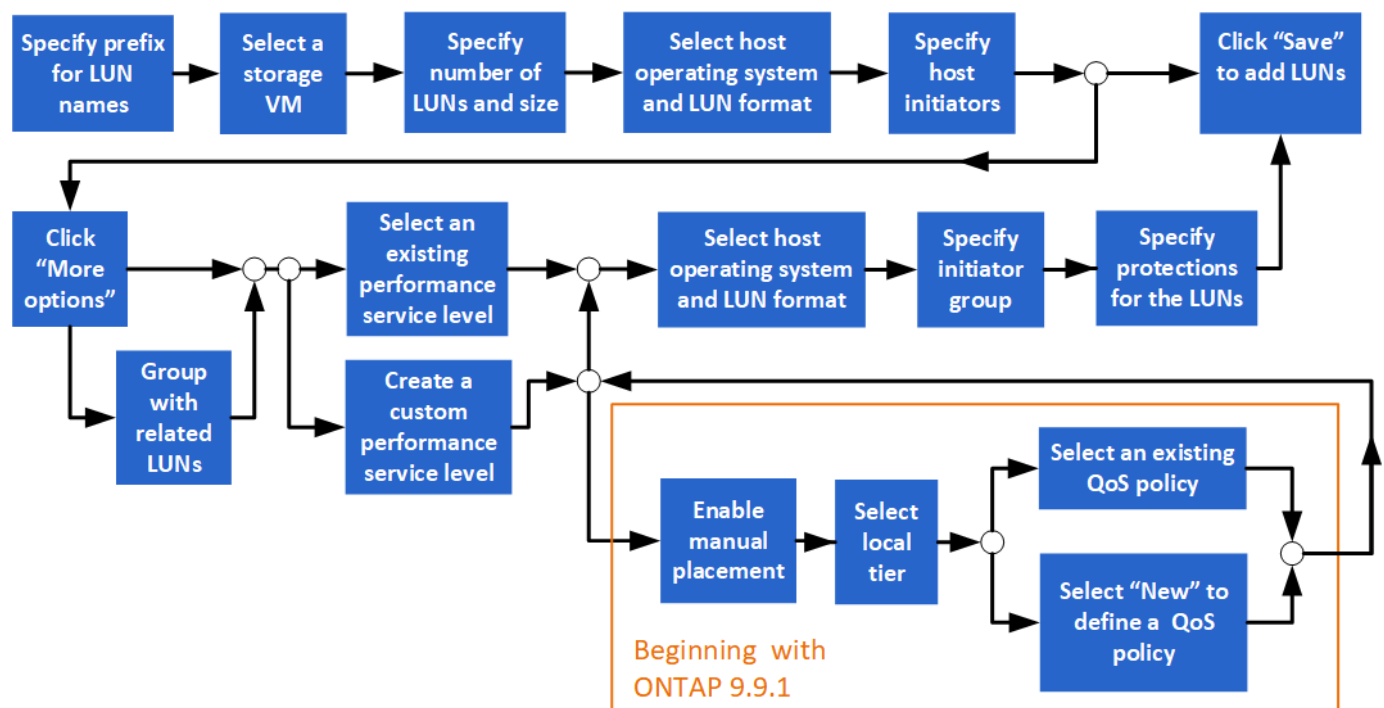
### Fasi

1. Rinominare il volume.
2. Impostare un percorso di giunzione (NAS).
3. Creare mappature per LUN nel volume (SAN).
4. Associare un criterio Snapshot e un criterio di esportazione al volume.
5. Aggiungere nuove regole dei criteri di quota per il volume.
6. Aggiungere un criterio QOS per il volume.

## Gestire le LUN

È possibile creare LUN e aggiungerli a una VM di storage esistente configurata con il protocollo SAN. È inoltre possibile raggruppare i LUN o rinominarli.

### Aggiungere LUN



### Prima di iniziare

Nel cluster dovrebbe essere presente una VM di storage configurata per il servizio SAN.

## Fasi

1. Accedere a **Storage > LUN**.
2. Fare clic su **+ Add**.
3. Specificare un prefisso da utilizzare all'inizio di ogni nome LUN. Se si crea un solo LUN, immettere il nome del LUN.
4. Selezionare una VM di storage dall'elenco a discesa.

Vengono elencate solo le VM di storage configurate per il protocollo SAN. Se è disponibile una sola VM di storage configurata per il protocollo SAN, il campo **Storage VM** non viene visualizzato.

5. Indicare il numero di LUN che si desidera creare e le dimensioni di ogni LUN.
6. Selezionare il sistema operativo host e il formato LUN dagli elenchi a discesa.
7. Inserire gli iniziatori host e separarli con virgole.
8. Eseguire una delle seguenti operazioni:

Fare clic su questo pulsante...	Per eseguire questa azione...
<b>Salva</b>	I LUN vengono creati con le specifiche inserite. Le impostazioni predefinite del sistema vengono utilizzate per altre specifiche. Non sono necessari passaggi aggiuntivi.
<b>Altre opzioni</b>	Passare a. <a href="#">[step9-define-add-specs]</a> Per definire specifiche aggiuntive per i LUN.

9. [\[\[fase 9-define-add-specs,fase 9\]\]](#) il prefisso LUN è già visualizzato se è stato immesso in precedenza, ma è possibile modificarlo. In caso contrario, inserire il prefisso.
10. Selezionare una VM di storage dall'elenco a discesa.

Vengono elencate solo le VM di storage configurate per il protocollo SAN. Se è disponibile una sola VM di storage configurata per il protocollo SAN, il campo **Storage VM** non viene visualizzato.

11. Determinare come si desidera raggruppare le LUN:

Quando fai questa scelta...	Ciò si verifica...
<b>Gruppo con LUN correlate</b>	Le LUN verranno raggruppate insieme alle LUN correlate su un volume esistente nella VM di storage.
Nessuna selezione	Le LUN verranno raggruppate su un volume chiamato "container".

12. Nella sezione **Storage and Optimization**, specificare i seguenti valori:
  - a. Il numero e la capacità dei LUN sono già visualizzati se precedentemente inseriti, ma è possibile modificarli. In caso contrario, inserire i valori.
  - b. Nel campo **Performance Service Level**, selezionare un livello di servizio:

Quando si seleziona questo livello di servizio...	Ciò si verifica...
---	--------------------

Un livello di servizio esistente, ad esempio "Extreme", "Performance" o "Value".  Vengono visualizzati solo i livelli di servizio validi per la piattaforma di sistema (AFF, FAS o altri).	Viene selezionato automaticamente un Tier locale. Passare a. <a href="#">fase 13</a> .
Personalizzato	Passare a. <a href="#">step12c</a> per definire un nuovo livello di servizio.

- c. [[fase 12c, fase 12c]] a partire da ONTAP 9.9.1, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale su cui si desidera inserire le LUN che si desidera creare (se è stato selezionato il livello di servizio "personalizzato").

Quando fai questa scelta...	Eseguire questi passaggi...
<b>Posizionamento manuale</b>	Il posizionamento manuale è attivato. Passare a. <a href="#">step12d</a> per completare il processo.
Nessuna selezione	La selezione manuale non è abilitata. Il Tier locale viene selezionato automaticamente. Passare a. <a href="#">fase 13</a> .

- d. [[fase 12d, fase 12d]]selezionare un livello locale dal menu a discesa.

- e. Selezionare un criterio QoS.

Selezionare "esistente" per scegliere da un elenco di policy esistenti oppure selezionare "nuovo" per inserire le specifiche di una nuova policy.

13. nella sezione **informazioni host**, il sistema operativo host e il formato LUN sono già visualizzati, ma è possibile modificarli.

14. In **host Mapping**, selezionare il tipo di iniziatori per i LUN:

- **Existing Initiator group** (Gruppo iniziatore esistente): Selezionare un gruppo iniziatore per l'elenco visualizzato.
- **Nuovo gruppo iniziatore che utilizza gruppi iniziatore esistenti**: Specificare il nome del nuovo gruppo e selezionare il gruppo o i gruppi che si desidera utilizzare per creare il nuovo gruppo.
- **Host initiator**: Specificare un nome dal nuovo gruppo di iniziatori e fare clic su **+Add Initiator** per aggiungere gli iniziatori al gruppo.

15. Nella sezione **protezione**, specificare le protezioni per i LUN.

Se si seleziona **Enable SnapMirror (Local or Remote)** (attiva SnapMirror (locale o remoto)), specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.

16. Fare clic su **Save** (Salva).

Le LUN vengono create e aggiunte alla VM del cluster e dello storage.




Puoi anche salvare le specifiche di questi LUN in un Ansible Playbook. Per ulteriori informazioni, visitare il sito Web all'indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

## Rinominare un LUN

È possibile rinominare un LUN dalla pagina di panoramica.

### Fasi

1. In System Manager, fare clic su **LUN**.
2. Fare clic su  Accanto al nome del LUN che si desidera rinominare, quindi modificare il nome del LUN.
3. Fare clic su **Save** (Salva).

## Espandere lo storage

Con System Manager, è possibile aumentare le dimensioni del volume o del LUN in modo che sia disponibile più spazio per l'host. Le dimensioni di un LUN non possono superare quelle del volume contenente.

A partire da ONTAP 9.12.1, quando si inserisce la nuova capacità di un volume, la finestra **Ridimensiona volume** mostra l'impatto che il ridimensionamento del volume avrà sullo spazio dati e sulla riserva di copia Snapshot.

- [Aumentare le dimensioni di un volume](#)
- [Aumentare le dimensioni di un LUN](#)


Inoltre, è possibile aggiungere un LUN a un volume esistente. I processi sono diversi quando si utilizza Gestione sistema con ONTAP 9.7 o 9.8

- [Aggiunta di un LUN a un volume esistente \(ONTAP 9.7\)](#)
- [Aggiunta di un LUN a un volume esistente \(ONTAP 9.8\)](#)

Inoltre, a partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per aggiungere un LUN a un volume esistente.


## Aumentare le dimensioni di un volume

### Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Posizionare il puntatore del mouse sul nome del volume che si desidera aumentare.
3. Fare clic su .
4. Selezionare **Modifica**.
5. Aumentare il valore della capacità.
6. Esaminare i dettagli dello spazio dati **esistente** e **nuovo** e della riserva Snapshot.

## Aumentare le dimensioni di un LUN

### Fasi

1. Fare clic su **Storage > LUN**.
2. Posizionare il puntatore del mouse sul nome del LUN che si desidera aumentare.
3. Fare clic su .

4. Selezionare **Modifica**.
5. Aumentare il valore della capacità.

### Aggiunta di un LUN a un volume esistente (ONTAP 9.7)

Per utilizzare Gestione sistema con ONTAP 9.7 per aggiungere un LUN a un volume esistente, passare prima alla visualizzazione classica.

#### Fasi

1. Accedere a Gestore di sistema in ONTAP 9.7.
2. Fare clic su **visualizzazione classica**.
3. Selezionare **Storage > LUN > Create** (archiviazione > LUN > Crea)
4. Specificare i dettagli per la creazione del LUN.
5. Specificare a quale volume o qtree esistente aggiungere il LUN.

### Aggiunta di un LUN a un volume esistente (ONTAP 9.8)

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per aggiungere un LUN a un volume esistente che dispone già di almeno un LUN.

#### Fasi

1. Fare clic su **Storage > LUN**.
2. Fare clic su **Aggiungi+**.
3. Compilare i campi nella finestra **Add LUN** (Aggiungi LUN).
4. Selezionare **altre opzioni**.
5. Selezionare la casella di controllo **Group with Related LUN** (Gruppo con LUN correlati).
6. Nel campo a discesa, selezionare un LUN esistente nel volume al quale si desidera aggiungere un altro LUN.
7. Completare gli altri campi. Per **host Mapping**, fare clic su uno dei pulsanti di opzione:
  - **Existing Initiator Group** (Gruppo iniziatore esistente) consente di selezionare un gruppo esistente da un elenco.
  - **New Initiator group** consente di inserire un nuovo gruppo nel campo.

### Risparmiare spazio di storage utilizzando compressione, compattazione e deduplica


Per i volumi su cluster non AFF, è possibile eseguire la deduplica, la compressione dei dati e la compattazione dei dati insieme o indipendentemente per ottenere risparmi di spazio ottimali.

- La deduplica elimina i blocchi di dati duplicati.
- La compressione dei dati comprime i blocchi di dati per ridurre la quantità di storage fisico richiesta.
- La compattazione dei dati memorizza più dati in meno spazio per aumentare l'efficienza dello storage.



Queste attività sono supportate per i volumi su cluster non AFF. A partire da ONTAP 9.2, tutte le funzionalità di efficienza dello storage inline, come la deduplica inline e la compressione inline, sono attivate per impostazione predefinita sui volumi AFF.

## Fasi

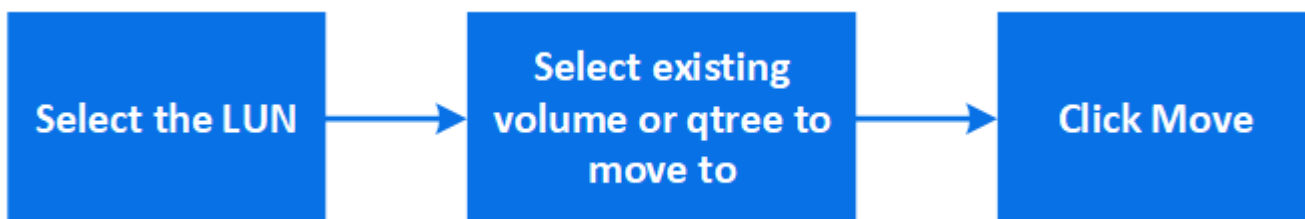
1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Accanto al nome del volume per il quale si desidera salvare lo storage, fare clic su .
3. Fare clic su **Edit** (Modifica) e scorrere fino a **Storage Efficiency** (efficienza dello storage).
4. *Opzionale*: Se si desidera attivare la deduplica in background, assicurarsi che la casella di controllo sia selezionata.
5. *Opzionale*: Se si desidera attivare la compressione in background, specificare il criterio di efficienza dello storage e assicurarsi che la casella di controllo sia selezionata.
6. *Opzionale*: Se si desidera attivare la compressione inline, assicurarsi che la casella di controllo sia selezionata.

## Bilanciare i carichi spostando le LUN

È possibile spostare un LUN in un altro volume all'interno della VM di storage per bilanciare il carico oppure spostarlo in un volume con un livello di servizio dalle performance più elevate per migliorare le performance.

### Spostare le restrizioni

- Un LUN non può essere spostato in un qtree all'interno dello stesso volume.
- Un LUN creato da un file utilizzando la CLI non può essere spostato con System Manager.
- Le LUN in linea e che forniscono dati non possono essere spostate.
- Non è possibile spostare i LUN se lo spazio allocato nel volume di destinazione non può contenere il LUN (anche se sul volume è attivata la funzione di crescita automatica).
- I LUN sui volumi SnapLock non possono essere spostati con Gestore di sistema.



## Fasi

1. Fare clic su **Storage > LUN**.
2. Selezionare il LUN che si desidera spostare e fare clic su **Sposta**.
3. Selezionare un volume esistente in cui si desidera spostare il LUN. Se il volume contiene qtree, selezionare il qtree.



Durante l'operazione di spostamento, il LUN viene visualizzato sia sul volume di origine che su quello di destinazione.

## Bilanciare i carichi spostando i volumi su un altro Tier

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per spostare un volume in un altro Tier per bilanciare il carico.

A partire da ONTAP 9.9.1, è anche possibile spostare i volumi in base all'analisi dello storage dei dati attivo e inattivo. Per ulteriori informazioni, vedere ["Panoramica di file System Analytics"](#).

### Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare il volume o i volumi che si desidera spostare, quindi fare clic su **Move** (Sposta).
3. Selezionare un Tier (aggregato) esistente in cui spostare il volume o i volumi.

## Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN

A partire da ONTAP 9.9.1, è possibile utilizzare i Playbook Ansible con Gestione di sistema per aggiungere o modificare volumi o LUN.

Questa funzione consente di utilizzare la stessa configurazione più volte o la stessa configurazione con lievi modifiche quando si aggiungono o modificano volumi o LUN.

### Attiva o disattiva i Playbook Ansible

È possibile attivare o disattivare l'utilizzo di Ansible Playbook con System Manager.

### Fasi

1. In System Manager, accedere alle impostazioni dell'interfaccia utente nella pagina delle impostazioni del cluster:

#### **Cluster > Impostazioni**

2. In **UI Settings** (Impostazioni interfaccia utente), impostare il cursore su "Enabled" (attivato) o "Disabled" (Disattivato).

### Salvare la configurazione di un volume in un Ansible Playbook

Quando si crea o si modifica la configurazione di un volume, è possibile salvare la configurazione come file Ansible Playbook.

### Fasi

1. Aggiungere o modificare il volume:

#### **Volume > Add** (oppure **Volume > Edit**)

2. Specificare o modificare i valori di configurazione del volume.
3. Selezionare **Salva in Ansible Playbook** per salvare la configurazione in Ansible Playbook Files.

Viene scaricato un file zip contenente i seguenti file:

- **variable.yaml**: I valori immessi o modificati per aggiungere o modificare il volume.
- **volumeAdd.yaml** (o **volumeEdit.yaml**): I casi di test necessari per creare o modificare i valori



durante la lettura degli input da `variable.yaml` file.

## Salvare una configurazione LUN in un Ansible Playbook

Quando si crea o si modifica la configurazione di un LUN, è possibile salvare la configurazione come file Ansible Playbook.

### Fasi

1. Aggiungere o modificare il LUN:

**LUN > Add** (o **LUN > Edit**)

2. Specificare o modificare i valori di configurazione del LUN.
3. Selezionare **Salva in Ansible Playbook** per salvare la configurazione in Ansible Playbook Files:


Viene scaricato un file zip contenente i seguenti file:

- **variable.yaml**: I valori immessi o modificati per aggiungere o modificare il LUN.
- **lunAdd.yaml** (o **lunEdit.yaml**): I casi di test necessari per creare o modificare i valori durante la lettura degli input da `variable.yaml` file.

## Scarica i file di Ansible Playbook dai risultati della ricerca globale

Puoi scaricare i file di Ansible Playbook quando effettui una ricerca globale.

### Fasi

1. Nel campo di ricerca, immettere "volume", "LUN" o "Playbook".
2. Trovare il risultato della ricerca, "Volume Management (Ansible Playbook)" o "LUN Management (Ansible Playbook)".
3. Fare clic su  Per scaricare i file di Ansible Playbook.

## Utilizzare i file Ansible Playbook

I file Ansible Playbook possono essere modificati ed eseguiti per specificare le configurazioni per volumi e LUN.

### A proposito di questa attività

Si utilizzano due file per eseguire un'operazione (aggiunta o modifica):

Se si desidera...	USA questo file variabile...	E utilizzare questo file di esecuzione...
Aggiungere un volume	volumeAdd-variable.yaml	valueAdd.yaml
Modificare un volume	volumeEdit-variable.yaml	volumeEdit.yaml
Aggiungere un LUN	lunAdd-variable.yaml	lunAdd.yaml
Modificare un LUN	lunEdit-variable.yaml	lunEdit.yaml

### Fasi

### 1. Modificare il file delle variabili.

Il file contiene i diversi valori utilizzati per configurare il volume o il LUN.

- Se non si modificano i valori, lasciarli commentati.
- Se si modificano i valori, rimuovere i commenti.

### 2. Eseguire il file di esecuzione associato.

Il file di esecuzione contiene i casi di test necessari per creare o modificare i valori durante la lettura degli input dal file variabile.

### 3. Immettere le credenziali di accesso utente.

## Gestire le policy di efficienza dello storage

A partire da ONTAP 9.8, è possibile utilizzare Gestione di sistema per attivare, disattivare, aggiungere, modificare o eliminare le policy di efficienza per le VM di storage sui sistemi FAS.



Questa funzione non è disponibile sui sistemi AFF.

### Fasi

1. Selezionare **Storage > Storage VM**
2. Selezionare la VM di storage per la quale si desidera gestire le policy di efficienza.
3. Nella scheda **Impostazioni**, selezionare ➔ Nella sezione **Efficiency Policy**. Vengono visualizzate le policy di efficienza per la VM di storage.

È possibile eseguire le seguenti operazioni:

- **Attivare o disattivare** una policy di efficienza facendo clic sul pulsante di commutazione nella colonna Status (Stato).
- **Aggiungere** una policy di efficienza facendo clic su **Add+**.
- **Modificare** una policy di efficienza facendo clic su A destra del nome del criterio e selezionando **Modifica**.
- **Eliminare** una policy di efficienza facendo clic su A destra del nome del criterio e selezionando **Delete** (Elimina).

### Elenco delle policy di efficienza

#### • Auto

Specifica che la deduplica viene eseguita continuamente in background. Questo criterio viene impostato per tutti i volumi appena creati e per tutti i volumi aggiornati che non sono stati configurati manualmente per la deduplica in background. Se si modifica il criterio in “default” o in qualsiasi altro criterio, il criterio “auto” viene disattivato.

Se un volume si sposta da un sistema non AFF a un sistema AFF, il criterio “auto” viene attivato sul nodo di destinazione per impostazione predefinita. Se un volume si sposta da un nodo AFF a un nodo non AFF, il criterio “auto” sul nodo di destinazione viene sostituito per impostazione predefinita dal criterio “inline-only”.

- **Policy**

Specifica il nome di una policy di efficienza.

- **Stato**

Specifica lo stato di una policy di efficienza. Lo stato può essere uno dei seguenti:

- Attivato

Specifica che la policy di efficienza può essere assegnata a un'operazione di deduplica.

- Disattivato

Specifica che la policy di efficienza è disattivata. È possibile attivare il criterio utilizzando il menu a discesa status (Stato) e assegnarlo successivamente a un'operazione di deduplica.

- **Esegui da**

Specifica se la policy di efficienza dello storage viene eseguita in base a una pianificazione o a un valore di soglia (modifica soglia log).

- **Policy QoS**

Specifica il tipo di QoS per la policy di efficienza dello storage. Il tipo di QoS può essere uno dei seguenti:

- Sfondo

Specifica che il criterio QoS è in esecuzione in background, riducendo il potenziale impatto delle performance sulle operazioni del client.

- Best-effort

Specifica che il criterio QoS viene eseguito con il massimo sforzo, consentendo di massimizzare l'utilizzo delle risorse di sistema.

- **Durata massima**

Specifica la durata massima del run-time di una policy di efficienza. Se questo valore non viene specificato, il criterio di efficienza viene eseguito fino al completamento dell'operazione.

## **Area dei dettagli**

L'area sotto l'elenco dei criteri di efficienza visualizza informazioni aggiuntive sulla policy di efficienza selezionata, tra cui il nome della pianificazione e i dettagli della pianificazione per una policy basata sulla pianificazione e il valore di soglia per una policy basata sulla soglia.

## **Gestire le risorse utilizzando le quote**

A partire da ONTAP 9.7, è possibile configurare e gestire le quote di utilizzo con Gestore di sistema.

Se si utilizza l'interfaccia utente di ONTAP per configurare e gestire le quote di utilizzo, fare riferimento a ["Gestione dello storage logico"](#).

Se si utilizza Gestione di sistema OnCommand legacy per ONTAP 9.7 e versioni precedenti per configurare e gestire le quote di utilizzo, vedere quanto segue per la versione in uso:

- ["Documentazione di ONTAP 9.6 e 9.7"](#)
- ["Documentazione di ONTAP 9.5"](#)
- ["Documentazione di ONTAP 9.4"](#)
- ["Documentazione di ONTAP 9.3"](#)
- ["Documentazione archiviata di ONTAP 9.2"](#)
- ["Documentazione archiviata di ONTAP 9.0"](#)

## Panoramica delle quote

Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree. Le quote vengono applicate a un volume o qtree specifico.

È possibile utilizzare le quote per tenere traccia e limitare l'utilizzo delle risorse nei volumi e fornire una notifica quando l'utilizzo delle risorse raggiunge livelli specifici.

Le quote possono essere morbide o difficili. Le quote morbide fanno sì che ONTAP invii una notifica quando vengono superati i limiti specificati, mentre le quote rigide impediscono il successo di un'operazione di scrittura quando vengono superati i limiti specificati.

## Impostare le quote per limitare l'utilizzo delle risorse

Aggiungere quote per limitare la quantità di spazio su disco che la destinazione della quota può utilizzare.

È possibile impostare un limite massimo e un limite massimo per una quota.

Le quote rigide impongono un limite massimo alle risorse di sistema; qualsiasi operazione che comporterebbe il superamento del limite fallisce. Le quote morbide inviano un messaggio di avviso quando l'utilizzo delle risorse raggiunge un determinato livello, ma non influiscono sulle operazioni di accesso ai dati, in modo da poter intraprendere le azioni appropriate prima che la quota venga superata.

### Fasi

1. Fare clic su **Storage > quote**.
2. Fare clic su **Aggiungi**.

## Clonare volumi e LUN per il test

È possibile clonare volumi e LUN per creare copie temporanee e scrivibili per il test. I cloni riflettono lo stato attuale e point-in-time dei dati. È inoltre possibile utilizzare i cloni per fornire agli utenti aggiuntivi l'accesso ai dati senza fornire loro l'accesso ai dati di produzione.




La licenza FlexClone deve essere di **"installato"** sul sistema storage.

## Clonare un volume

Creare un clone di un volume, come segue:

### Fasi


1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Fare clic su  accanto al nome del volume che si desidera clonare.
3. Selezionare **Clone** dall'elenco.
4. Specificare un nome per il clone e completare le altre selezioni.
5. Fare clic su **Clone** e verificare che il clone del volume compaia nell'elenco dei volumi.

In alternativa, è possibile clonare un volume da **Overview** (Panoramica) che viene visualizzato quando si visualizzano i dettagli del volume.

## Clonazione di un LUN

Creare un clone di un LUN, come segue:

### Fasi

1. Fare clic su **Storage > LUN**.
2. Fare clic su  Accanto al nome del LUN che si desidera clonare.
3. Selezionare **Clone** dall'elenco.
4. Specificare un nome per il clone e completare le altre selezioni.
5. Fare clic su **Clone** e verificare che il clone del LUN compaia nell'elenco delle LUN.

In alternativa, è possibile clonare un LUN dalla schermata **Overview** (Panoramica) che viene visualizzata quando si visualizzano i dettagli del LUN.

Quando si crea un clone del LUN, System Manager attiva automaticamente l'eliminazione del clone quando è necessario spazio.

## Cercare, filtrare e ordinare le informazioni in System Manager

In System Manager è possibile cercare azioni, oggetti e informazioni. È inoltre possibile cercare dati di tabella per voci specifiche.

System Manager offre due tipi di ricerca:

- [Ricerca globale](#)

Quando si inserisce un argomento di ricerca nel campo nella parte superiore di ogni pagina, System Manager ricerca le corrispondenze nell'interfaccia. È quindi possibile ordinare e filtrare i risultati.

A partire da ONTAP 9.12.1, System Manager fornisce anche i risultati della ricerca dal sito di supporto NetApp per fornire collegamenti alle informazioni di supporto pertinenti.

- [Ricerca tabella-griglia](#)

A partire da ONTAP 9.8, quando si inserisce un argomento di ricerca nel campo nella parte superiore della griglia di una tabella, Gestore di sistema ricerca solo le colonne e le righe della tabella per trovare le

corrispondenze.

## Ricerca globale

Nella parte superiore di ogni pagina di System Manager, è possibile utilizzare un campo di ricerca globale per cercare vari oggetti e azioni nell'interfaccia. Ad esempio, è possibile cercare diversi oggetti per nome, pagine disponibili nella colonna del navigatore (a sinistra), varie azioni, come "Add Volume" (Aggiungi volume) o "Add License" (Aggiungi licenza) e collegamenti ad argomenti esterni della guida. È inoltre possibile filtrare e ordinare i risultati.



Per ottenere risultati migliori, eseguire ricerche, filtrare e ordinare un minuto dopo l'accesso e cinque minuti dopo la creazione, la modifica o l'eliminazione di un oggetto.

### Ottenere i risultati della ricerca

La ricerca non fa distinzione tra maiuscole e minuscole. È possibile immettere una serie di stringhe di testo per trovare la pagina, le azioni o gli argomenti delle informazioni necessari. Vengono elencati fino a 20 risultati. Se vengono trovati altri risultati, fare clic su **Mostra altri** per visualizzare tutti i risultati. I seguenti esempi descrivono le ricerche tipiche:

Tipo di ricerca	Stringa di ricerca di esempio	Risultati di ricerca di esempio
Per nome oggetto	vol_	Vol_lun_dest su storage VM: Svm0 (volume) /vol/vol...est1/lun su storage VM: Svm0 (LUN) svm0:vol_lun_dest1 ruolo: Destinazione (relazione)
Per posizione nell'interfaccia	volume	Add Volume (azione) Protection – Overview (pagina) Recover deleted volume (Guida)
Per azioni	aggiungi	Add Volume (Action) Network (Aggiungi rete volume (azione)) - Panoramica (pagina) Expand Volumes and LUN (Espandi volumi e LUN) (Guida)
Per contenuto della guida	san	Storage – Panoramica (pagina) Panoramica SAN (Guida) Provision SAN storage for databases (Guida)

### Risultati della ricerca globale dal sito di supporto NetApp



A partire da ONTAP 9.12.1, per gli utenti registrati con Active IQ, System Manager visualizza un'altra colonna di risultati che fornisce collegamenti alle informazioni sul sito di supporto NetApp, incluse le informazioni sul prodotto System Manager.

I risultati della ricerca contengono le seguenti informazioni:

- **Titolo** delle informazioni che costituiscono un link al documento in formato HTML, PDF, EPUB o altro.
- **Tipo di contenuto**, che identifica se si tratta di un argomento della documentazione del prodotto, di un articolo della Knowledge base o di un altro tipo di informazioni.
- **Descrizione sintetica** del contenuto.

- Data **creata** della prima pubblicazione.
- **Updated** data dell'ultimo aggiornamento.

È possibile eseguire le seguenti operazioni:


Azione	Risultato
Fare clic su <b>Gestore di sistema di ONTAP</b> , quindi immettere il testo nel campo di ricerca.	I risultati della ricerca includono informazioni sul sito di supporto NetApp relative a System Manager.
Fare clic su <b>tutti i prodotti</b> , quindi inserire il testo nel campo di ricerca.	I risultati della ricerca includono informazioni sul sito di supporto NetApp per tutti i prodotti NetApp, non solo per System Manager.
Fare clic su un risultato della ricerca.	Le informazioni del NetApp Support Site vengono visualizzate in una finestra o in una scheda separata del browser.
Fare clic su <b>Visualizza altri risultati</b> .	Se sono presenti più di dieci risultati, fare clic su <b>Visualizza altri risultati</b> dopo il decimo risultato per visualizzare altri risultati. Ogni volta che si fa clic su <b>Visualizza altri risultati</b> , vengono visualizzati altri dieci risultati, se disponibili.
Copia il link.	Il collegamento viene copiato negli Appunti. È possibile incollare il collegamento in un file o in una finestra del browser.
Fare clic su  .	Il pannello in cui vengono visualizzati i risultati viene bloccato in modo che rimanga visualizzato quando si lavora in un altro pannello.
Fare clic su  .	Il pannello dei risultati non è più bloccato e viene chiuso.

#### Filtraggio dei risultati della ricerca

È possibile restringere i risultati con filtri, come illustrato negli esempi seguenti:

Filtro	Sintassi	Stringa di ricerca di esempio
Per tipo di oggetto	<type>: <objectName>	volume:vol_2
In base alla dimensione dell'oggetto	<type> <size-symbol> <number> <units>	lun<500 mb
Da dischi rotti	"disco rotto" o "disco non integro"	disco non integro
Per interfaccia di rete	<IP address>	172.22.108.21

#### Ordinamento dei risultati della ricerca

Quando visualizzi tutti i risultati della ricerca, vengono ordinati in ordine alfabetico. È possibile ordinare i risultati facendo clic su  **Filter** e selezionare la modalità di ordinamento dei risultati.

## Ricerca tabella-griglia

A partire da ONTAP 9.8, ogni volta che Gestione sistema visualizza le informazioni in formato tabella-griglia, viene visualizzato un pulsante di ricerca nella parte superiore della tabella.

Quando si fa clic su **Cerca**, viene visualizzato un campo di testo in cui è possibile inserire un argomento di ricerca. System Manager ricerca l'intera tabella e visualizza solo le righe che contengono testo corrispondente all'argomento di ricerca.

È possibile utilizzare un asterisco ( \* ) come carattere "jolly" in sostituzione dei caratteri. Ad esempio, la ricerca `vol1*` potrebbe fornire righe che contengono quanto segue:

- Vol\_122\_D9
- vol\_lun\_dest1
- vol2866
- volspec1
- volum\_dest\_765
- volume
- volume\_new4
- volume9987

## Misurazioni della capacità in System Manager

La capacità del sistema può essere misurata come spazio fisico o spazio logico. A partire da ONTAP 9.7, System Manager fornisce misurazioni della capacità fisica e logica.

Le differenze tra le due misurazioni sono spiegate nelle seguenti descrizioni:

- **Capacità fisica:** Lo spazio fisico si riferisce ai blocchi fisici di storage utilizzati nel volume o nel Tier locale. Il valore della capacità fisica utilizzata è in genere inferiore al valore della capacità logica utilizzata a causa della riduzione dei dati dalle funzionalità di efficienza dello storage (come deduplica e compressione).
- **Capacità logica:** Lo spazio logico si riferisce allo spazio utilizzabile (i blocchi logici) in un volume o in un Tier locale. Lo spazio logico si riferisce al modo in cui lo spazio teorico può essere utilizzato, senza tenere conto dei risultati della deduplica o della compressione. Il valore dello spazio logico utilizzato deriva dalla quantità di spazio fisico utilizzato e dai risparmi derivanti dalle funzionalità di efficienza dello storage (come deduplica e compressione) configurate. Questa misurazione appare spesso più grande della capacità fisica utilizzata perché include copie Snapshot, cloni e altri componenti e non riflette la compressione dei dati e altre riduzioni dello spazio fisico. Pertanto, la capacità logica totale potrebbe essere superiore allo spazio fornito.



In System Manager, le rappresentazioni della capacità non tengono conto delle capacità del Tier storage root (aggregato).

## Misurazioni della capacità utilizzata

Le misurazioni della capacità utilizzata vengono visualizzate in modo diverso a seconda della versione di System Manager in uso, come illustrato nella seguente tabella:



Versione di System Manager	Termine utilizzato per la capacità	Tipo di capacità a cui si fa riferimento
9.9.1 e versioni successive	Logica utilizzata	Spazio logico utilizzato se sono state attivate le impostazioni di efficienza dello storage)
9.7 e 9.8	Utilizzato	Spazio logico utilizzato (se sono state attivate le impostazioni di efficienza dello storage)
9.5 e 9.6 (visualizzazione classica)	Utilizzato	Spazio fisico utilizzato

### Termini di misurazione della capacità

Quando si descrive la capacità, vengono utilizzati i seguenti termini:

- **Capacità allocata:** Quantità di spazio allocato per i volumi in una VM di storage.
- **Available:** La quantità di spazio fisico disponibile per memorizzare i dati o per eseguire il provisioning dei volumi in una VM di storage o su un Tier locale.
- **Capacità tra volumi:** La somma dello storage utilizzato e dello storage disponibile di tutti i volumi su una VM di storage.
- **Dati del client:** Quantità di spazio utilizzata dai dati del client (fisici o logici).
  - A partire da ONTAP 9.13.1, la capacità utilizzata dai dati del client viene definita **uso logico** e la capacità utilizzata dalle copie Snapshot viene visualizzata separatamente.
  - In ONTAP 9.12.1 e versioni precedenti, la capacità utilizzata dai dati del client aggiunta alla capacità utilizzata dalle copie Snapshot viene definita **logica utilizzata**.
- **Impegnato:** Quantità di capacità impegnata per un Tier locale.
- **Riduzione dei dati:**
  - A partire da ONTAP 9.13.1, i rapporti di riduzione dei dati vengono visualizzati come segue:
    - Il valore di riduzione dei dati visualizzato sul pannello **Capacity** è il rapporto tra lo spazio logico utilizzato e lo spazio fisico utilizzato senza considerare le riduzioni significative ottenute utilizzando le funzionalità di efficienza dello storage, come le copie Snapshot.
    - Quando si visualizza il pannello dei dettagli, vengono visualizzati sia il rapporto visualizzato nel pannello di panoramica che il rapporto complessivo di tutto lo spazio logico utilizzato rispetto allo spazio fisico utilizzato. Definito **con copie Snapshot**, questo valore include i benefici derivanti dall'utilizzo di copie Snapshot e altre funzionalità di efficienza dello storage.
  - In ONTAP 9.12.1 e versioni precedenti, i rapporti di riduzione dei dati vengono visualizzati come segue:
    - Il valore di riduzione dei dati visualizzato sul pannello **Capacity** è il rapporto complessivo di tutto lo spazio logico utilizzato rispetto allo spazio fisico utilizzato e include i benefici derivanti dall'utilizzo di copie Snapshot e altre funzionalità di efficienza dello storage.
    - Quando si visualizza il pannello dei dettagli, vengono visualizzati il rapporto **complessivo** visualizzato nel pannello di panoramica e il rapporto dello spazio logico utilizzato solo dai dati del client rispetto allo spazio fisico utilizzato solo dai dati del client, denominato **senza copie Snapshot e cloni**.

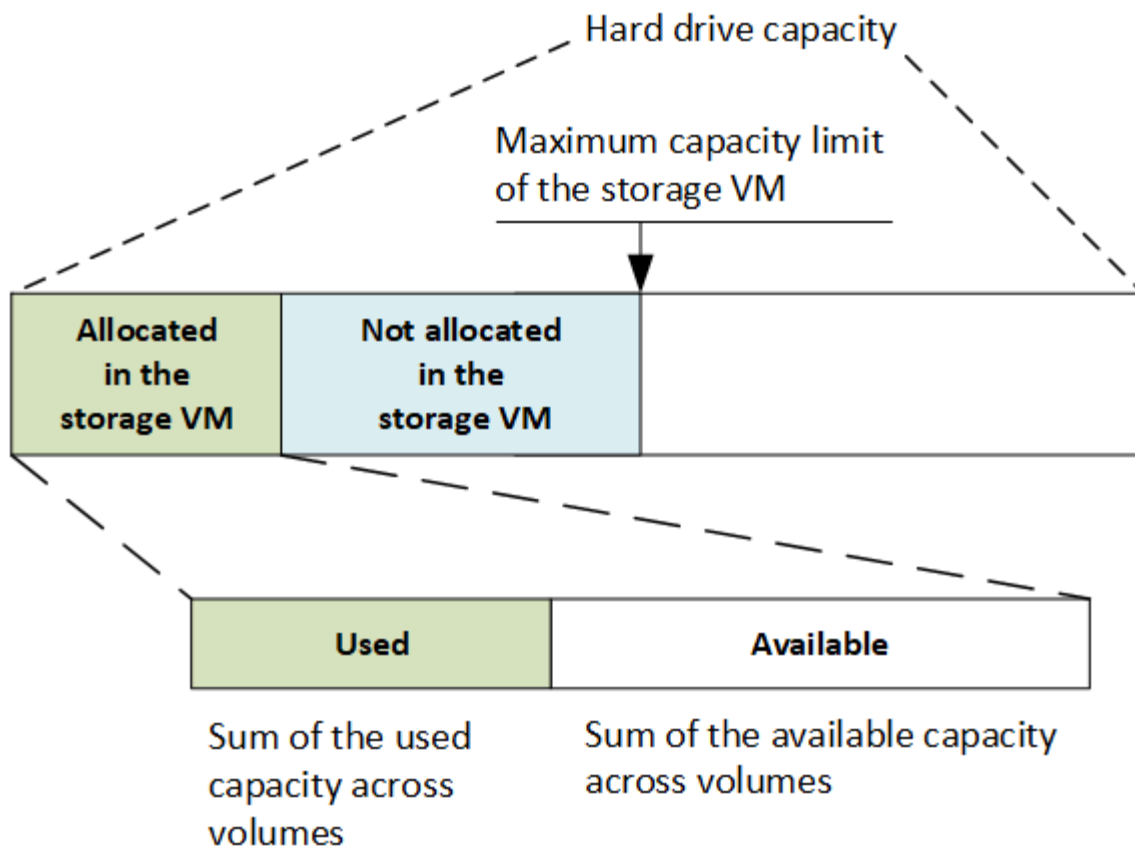
- **Logica utilizzata:**
  - A partire da ONTAP 9.13.1, la capacità utilizzata dai dati del client viene definita **uso logico** e la capacità utilizzata dalle copie Snapshot viene visualizzata separatamente.
  - In ONTAP 9.12.1 e versioni precedenti, la capacità utilizzata dai dati client aggiunti alla capacità utilizzata dalle copie Snapshot viene definita **logica utilizzata**.
- **Logical used %:** Percentuale della capacità logica utilizzata corrente rispetto alle dimensioni fornite, escluse le riserve Snapshot. Questo valore può essere superiore al 100%, perché include risparmi di efficienza nel volume.
- **Capacità massima:** Quantità massima di spazio allocato per i volumi su una VM di storage.
- **Fisico utilizzato:** La quantità di capacità utilizzata nei blocchi fisici di un volume o di un Tier locale.
- **Physical used %:** Percentuale di capacità utilizzata nei blocchi fisici di un volume rispetto alle dimensioni del provisioning.
- **Capacità di provisioning:** Un file system (volume) allocato da un sistema Cloud Volumes ONTAP ed pronto per l'archiviazione dei dati dell'utente o dell'applicazione.
- **Reserved:** Quantità di spazio riservato ai volumi già sottoposti a provisioning in un Tier locale.
- **Used:** Quantità di spazio che contiene dati.
- **Utilizzato e riservato:** La somma dello spazio fisico utilizzato e riservato.

## Capacità di una VM storage

La capacità massima di una VM di storage è determinata dallo spazio allocato totale per i volumi più lo spazio non allocato rimanente.

- Lo spazio allocato per i volumi è la somma della capacità utilizzata e della capacità disponibile di volumi FlexVol, FlexGroup e FlexCache.
- La capacità dei volumi viene inclusa nelle somme, anche quando sono limitate, offline o nella coda di ripristino dopo l'eliminazione.
- Se i volumi sono configurati con la crescita automatica, il valore massimo di dimensionamento automatico del volume viene utilizzato nelle somme. Senza la crescita automatica, la capacità effettiva del volume viene utilizzata nelle somme.

Il grafico seguente spiega come la misurazione della capacità tra i volumi si riferisce al limite massimo di capacità.



A partire da ONTAP 9.13.1, gli amministratori del cluster possono farlo ["Abilitare un limite massimo di capacità per una VM di storage"](#). Tuttavia, non è possibile impostare limiti di storage per una VM di storage che contiene volumi per la protezione dei dati, in una relazione SnapMirror o in una configurazione MetroCluster. Inoltre, le quote non possono essere configurate in modo da superare la capacità massima di una VM di storage.

Una volta impostato il limite massimo di capacità, non è possibile modificarlo in una dimensione inferiore alla capacità attualmente allocata.

Quando una VM di storage raggiunge il limite massimo di capacità, alcune operazioni non possono essere eseguite. System Manager fornisce suggerimenti per le fasi successive di ["Insights"](#).

## Unità di misura della capacità

System Manager calcola la capacità dello storage in base a unità binarie di 1024 ( $2^{10}$ ) byte.

- A partire da ONTAP 9.10.1, le unità di capacità dello storage vengono visualizzate in Gestione sistemi come KiB, MiB, GiB, TiB e PiB.
- In ONTAP 9.10.0 e versioni precedenti, queste unità vengono visualizzate in Gestione sistema come KB, MB, GB, TB e PB.



Le unità utilizzate in Gestione sistema per il throughput continuano a essere KB/s, MB/s, GB/s, TB/s e PB/s per tutte le release di ONTAP.

Unità di capacità visualizzata in Gestore di sistema per ONTAP 9.10.0 e versioni precedenti	Unità di capacità visualizzata in Gestore di sistema per ONTAP 9.10.1 e versioni successive	Calcolo	Valore in byte
KB	KiB	1024	1024 byte
MB	MiB	1024 * 1024	1,048,576 byte
GB	GiB	1024 * 1024 * 1024	1,073,741,824 byte
TB	TiB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 byte
PB	PiB	1024 * 1024 * 1024 * 1024 * 1024	1,125,899,906,842,624 byte

#### Informazioni correlate

["Monitorare la capacità in System Manager"](#)

["Creazione di report e applicazione dello spazio logico per i volumi"](#)

## Gestione dello storage logico con la CLI

### Panoramica sulla gestione dello storage logico con la CLI

Utilizzando l'interfaccia CLI di ONTAP, è possibile creare e gestire volumi FlexVol, utilizzare la tecnologia FlexClone per creare copie efficienti di volumi, file e LUN, creare qtree e quote e gestire funzionalità di efficienza come deduplica e compressione.

Attenersi alle seguenti procedure nei seguenti casi:

- Vuoi conoscere la gamma di funzionalità dei volumi ONTAP FlexVol e le funzionalità di efficienza dello storage.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

### Creare e gestire i volumi

#### Creare un volume

È possibile creare un volume e specificarne il punto di giunzione e altre proprietà utilizzando `volume create` comando.

#### A proposito di questa attività

Un volume deve includere un *percorso di giunzione* per rendere i dati disponibili ai client. È possibile specificare il percorso di giunzione quando si crea un nuovo volume. Se si crea un volume senza specificare un percorso di giunzione, è necessario *montare* il volume nello spazio dei nomi SVM utilizzando `volume`

mount comando.

## Prima di iniziare

- La SVM per il nuovo volume e l'aggregato che fornirà lo storage al volume devono già esistere.
- Se la SVM dispone di un elenco di aggregati associati, l'aggregato deve essere incluso nell'elenco.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilita analisi del file system](#).

## Fasi

### 1. Creare un volume:

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name  
-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -user  
user_name_or_number -group group_name_or_number -junction-path junction_path  
[-policy export_policy_name]
```

Il `-security style`, `-user`, `-group`, `-junction-path`, e. `-policy` Le opzioni sono solo per gli spazi dei nomi NAS.

Le scelte per `-junction-path` sono i seguenti:

- Direttamente sotto `root`, ad esempio `/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio direttamente nel volume `root` SVM.

- In una `directory` esistente, ad esempio `/existing_dir/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio in un volume esistente (in una gerarchia esistente), espresso come `directory`.

Se si desidera creare un volume in una nuova `directory` (in una nuova gerarchia sotto un nuovo volume), ad esempio, `/new_dir/new_vol`, Quindi, è necessario creare prima un nuovo volume padre che sia congiunto al volume `root` SVM. Creare quindi il nuovo volume figlio nel percorso di giunzione del nuovo volume padre (nuova `directory`).

### 2. Verificare che il volume sia stato creato con il punto di giunzione desiderato:

```
volume show -vserver svm_name -volume volume_name -junction
```

## Esempi

Il seguente comando crea un nuovo volume denominato `users1` sulla SVM `vs1.example.com` e l'aggregato `aggr1`. Il nuovo volume è disponibile all'indirizzo `/users`. Il volume ha una dimensione di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

Il seguente comando crea un nuovo volume denominato “home4” su SVM “vs1.example.com” e l’aggregato “aggr1”. La directory /eng/ Esiste già nello spazio dei nomi per vs1 SVM e il nuovo volume è disponibile all’indirizzo /eng/home, che diventa la home directory di /eng/ namespace. Il volume è di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

## Supporta volumi di grandi dimensioni e file di grandi dimensioni

A partire da ONTAP 9.12.1 P2, è possibile creare un nuovo volume o modificare un volume esistente per abilitare il supporto di dimensioni massime di un volume di 300TB TB e dimensioni massime di un file (LUN) di 128TB TB.

### Prima di iniziare

- Sul cluster viene installato ONTAP 9.12.1 P2 o versione successiva.
- Se abiliti il supporto di un volume di grandi dimensioni nel cluster di origine in una relazione SnapMirror, devi avere installato ONTAP 9.12.1 P2 o versioni successive nel cluster che ospita il volume di origine nonché il cluster che ospita il volume di destinazione.
- Sei un amministratore di cluster o SVM.

### Creare un nuovo volume

#### Fase

1. Creazione di un volume con supporto file e volumi di grandi dimensioni abilitato:

```
volume create -vserver _svm_name_ -volume _volume_name_ -aggregate  
_aggregate_name_ -is-large-size-enabled true
```

### Esempio

Nell'esempio seguente viene creato un nuovo volume con il supporto di grandi volumi e dimensioni file abilitato.

```
volume create -vserver vs1 -volume big_vol1 -aggregate aggr1 -is-large  
-size-enabled true
```

### Modificare un volume esistente

#### Fase

1. Modificare un volume per attivare il supporto di file e volumi di grandi dimensioni:

```
volume modify -vserver _svm_name_ -volume _volume_name_ -is-large-size  
-enabled true
```

### Esempio

Nell'esempio seguente viene modificato un volume esistente per supportare volumi e dimensioni dei file di grandi dimensioni.

```
volume modify -vserver vs2 -volume data_vol -is-large-size-enabled true
```

### Informazioni correlate

- ["Creare un volume"](#)
- ["Riferimento comando"](#)

### Volumi SAN

#### A proposito dei volumi SAN

ONTAP offre tre opzioni di base per il provisioning dei volumi: Thick provisioning, thin provisioning e provisioning semi-thick. Ciascuna opzione utilizza diversi modi per gestire lo spazio del volume e i requisiti di spazio per le tecnologie di condivisione a blocchi di ONTAP. La comprensione del funzionamento delle opzioni consente di scegliere l'opzione migliore per il proprio ambiente.



Si sconsiglia di inserire LUN SAN e condivisioni NAS nello stesso volume FlexVol. È necessario eseguire il provisioning di volumi FlexVol separati specifici per LE LUN SAN e fornire volumi FlexVol separati in modo specifico alle condivisioni NAS. Ciò semplifica le implementazioni di gestione e replica e consente di utilizzare i volumi FlexVol supportati in Active IQ Unified Manager (in precedenza OnCommand Unified Manager).

## Thin provisioning per i volumi

Quando viene creato un volume con thin provisioning, ONTAP non riserva spazio extra quando viene creato il volume. Quando i dati vengono scritti nel volume, il volume richiede all'aggregato lo storage necessario per consentire l'operazione di scrittura. L'utilizzo di volumi con thin provisioning consente di eseguire l'overcommit dell'aggregato, il che introduce la possibilità che il volume non sia in grado di proteggere lo spazio necessario quando l'aggregato esaurisce lo spazio libero.

È possibile creare un volume FlexVol con thin provisioning impostandone l'impostazione `-space-guarantee` opzione a. `none`.

## Thick provisioning per i volumi

Quando viene creato un volume con thick provisioning, ONTAP mette a disposizione una quantità di storage sufficiente dall'aggregato per garantire che qualsiasi blocco del volume possa essere scritto in qualsiasi momento. Quando si configura un volume per l'utilizzo del thick provisioning, è possibile utilizzare una qualsiasi delle funzionalità di efficienza dello storage ONTAP, come compressione e deduplica, per compensare i requisiti di storage anticipati più ampi.

È possibile creare un volume FlexVol con thick provisioning impostandone l'impostazione `-space-slo` (obiettivo del livello di servizio) opzione a. `thick`.

## Provisioning semi-spessi per i volumi

Quando viene creato un volume che utilizza il provisioning semi-thick, ONTAP mette da parte lo spazio di storage dell'aggregato per tenere conto delle dimensioni del volume. Se il volume sta esaurendo lo spazio libero perché i blocchi vengono utilizzati dalle tecnologie di condivisione dei blocchi, ONTAP si impegna a eliminare gli oggetti dati di protezione (copie Snapshot, file FlexClone e LUN) per liberare spazio. Fino a quando ONTAP può eliminare gli oggetti dati di protezione abbastanza velocemente da tenere il passo con lo spazio richiesto per le sovrascritture, le operazioni di scrittura continuano a avere successo. Si tratta di una garanzia di scrittura "Best effort".



Non è possibile utilizzare tecnologie per l'efficienza dello storage come deduplica, compressione e compattazione su un volume che utilizza il provisioning semi-spesso.

È possibile creare un volume FlexVol con provisioning semi-thick impostandone il valore `-space-slo` (obiettivo del livello di servizio) opzione a. `semi-thick`.

## Da utilizzare con file e LUN con spazio riservato

Un file o LUN con spazio riservato è un file per il quale lo storage viene allocato al momento della creazione. Storicamente, NetApp ha utilizzato il termine "LUN con thin provisioning" per indicare un LUN per il quale la prenotazione dello spazio è disattivata (un LUN non riservato allo spazio).



I file non riservati allo spazio non sono generalmente denominati "file con thin provisioning".

La seguente tabella riassume le principali differenze di utilizzo delle tre opzioni di provisioning dei volumi con file e LUN con spazio riservato:



Provisioning di volumi	Prenotazione di spazio LUN/file	Sovrascrive	Dati di protezione <sup>2</sup>	Efficienza dello storage <sup>3</sup>
Spesso	Supportato	Garantito <sup>1</sup>	Garantito	Supportato
Sottile	Nessun effetto	Nessuno	Garantito	Supportato
Semi-spessa	Supportato	Best effort <sup>1</sup>	Il massimo sforzo	Non supportato

## Note

1. La capacità di garantire le sovrascritture o fornire una garanzia di sovrascrittura con il massimo sforzo richiede che la riserva di spazio sia attivata sul LUN o sul file.
2. I dati di protezione includono copie Snapshot, file FlexClone e LUN contrassegnati per l'eliminazione automatica (cloni di backup).
3. L'efficienza dello storage include deduplica, compressione, qualsiasi file FlexClone e LUN non contrassegnati per l'eliminazione automatica (cloni attivi) e file secondari FlexClone (utilizzati per l'offload delle copie).

## Supporto per LUN con thin provisioning SCSI

ONTAP supporta LUN con thin provisioning SCSI T10 e LUN con thin provisioning NetApp. Il thin provisioning SCSI T10 consente alle applicazioni host di supportare funzionalità SCSI, tra cui funzionalità di recupero dello spazio del LUN e di monitoraggio dello spazio del LUN per gli ambienti a blocchi. Il thin provisioning SCSI T10 deve essere supportato dal software host SCSI.

Si utilizza ONTAP `space-allocation` Impostazione per abilitare/disabilitare il supporto per il thin provisioning T10 su un LUN. Si utilizza ONTAP `space-allocation enable` Impostazione per abilitare il thin provisioning SCSI T10 su un LUN.

Il `[-space-allocation {enabled|disabled}]` Nel Manuale di riferimento dei comandi ONTAP sono disponibili ulteriori informazioni per attivare/disattivare il supporto per il thin provisioning T10 e per abilitare il thin provisioning SCSI T10 su un LUN.

## "Comandi di ONTAP 9"

### Configurare le opzioni di provisioning dei volumi

È possibile configurare un volume per il thin provisioning, il thick provisioning o il provisioning semi-thick.

### A proposito di questa attività

Impostazione di `-space-slo` opzione a. `thick` garantisce quanto segue:

- L'intero volume viene preallocato nell'aggregato. Non è possibile utilizzare `volume create` oppure `volume modify` per configurare i volumi `-space-guarantee` opzione.
- il 100% dello spazio richiesto per le sovrascritture è riservato. Non è possibile utilizzare `volume modify` per configurare i volumi `-fractional-reserve` opzione

Impostazione di `-space-slo` opzione a. `semi-thick` garantisce quanto segue:

- L'intero volume viene preallocato nell'aggregato. Non è possibile utilizzare `volume create` oppure `volume modify` per configurare i volumi `-space-guarantee` opzione.
- Nessuno spazio riservato per le sovrascritture. È possibile utilizzare `volume modify` per configurare i volumi `-fractional-reserve` opzione.
- L'eliminazione automatica delle copie Snapshot è attivata.

## Fase

### 1. Configurare le opzioni di provisioning dei volumi:

```
volume create -vserver vserver_name -volume volume_name -aggregate
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

Il `-space-guarantee` l'opzione predefinita è `none` Per sistemi AFF e volumi DP non AFF. In caso contrario, l'impostazione predefinita è `volume`. Per i volumi FlexVol esistenti, utilizzare `volume modify` per configurare le opzioni di provisioning.

Il seguente comando configura vol1 su SVM vs1 per il thin provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee
none
```

Il seguente comando configura vol1 su SVM vs1 per il thick provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

Il seguente comando configura vol1 su SVM vs1 per il provisioning semi-spesso:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-
thick
```

## Determinare l'utilizzo dello spazio in un volume o aggregato

L'abilitazione di una funzione in ONTAP potrebbe occupare più spazio del previsto. ONTAP ti aiuta a determinare il consumo di spazio fornendo tre prospettive da cui visualizzare lo spazio: Il volume, l'impatto di un volume all'interno dell'aggregato e l'aggregato.

Un volume può esaurire lo spazio a causa del consumo di spazio o dello spazio insufficiente all'interno del volume, dell'aggregato o di una combinazione di entrambi. Visualizzando una suddivisione orientata alle funzioni dell'utilizzo dello spazio da diverse prospettive, è possibile valutare quali funzioni si desidera regolare o disattivare o se è necessario eseguire altre azioni (come l'aumento delle dimensioni dell'aggregato o del volume).

È possibile visualizzare i dettagli sull'utilizzo dello spazio da una delle seguenti prospettive:

- L'utilizzo dello spazio del volume

Questa prospettiva fornisce dettagli sull'utilizzo dello spazio all'interno del volume, incluso l'utilizzo da parte delle copie Snapshot.

Utilizzare `volume show-space` per visualizzare l'utilizzo dello spazio di un volume.

A partire da ONTAP 9.14.1, su volumi con [Efficienza dello storage sensibile alla temperatura \(TSSE\)](#) attivata, la quantità di spazio utilizzata sul volume riportato da `volume show-space -physical used` Il comando include i risparmi di spazio ottenuti come risultato di TSSE.

- L'impatto del volume all'interno dell'aggregato

Questa prospettiva fornisce dettagli sulla quantità di spazio utilizzata da ciascun volume nell'aggregato contenente, inclusi i metadati del volume.

Utilizzare `volume show-footprint` per visualizzare l'impatto di un volume con l'aggregato.

- L'utilizzo dello spazio dell'aggregato

Questa prospettiva include i totali delle impronte dei volumi di tutti i volumi contenuti nell'aggregato, lo spazio riservato per le copie Snapshot aggregate e altri metadati aggregati.

WAFL riserva il 10% dello spazio totale su disco per le performance e i metadati a livello aggregato. Lo spazio utilizzato per mantenere i volumi nell'aggregato esce dalla WAFL Reserve e non può essere modificato.

A partire dal ONTAP 9.12.1, la riserva WAFL per gli aggregati superiori a 30TB si riduce dal 10% al 5% per le piattaforme AFF e FAS500f. A partire dal sistema ONTAP 9.14.1, questa stessa riduzione si applica agli aggregati su tutte le piattaforme FAS, producendo il 5% di spazio utilizzabile in più negli aggregati.

Utilizzare `storage aggregate show-space` per visualizzare l'utilizzo dello spazio dell'aggregato.

Alcune funzionalità, come il backup su nastro e la deduplica, utilizzano lo spazio per i metadati sia dal volume che direttamente dall'aggregato. Queste funzionalità mostrano un utilizzo diverso dello spazio tra le prospettive di volume e volume footprint.

### Informazioni correlate

- ["Articolo della Knowledge base: Utilizzo dello spazio"](#)
- ["Liberate fino al 5% della vostra capacità di storage eseguendo l'upgrade a ONTAP 9.12.1"](#)

### Elimina automaticamente le copie Snapshot

È possibile definire e attivare un criterio per l'eliminazione automatica delle copie Snapshot e dei LUN FlexClone. L'eliminazione automatica delle copie Snapshot e dei LUN FlexClone consente di gestire l'utilizzo dello spazio.

### A proposito di questa attività

È possibile eliminare automaticamente le copie Snapshot dai volumi di lettura/scrittura e dalle LUN FlexClone dai volumi padre di lettura/scrittura. Non è possibile impostare l'eliminazione automatica delle copie Snapshot dai volumi di sola lettura, ad esempio i volumi di destinazione di SnapMirror.

### Fase

1. Definire e attivare un criterio per l'eliminazione automatica delle copie Snapshot utilizzando `volume`

snapshot autodelete modify comando.

Vedere volume snapshot autodelete modify pagina man per informazioni sui parametri che è possibile utilizzare con questo comando per definire una policy che soddisfi le proprie esigenze.

Il seguente comando consente di eliminare automaticamente le copie Snapshot e imposta il trigger su snap\_reserve Per il volume vol3, che fa parte della SVM (Storage Virtual Machine) vs0.example.com:

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger snap_reserve
```

Il seguente comando consente l'eliminazione automatica delle copie Snapshot e delle LUN FlexClone contrassegnate per l'autodeletion per il volume vol3, che fa parte della macchina virtuale di storage vs0.example.com (SVM):

```
cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
-volume vol3 -enabled true -trigger volume -commitment try -delete-order
oldest_first -destroy-list lun_clone,file_clone
```



Le copie Snapshot a livello di aggregato funzionano in modo diverso rispetto alle copie Snapshot a livello di volume e vengono gestite automaticamente da ONTAP. L'opzione di eliminazione delle copie Snapshot aggregate è sempre attivata e consente di gestire l'utilizzo dello spazio.

Se il parametro trigger è impostato su snap\_reserve Per un aggregato, le copie Snapshot vengono mantenute fino a quando lo spazio riservato non supera la capacità di soglia. Pertanto, anche se il parametro trigger non è impostato su snap\_reserve, Lo spazio utilizzato dalla copia Snapshot nel comando verrà elencato come 0 Perché queste copie Snapshot vengono eliminate automaticamente. Inoltre, lo spazio utilizzato dalle copie Snapshot in un aggregato è considerato libero ed è incluso nel parametro Available space del comando.

#### Configurare i volumi in modo che forniscano automaticamente più spazio quando sono pieni

Quando i volumi FlexVol si esauriranno, ONTAP può utilizzare diversi metodi per tentare di fornire automaticamente più spazio libero per il volume. È possibile scegliere i metodi che ONTAP può utilizzare e in quale ordine, a seconda dei requisiti imposti dall'applicazione e dall'architettura di storage.

#### A proposito di questa attività

ONTAP può fornire automaticamente più spazio libero per un volume completo utilizzando uno o entrambi i metodi seguenti:

- Aumentare le dimensioni del volume (noto come *crescita automatica*).

Questo metodo è utile se l'aggregato contenente il volume dispone di spazio sufficiente per supportare un volume più grande. È possibile configurare ONTAP in modo da impostare una dimensione massima per il volume. L'aumento viene attivato automaticamente in base alla quantità di dati scritti nel volume in

relazione alla quantità corrente di spazio utilizzato e alle soglie impostate.

La crescita automatica non viene attivata per supportare la creazione di copie Snapshot. Se si tenta di creare una copia Snapshot e lo spazio è insufficiente, la creazione della copia Snapshot non riesce, anche con l'opzione di crescita automatica attivata.

- Eliminare copie Snapshot, file FlexClone o LUN FlexClone.

Ad esempio, è possibile configurare ONTAP in modo che elimini automaticamente le copie Snapshot non collegate alle copie Snapshot in volumi o LUN clonati oppure definire quali copie Snapshot si desidera che ONTAP elimini per prima: Le copie Snapshot più vecchie o più recenti. È inoltre possibile determinare quando ONTAP deve iniziare a eliminare le copie Snapshot, ad esempio quando il volume è quasi pieno o quando la riserva Snapshot del volume è quasi piena.

Se si abilitano entrambi questi metodi, è possibile specificare il metodo che ONTAP tenta per primo quando un volume è quasi pieno. Se il primo metodo non fornisce spazio aggiuntivo sufficiente al volume, ONTAP tenta di utilizzare l'altro metodo.

Per impostazione predefinita, ONTAP tenta di aumentare prima le dimensioni del volume. Nella maggior parte dei casi, la configurazione predefinita è preferibile, perché quando una copia Snapshot viene eliminata, non può essere ripristinata. Tuttavia, se si desidera evitare di aumentare le dimensioni di un volume quando possibile, è possibile configurare ONTAP in modo che elimini le copie Snapshot prima di aumentare le dimensioni del volume.

## Fasi

1. Se si desidera che ONTAP cerchi di aumentare le dimensioni del volume quando si esaurisce, attivare la funzione di crescita automatica del volume utilizzando `volume autosize` comando con `grow` modalità.

Tenere presente che quando il volume cresce, consuma più spazio libero dall'aggregato associato. Se si dipende dalla capacità del volume di crescere ogni volta che è necessario, è necessario monitorare lo spazio libero nell'aggregato associato e aggiungerne di più quando necessario.

2. Se si desidera che ONTAP elimini copie Snapshot, file FlexClone o LUN FlexClone quando il volume si esaurisce, attivare l'eliminazione automatica per questi tipi di oggetti.
3. Se sono state attivate sia la funzionalità di crescita automatica del volume che una o più funzionalità di eliminazione automatica, selezionare il primo metodo che ONTAP deve utilizzare per fornire spazio libero a un volume utilizzando `volume modify` con il `-space-mgmt-try-first` opzione.

Per specificare prima di tutto l'aumento delle dimensioni del volume (impostazione predefinita), utilizzare `volume_grow`. Per specificare prima di tutto l'eliminazione delle copie Snapshot, utilizzare `snap_delete`.

## Configurare i volumi per aumentare e ridurre automaticamente le dimensioni

È possibile configurare i volumi FlexVol in modo che aumentino e diminuiscano automaticamente in base allo spazio attualmente richiesto. La crescita automatica aiuta a evitare che un volume esaurisca lo spazio, se l'aggregato è in grado di fornire più spazio. La riduzione automatica impedisce a un volume di essere più grande del necessario, liberando spazio nell'aggregato per l'utilizzo da parte di altri volumi.

## Di cosa hai bisogno

Il volume FlexVol deve essere online.

## A proposito di questa attività

La riduzione automatica può essere utilizzata solo in combinazione con la crescita automatica per soddisfare le esigenze di spazio in continua evoluzione e non è disponibile da sola. Quando la funzione di riduzione automatica è attivata, ONTAP gestisce automaticamente il comportamento di riduzione di un volume per evitare un loop infinito di operazioni di crescita automatica e di riduzione automatica.

Man mano che un volume cresce, il numero massimo di file che può contenere potrebbe aumentare automaticamente. Quando un volume viene ridotto, il numero massimo di file che può contenere rimane invariato e un volume non può essere ridotto automaticamente al di sotto delle dimensioni corrispondenti al numero massimo di file corrente. Per questo motivo, potrebbe non essere possibile ridurre automaticamente un volume fino alle dimensioni originali.

Per impostazione predefinita, la dimensione massima a cui un volume può crescere è pari al 120% della dimensione a cui è attivata la funzione di crescita automatica. Se è necessario garantire che il volume possa crescere fino a raggiungere un valore superiore, è necessario impostare di conseguenza la dimensione massima del volume.

## Fase

1. Configurare il volume in modo che aumenti e riduca automaticamente le sue dimensioni:

```
volume autosize -vserver vs1 vol_name -mode grow_shrink
```

Il seguente comando consente di modificare automaticamente le dimensioni di un volume chiamato test2. Il volume viene configurato per iniziare la riduzione quando è pieno al 60%. I valori predefiniti vengono utilizzati per il momento in cui inizierà a crescere e per le dimensioni massime.

```
cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent 60
vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

Volume modify successful on volume: test2
```

## Requisiti per l'abilitazione della riduzione automatica e dell'eliminazione automatica delle copie Snapshot

La funzionalità di riduzione automatica può essere utilizzata con l'eliminazione automatica della copia Snapshot se vengono soddisfatti determinati requisiti di configurazione.

Se si desidera attivare la funzionalità di riduzione automatica e l'eliminazione automatica della copia Snapshot, la configurazione deve soddisfare i seguenti requisiti:

- ONTAP deve essere configurato per tentare di aumentare le dimensioni del volume prima di tentare di eliminare le copie Snapshot (il `-space-mgmt-try-first` l'opzione deve essere impostata su `volume_grow`).
- Il trigger per l'eliminazione automatica della copia Snapshot deve essere `volume_fullness` (volume pieno) `trigger` il parametro deve essere impostato su `volume`).

## Come la funzionalità di riduzione automatica interagisce con l'eliminazione delle copie Snapshot

Poiché la funzionalità di riduzione automatica riduce le dimensioni di un volume FlexVol,

può influire anche sull'eliminazione automatica delle copie Snapshot del volume.

La funzionalità di riduzione automatica interagisce con l'eliminazione automatica della copia Snapshot del volume nei seguenti modi:

- Se entrambi i `grow_shrink` La modalità di dimensionamento automatico e l'eliminazione automatica della copia Snapshot sono attivate, quando le dimensioni di un volume si restringono, possono attivare l'eliminazione automatica della copia Snapshot.

Questo perché la riserva Snapshot si basa su una percentuale delle dimensioni del volume (5% per impostazione predefinita) e tale percentuale si basa ora su un volume più piccolo. Ciò può causare la fuoriuscita delle copie Snapshot dalla riserva e l'eliminazione automatica.

- Se il `grow_shrink` La modalità di dimensionamento automatico è attivata e si elimina manualmente una copia Snapshot, che potrebbe attivare un ritiro automatico del volume.

#### **Risolvere gli avvisi di riempimento e di overallocation dei volumi FlexVol**

ONTAP emette messaggi EMS quando i volumi FlexVol stanno esaurendo lo spazio, in modo da poter intraprendere azioni correttive fornendo più spazio per l'intero volume. Conoscere i tipi di avvisi e come risolverli aiuta a garantire la disponibilità dei dati.

Quando un volume viene descritto come *full*, significa che la percentuale dello spazio nel volume disponibile per l'utilizzo da parte del file system attivo (dati utente) è scesa al di sotto di una soglia (configurabile). Quando un volume viene *overallocato*, lo spazio utilizzato da ONTAP per i metadati e per supportare l'accesso ai dati di base è esaurito. A volte lo spazio normalmente riservato ad altri scopi può essere utilizzato per mantenere il volume funzionante, ma la riserva di spazio o la disponibilità dei dati possono essere a rischio.

L'allocazione in eccesso può essere logica o fisica. *Overallocation logica* significa che lo spazio riservato per onorare gli impegni futuri in termini di spazio, come la prenotazione dello spazio, è stato utilizzato per un altro scopo. *Overallocation fisica* significa che il volume sta esaurendo i blocchi fisici da utilizzare. I volumi in questo stato sono a rischio di rifiutare le scritture, di andare offline o di causare un'interruzione del controller.

Un volume può essere pieno oltre il 100% a causa dello spazio utilizzato o riservato dai metadati. Tuttavia, un volume che è pieno oltre il 100% potrebbe essere o meno overallocato. Se le condivisioni a livello di qtree e di volume sono presenti nello stesso pool di FlexVol o SCVMM, le qtree vengono visualizzate come directory nella condivisione di FlexVol. Pertanto, è necessario fare attenzione a non eliminarle accidentalmente.

La seguente tabella descrive gli avvisi di riempimento e overallocation del volume, le azioni che è possibile intraprendere per risolvere il problema e i rischi di non intraprendere azioni:

Tipo di avviso	Livello EMS	Configurabile?	Definizione	Modi per risolvere il caso	Rischio se non viene intrapresa alcuna azione
Quasi pieno	Debug	Y	Il file system ha superato la soglia impostata per questo avviso (il valore predefinito è 95%). La percentuale è <code>Used Totale</code> meno la dimensione della riserva di Snapshot.	<ul style="list-style-type: none"> <li>• Aumento delle dimensioni del volume</li> <li>• Riduzione dei dati degli utenti</li> </ul>	Nessun rischio di operazioni di scrittura o disponibilità dei dati.
Completo	Debug	Y	Il file system ha superato la soglia impostata per questo avviso (il valore predefinito è 98%). La percentuale è <code>Used Totale</code> meno la dimensione della riserva di Snapshot.	<ul style="list-style-type: none"> <li>• Aumento delle dimensioni del volume</li> <li>• Riduzione dei dati degli utenti</li> </ul>	Non esiste ancora alcun rischio per operazioni di scrittura o disponibilità dei dati, ma il volume si sta avvicinando alla fase in cui le operazioni di scrittura potrebbero essere a rischio.
Allocato logicamente in eccesso	Errore SVC	N	Oltre al file system pieno, lo spazio nel volume utilizzato per i metadati è stato esaurito.	<ul style="list-style-type: none"> <li>• Aumento delle dimensioni del volume</li> <li>• Eliminazione delle copie Snapshot</li> <li>• Riduzione dei dati degli utenti</li> <li>• Disattivazione e della riserva di spazio per file o LUN</li> </ul>	Le operazioni di scrittura su file non riservati potrebbero non riuscire.



Tipo di avviso	Livello EMS	Configurabile?	Definizione	Modi per risolvere il caso	Rischio se non viene intrapresa alcuna azione
Fisicamente allocato in eccesso	Errore del nodo	N	Il volume sta esaurendo i blocchi fisici su cui può scrivere.	<ul style="list-style-type: none"> <li>• Aumento delle dimensioni del volume</li> <li>• Eliminazione delle copie Snapshot</li> <li>• Riduzione dei dati degli utenti</li> </ul>	Le operazioni di scrittura sono a rischio, così come la disponibilità dei dati; il volume potrebbe andare offline.

Ogni volta che viene superata una soglia per un volume, sia che la percentuale di pienezza sia in aumento o in diminuzione, viene generato un messaggio EMS. Quando il livello di riempimento del volume scende al di sotto di una soglia, viene visualizzato un `volume ok`. Viene generato il messaggio EMS.

#### Gestire gli avvisi di fullness e overallocation aggregati

ONTAP emette messaggi EMS quando gli aggregati stanno esaurendo lo spazio in modo da poter intraprendere azioni correttive fornendo più spazio per l'intero aggregato. Conoscere i tipi di avvisi e come risolverli aiuta a garantire la disponibilità dei dati.

Quando un aggregato viene descritto come *full*, significa che la percentuale dello spazio nell'aggregato disponibile per l'utilizzo da parte dei volumi è scesa al di sotto di una soglia predefinita. Quando un aggregato viene *overallocato*, lo spazio utilizzato da ONTAP per i metadati e per supportare l'accesso ai dati di base è esaurito. A volte lo spazio normalmente riservato ad altri scopi può essere utilizzato per mantenere l'aggregato funzionante, ma le garanzie di volume per i volumi associati all'aggregato o alla disponibilità dei dati possono essere a rischio.

L'allocazione in eccesso può essere logica o fisica. *Overallocation logica* significa che lo spazio riservato per onorare gli impegni futuri in termini di spazio, come le garanzie di volume, è stato utilizzato per un altro scopo. *Overallocation fisica* significa che l'aggregato sta esaurendo i blocchi fisici da utilizzare. Gli aggregati in questo stato sono a rischio di rifiutare le scritture, di andare offline o di causare potenzialmente un'interruzione del controller.

La seguente tabella descrive gli avvisi di fullness e overallocation aggregati, le azioni che è possibile intraprendere per risolvere il problema e i rischi di non intraprendere azioni.

Tip o di avvi so	Liv ello EM S	Con figu rabi le?	Definizione	Modi per risolvere il caso	Rischio se non viene intrapresa alcuna azione
Quasi pieno	Debu g	N	La quantità di spazio allocato per i volumi, incluse le relative garanzie, ha superato la soglia impostata per questo avviso (95%). La percentuale è Used Totale meno la dimensione della riserva di Snapshot.	<ul style="list-style-type: none"> <li>• Aggiunta di storage all'aggregato</li> <li>• Riduzione o eliminazione dei volumi</li> <li>• Spostamento dei volumi in un altro aggregato con più spazio</li> <li>• Rimozione delle garanzie di volume (impostandole su none)</li> </ul>	Nessun rischio di operazioni di scrittura o disponibilità dei dati.
Completo	Debu g	N	Il file system ha superato la soglia impostata per questo avviso (98%). La percentuale è Used Totale meno la dimensione della riserva di Snapshot.	<ul style="list-style-type: none"> <li>• Aggiunta di storage all'aggregato</li> <li>• Riduzione o eliminazione dei volumi</li> <li>• Spostamento dei volumi in un altro aggregato con più spazio</li> <li>• Rimozione delle garanzie di volume (impostandole su none)</li> </ul>	Le garanzie di volume per i volumi nell'aggregato potrebbero essere a rischio, così come le operazioni di scrittura su tali volumi.
Allo cat o logi ca me nte in ecc ess o	Err ore SV C	N	Oltre allo spazio riservato ai volumi pieno, lo spazio nell'aggregato utilizzato per i metadati è stato esaurito.	<ul style="list-style-type: none"> <li>• Aggiunta di storage all'aggregato</li> <li>• Riduzione o eliminazione dei volumi</li> <li>• Spostamento dei volumi in un altro aggregato con più spazio</li> <li>• Rimozione delle garanzie di volume (impostandole su none)</li> </ul>	Le garanzie di volume per i volumi nell'aggregato sono a rischio, così come le operazioni di scrittura su tali volumi.

Tip o di avvi so	Liv ello EM S	Con figu rabi le?	Definizione	Modi per risolvere il caso	Rischio se non viene intrapresa alcuna azione
Fisi ca me nte allo cat o in ecc ess o	Err ore del nod o	N	L'aggregato sta esaurendo i blocchi fisici sui quali può scrivere.	<ul style="list-style-type: none"> <li>• Aggiunta di storage all'aggregato</li> <li>• Riduzione o eliminazione dei volumi</li> <li>• Spostamento dei volumi in un altro aggregato con più spazio</li> </ul>	Le operazioni di scrittura nei volumi dell'aggregato sono a rischio, così come la disponibilità dei dati; l'aggregato potrebbe andare offline. In casi estremi, il nodo potrebbe subire un'interruzione.

Ogni volta che viene superata una soglia per un aggregato, sia che la percentuale di pienezza sia in aumento o in diminuzione, viene generato un messaggio EMS. Quando il livello di pienezza dell'aggregato scende al di sotto di una soglia, un aggregato `ok` Viene generato il messaggio EMS.

#### Considerazioni per l'impostazione della riserva frazionale

La riserva frazionale, detta anche *riserva di sovrascrittura LUN*, consente di disattivare la riserva di sovrascrittura per i LUN e i file con spazio riservato in un volume FlexVol. In questo modo è possibile massimizzare l'utilizzo dello storage, ma se l'ambiente viene influenzato negativamente da operazioni di scrittura non riuscite a causa della mancanza di spazio, è necessario comprendere i requisiti imposti da questa configurazione.

L'impostazione della riserva frazionale viene espressa in percentuale; gli unici valori validi sono 0 e 100 percentuale. L'impostazione della riserva frazionale è un attributo del volume.

Impostazione della riserva frazionale a 0 aumenta l'utilizzo dello storage. Tuttavia, un'applicazione che accede ai dati che risiedono nel volume potrebbe riscontrare un'interruzione dei dati se il volume non dispone di spazio libero, anche se la garanzia del volume è impostata su `volume`. Tuttavia, con una configurazione e un utilizzo corretti del volume, è possibile ridurre al minimo il rischio di errori di scrittura. ONTAP offre una garanzia di scrittura "Best effort" per i volumi con riserva frazionale impostata su 0 quando *tutti* i seguenti requisiti sono soddisfatti:

- La deduplica non è in uso
- La compressione non è in uso
- I file secondari FlexClone non sono in uso
- Tutti i file FlexClone e i LUN FlexClone sono abilitati per l'eliminazione automatica

Questa non è l'impostazione predefinita. È necessario attivare esplicitamente l'eliminazione automatica, al momento della creazione o modificando il file FlexClone o il LUN FlexClone dopo la creazione.

- L'offload delle copie di ODX e FlexClone non è in uso
- La garanzia del volume è impostata su `volume`
- La prenotazione dello spazio del file o del LUN è `enabled`

- Volume Snapshot Reserve (Riserva snapshot volume) è impostato su 0
- L'eliminazione automatica della copia Snapshot del volume è enabled con un livello di impegno di destroy, un elenco di destroy di lun\_clone, vol\_clone, cifs\_share, file\_clone, sfsr`e un trigger di `volume

Questa impostazione garantisce inoltre che i file FlexClone e le LUN FlexClone vengano cancellati quando necessario.



- Se tutti i requisiti sopra indicati vengono soddisfatti ma la velocità di modifica è elevata, in rari casi, l'eliminazione automatica della copia Snapshot potrebbe fallire, provocando l'esaurimento dello spazio del volume.
- Se tutti i requisiti sopra indicati vengono soddisfatti e le copie Snapshot non vengono utilizzate, le scritture dei volumi garantiscono di non esaurire lo spazio.

Inoltre, è possibile utilizzare la funzione di crescita automatica del volume per ridurre la probabilità che le copie Snapshot del volume debbano essere eliminate automaticamente. Se si attiva la funzione di crescita automatica, è necessario monitorare lo spazio libero nell'aggregato associato. Se l'aggregato diventa sufficientemente pieno da impedire la crescita del volume, è probabile che vengano eliminate più copie Snapshot man mano che lo spazio libero nel volume si esaurisce.

Se non si riesce a soddisfare tutti i requisiti di configurazione sopra indicati ed è necessario assicurarsi che il volume non esaurisca lo spazio, è necessario impostare la riserva frazionale del volume su 100. Ciò richiede più spazio libero in anticipo, ma garantisce che le operazioni di modifica dei dati avranno successo anche quando le tecnologie sopra elencate sono in uso.

Il valore predefinito e i valori consentiti per l'impostazione della riserva frazionale dipendono dalla garanzia del volume:

Garanzia di volume	Riserva frazionaria predefinita	Valori consentiti
Volume	100	0, 100
Nessuno	0	0, 100

## Visualizzazione dell'utilizzo di file o inode

I volumi FlexVol possono contenere un numero massimo di file. Conoscere il numero di file contenuti nei volumi consente di determinare se è necessario aumentare il numero di inode (pubblici) per i volumi per evitare che colpiscano il limite massimo di file.

### A proposito di questa attività

Gli inode pubblici possono essere liberi (non associati a un file) o utilizzati (puntano a un file). Il numero di inode liberi per un volume è il numero totale di inode per il volume meno il numero di inode utilizzati (il numero di file).

Se le condivisioni a livello di qtree e di volume sono presenti nello stesso pool di FlexVol o SCVMM, le qtree vengono visualizzate come directory nella condivisione di FlexVol. Pertanto, è necessario fare attenzione a non eliminarle accidentalmente.

## Fase

1. Per visualizzare l'utilizzo inode di un volume, immettere il seguente comando:

```
volume show -vserver <SVM_name> -volume <volume_name> -fields files
```

### Esempio

```
cluster1::*> volume show -vserver vs1 -volume vol1 -fields files
Vserver Name: vs1
Files Used (for user-visible data): 98
```

### Controllo e monitoraggio delle performance i/o dei volumi FlexVol utilizzando la QoS dello storage

È possibile controllare le prestazioni di input/output (i/o) dei volumi FlexVol assegnando i volumi ai gruppi di policy di qualità del servizio di storage. È possibile controllare le performance di i/o per garantire che i carichi di lavoro raggiungano specifici obiettivi di performance o per ridurre il carico di lavoro che ha un impatto negativo su altri carichi di lavoro.

#### A proposito di questa attività

I gruppi di policy applicano un limite massimo di throughput (ad esempio, 100 MB/s). È possibile creare un gruppo di criteri senza specificare un throughput massimo, che consente di monitorare le performance prima di controllare il carico di lavoro.

È inoltre possibile assegnare SVM, LUN e file ai gruppi di criteri.

Tenere presente i seguenti requisiti relativi all'assegnazione di un volume a un gruppo di criteri:

- Il volume deve essere contenuto dalla SVM a cui appartiene il gruppo di criteri.

Specificare la SVM quando si crea il gruppo di criteri.

- Se si assegna un volume a un gruppo di criteri, non è possibile assegnare a un gruppo di criteri i volumi contenenti SVM o i LUN o i file figlio.

Per ulteriori informazioni sull'utilizzo di Storage QoS, consultare ["System Administration Reference \(Guida all'amministrazione del sistema\)"](#).

### Fasi

1. Utilizzare `qos policy-group create` per creare un gruppo di criteri.
2. Utilizzare `volume create` o il `volume modify` con il `-qos-policy-group` parametro per assegnare un volume a un gruppo di criteri.
3. Utilizzare `qos statistics` comandi per visualizzare i dati delle performance.
4. Se necessario, utilizzare `qos policy-group modify` comando per regolare il limite massimo di throughput del gruppo di criteri.

## Eliminare un volume FlexVol

È possibile eliminare un volume FlexVol che non è più necessario o che contiene dati corrotti.

### Di cosa hai bisogno

Nessuna applicazione deve accedere ai dati nel volume che si desidera eliminare.



Se si elimina accidentalmente un volume, consultare l'articolo della Knowledge base ["Come utilizzare la coda di ripristino del volume"](#).

### Fasi

1. Se il volume è stato montato, smontarlo:

```
volume unmount -vserver vserver_name -volume volume_name
```

2. Se il volume fa parte di una relazione SnapMirror, eliminare la relazione utilizzando `snapmirror delete` comando.
3. Se il volume è online, portarlo offline:

```
volume offline -vserver vserver_name volume_name
```

4. Eliminare il volume:

```
volume delete -vserver vserver_name volume_name
```

### Risultato

Il volume viene eliminato, insieme a eventuali criteri di quota e qtree associati.

### Protezione contro l'eliminazione accidentale del volume

Il comportamento predefinito di eliminazione del volume facilita il ripristino dei volumi FlexVol cancellati accidentalmente.

R `volume delete` richiesta a fronte di un volume con tipo RW oppure DP (come illustrato nella `volume show` output del comando) fa sì che il volume venga spostato in uno stato parzialmente cancellato. Per impostazione predefinita, viene conservato in una coda di ripristino per almeno 12 ore prima di essere eliminato completamente.

Per ulteriori informazioni, consulta l'articolo della Knowledge base ["Come utilizzare la coda di ripristino del volume"](#).

### Comandi per la gestione dei volumi FlexVol

Sono disponibili comandi specifici per la gestione dei volumi FlexVol mediante l'interfaccia CLI di ONTAP.

Se si desidera...	Utilizzare questo comando...
Porta un volume online	<code>volume online</code>
Modificare le dimensioni di un volume	<code>volume size</code>
Determinare l'aggregato associato di un volume	<code>volume show</code>
Determinare l'aggregato associato per tutti i volumi su una macchina virtuale di storage (SVM)	<code>volume show -vserver -fields aggregate</code>
Determinare il formato di un volume	<code>volume show -fields block-type</code>
Montare un volume su un altro volume utilizzando una giunzione	<code>volume mount</code>
Impostare un volume nello stato con restrizioni	<code>volume restrict</code>
Rinominare un volume	<code>volume rename</code>
Portare un volume offline	<code>volume offline</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la visualizzazione delle informazioni sull'utilizzo dello spazio

Si utilizza `storage aggregate` e `volume` Comandi per vedere come viene utilizzato lo spazio negli aggregati, nei volumi e nelle relative copie Snapshot.

Per visualizzare informazioni su...	Utilizzare questo comando...
Aggregati, inclusi i dettagli sulle percentuali di spazio utilizzate e disponibili, le dimensioni della riserva Snapshot e altre informazioni sull'utilizzo dello spazio	<code>storage aggregate show storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code>
Modalità di utilizzo dei dischi e dei gruppi RAID in un aggregato e nello stato RAID	<code>storage aggregate show-status</code>
La quantità di spazio su disco che verrebbe recuperata se si elimina una copia Snapshot specifica	<code>volume snapshot compute-reclaimable</code> (avanzato)
La quantità di spazio utilizzata da un volume	<code>volume show -fields size,used,available,percent-used</code> <code>volume show-space</code>

Per visualizzare informazioni su...	Utilizzare questo comando...
La quantità di spazio utilizzata da un volume nell'aggregato contenente	<code>volume show-footprint</code>

## Spostamento e copia dei volumi

### Spostare una panoramica del volume FlexVol

È possibile spostare o copiare volumi per l'utilizzo della capacità, migliorare le performance e soddisfare i service level agreement.

Conoscere il funzionamento dello spostamento di un volume FlexVol consente di determinare se lo spostamento del volume soddisfa gli accordi sui livelli di servizio e di capire dove si trova lo spostamento di un volume nel processo di spostamento del volume.

I volumi FlexVol vengono spostati da un aggregato o nodo a un altro all'interno della stessa macchina virtuale di storage (SVM). Lo spostamento di un volume non interrompe l'accesso del client durante lo spostamento.

Lo spostamento di un volume avviene in più fasi:

- Viene creato un nuovo volume sull'aggregato di destinazione.
- I dati del volume originale vengono copiati nel nuovo volume.

Durante questo periodo di tempo, il volume originale è intatto e disponibile per l'accesso dei client.

- Al termine del processo di spostamento, l'accesso client viene temporaneamente bloccato.

Durante questo periodo, il sistema esegue una replica finale dal volume di origine al volume di destinazione, scambia le identità dei volumi di origine e di destinazione e modifica il volume di destinazione nel volume di origine.

- Una volta completato lo spostamento, il sistema instrada il traffico client al nuovo volume di origine e ripristina l'accesso al client.

Lo spostamento non comporta interruzioni per l'accesso al client, in quanto il tempo in cui l'accesso al client viene bloccato termina prima che i client notino un'interruzione e un timeout. Per impostazione predefinita, l'accesso al client viene bloccato per 35 secondi. Se l'operazione di spostamento del volume non riesce a terminare nel momento in cui l'accesso viene negato, il sistema interrompe questa fase finale dell'operazione di spostamento del volume e consente l'accesso del client. Per impostazione predefinita, il sistema tenta la fase finale tre volte. Dopo il terzo tentativo, il sistema attende un'ora prima di tentare nuovamente la sequenza di fase finale. Il sistema esegue la fase finale dell'operazione di spostamento del volume fino al completamento dello spostamento del volume.

### Considerazioni e consigli per lo spostamento dei volumi

Lo spostamento di un volume contiene molte considerazioni e consigli che sono influenzati dal volume che si sta spostando o dalla configurazione del sistema, ad esempio una configurazione MetroCluster. È necessario comprendere le considerazioni e i consigli relativi allo spostamento dei volumi.



## Considerazioni e raccomandazioni generali

- Se si sta aggiornando la famiglia di release per un cluster, non spostare un volume fino a quando non si aggiornano tutti i nodi del cluster.

Questo suggerimento impedisce di tentare inavvertitamente di spostare un volume da una famiglia di release più recente a una famiglia di release più vecchia.

- Il volume di origine deve essere coerente.
- Se sono stati assegnati uno o più aggregati alla SVM (Storage Virtual Machine) associata, l'aggregato di destinazione deve essere uno degli aggregati assegnati.
- Non è possibile spostare un volume da o verso un aggregato CFO preso in consegna.
- Se un volume contenente LUN non è abilitato prima dello spostamento, il volume sarà abilitato NVFAIL dopo lo spostamento.
- È possibile spostare un volume da un aggregato di Flash Pool a un altro aggregato di Flash Pool.
  - Vengono spostate anche le policy di caching di quel volume.
  - Lo spostamento potrebbe influire sulle prestazioni del volume.
- È possibile spostare i volumi tra un aggregato di Flash Pool e un aggregato non di Flash Pool.
  - Se si sposta un volume da un aggregato di Flash Pool a un aggregato non di Flash Pool, ONTAP visualizza un messaggio che avvisa che lo spostamento potrebbe influire sulle prestazioni del volume e chiede se si desidera continuare.
  - Se si sposta un volume da un aggregato non Flash Pool a un aggregato Flash Pool, ONTAP assegna il `auto` policy di caching.
- I volumi dispongono delle protezioni dei dati a riposo dell'aggregato su cui risiedono. Se si sposta un volume da un aggregato costituito da unità NSE a un volume che non lo utilizza, il volume non dispone più della protezione NSE per i dati inattivi.

## Considerazioni e consigli sul volume FlexClone

- I volumi FlexClone non possono essere offline quando vengono spostati.
- È possibile spostare volumi FlexClone da un aggregato a un altro aggregato sullo stesso nodo o su un altro nodo nella stessa SVM senza avviare `vol clone split start` comando.

Avviando un'operazione di spostamento del volume su un volume FlexClone, il volume clone viene suddiviso durante il processo di spostamento in un aggregato diverso. Una volta completato lo spostamento del volume sul volume clone, il volume spostato non viene più visualizzato come clone, ma come volume indipendente senza alcuna relazione di clone con il volume padre precedente.

- Le copie Snapshot del volume FlexClone non vengono perse dopo lo spostamento di un clone.
- È possibile spostare volumi padre FlexClone da un aggregato a un altro.

Quando si sposta un volume padre FlexClone, viene lasciato un volume temporaneo che funge da volume padre per tutti i volumi FlexClone. Non sono consentite operazioni sul volume temporaneo, ad eccezione di portarlo offline o eliminarlo. Una volta che tutti i volumi FlexClone sono stati divisi o distrutti, il volume temporaneo viene ripulito automaticamente.

- Dopo aver spostato un volume figlio FlexClone, il volume non è più un volume FlexClone.
- Le operazioni di spostamento di FlexClone si escludono a vicenda dalle operazioni di copia o divisione di FlexClone.

- Se è in corso un'operazione di suddivisione dei cloni, lo spostamento di un volume potrebbe non riuscire.

Non spostare un volume fino al completamento delle operazioni di suddivisione dei cloni.

### **Considerazioni sulla configurazione di MetroCluster**

- Durante lo spostamento di un volume in una configurazione MetroCluster, quando viene creato un volume temporaneo sull'aggregato di destinazione nel cluster di origine, viene creato un record del volume temporaneo corrispondente al volume nel mirror, ma non assimilato, anche l'aggregato nel cluster esistente.
- Se si verifica uno switchover MetroCluster prima del cutover, il volume di destinazione ha un record ed è un volume temporaneo (un volume di tipo TMP).

Lo spostamento dei job viene riavviato nel cluster sopravvissuto (disaster recovery), segnala un errore e ripulisce tutti gli elementi correlati allo spostamento, incluso il volume temporaneo. In qualsiasi caso in cui la pulizia non possa essere eseguita correttamente, viene generato un EMS che avvisa l'amministratore di sistema di eseguire la pulizia necessaria.

- Se si verifica uno switchover MetroCluster dopo l'avvio della fase di cutover, ma prima del completamento del processo di spostamento (ovvero, lo spostamento ha raggiunto una fase in cui può aggiornare il cluster per puntare all'aggregato di destinazione), il processo di spostamento viene riavviato sulla cluster e viene eseguito fino al completamento.

Tutti gli elementi correlati allo spostamento vengono ripuliti, incluso il volume temporaneo (origine originale). In qualsiasi caso in cui la pulizia non possa essere eseguita correttamente, viene generato un EMS che avvisa l'amministratore di sistema di eseguire la pulizia necessaria.

- Non sono consentiti switchback MetroCluster forzati o non forzati se sono in corso operazioni di spostamento del volume per volumi appartenenti al sito di switchover.

I switchback non vengono bloccati quando sono in corso operazioni di spostamento del volume per i volumi locali nel sito sopravvissuto.

- Gli switchover MetroCluster non forzati sono bloccati, ma gli switchover MetroCluster forzati non vengono bloccati se sono in corso operazioni di spostamento del volume.

### **Requisito per lo spostamento di volumi in ambienti SAN**

Prima di spostare un volume contenente LUN o spazi dei nomi, è necessario soddisfare determinati requisiti.

- Per i volumi contenenti una o più LUN, è necessario disporre di almeno due percorsi per LUN (LIF) connessi a ciascun nodo del cluster.

In questo modo si eliminano i singoli punti di errore e si consente al sistema di sopravvivere ai guasti dei componenti.

- Per i volumi contenenti spazi dei nomi, il cluster deve eseguire ONTAP 9.6 o versione successiva.

Lo spostamento del volume non è supportato per le configurazioni NVMe che eseguono ONTAP 9.5.

## Spostare un volume

È possibile spostare un volume FlexVol in un aggregato, nodo o entrambi diversi all'interno della stessa SVM (Storage Virtual Machine) per bilanciare la capacità dello storage dopo aver determinato lo squilibrio della capacità dello storage.

### A proposito di questa attività

Per impostazione predefinita, se l'operazione di cutover non viene completata entro 30 secondi, viene eseguita una riesecuzione. È possibile regolare il comportamento predefinito utilizzando `-cutover-window` e `-cutover-action` parametri che richiedono un accesso avanzato a livello di privilegio. Per ulteriori informazioni, vedere `volume move start` pagina man.

### Fasi

1. Se si sposta un mirror di protezione dati e non si è inizializzata la relazione di mirroring, inizializzare la relazione di mirroring utilizzando `snapmirror initialize` comando.

Prima di poter spostare uno dei volumi, è necessario inizializzare le relazioni mirror di protezione dei dati.

2. Determinare un aggregato in cui è possibile spostare il volume utilizzando `volume move target-aggr show` comando.

L'aggregato selezionato deve disporre di spazio sufficiente per il volume, ovvero le dimensioni disponibili sono maggiori del volume che si sta spostando.

L'esempio seguente mostra che il volume `vs2` può essere spostato in uno qualsiasi degli aggregati elencati:

```
cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
Aggregate Name    Available Size    Storage Type
-----
aggr2             467.9GB          hdd
node12a_aggr3     10.34GB          hdd
node12a_aggr2     10.36GB          hdd
node12a_aggr1     10.36GB          hdd
node12a_aggr4     10.36GB          hdd
5 entries were displayed.
```

3. Verificare che il volume possa essere spostato nell'aggregato desiderato utilizzando `volume move start -perform-validation-only` per eseguire un controllo di convalida.
4. Spostare il volume utilizzando `volume move start` comando.

Il seguente comando sposta il volume `user_max` su `vs2` SVM nell'aggregato `node12a_aggr3`. Lo spostamento viene eseguito come processo in background.

```
cluster1::> volume move start -vserver vs2 -volume user_max
               -destination-aggregate node12a_aggr3
```

5. Determinare lo stato dell'operazione di spostamento del volume utilizzando `volume move show` comando.

L'esempio seguente mostra lo stato di uno spostamento di un volume che ha completato la fase di replica e si trova nella fase di cutover:

```
cluster1::> volume move show
Vserver   Volume      State      Move Phase  Percent-Complete  Time-To-Complete
-----
vs2       user_max    healthy    cutover     -                  -
```

Lo spostamento del volume è completo quando non viene più visualizzato in `volume move show` output del comando.

### Comandi per lo spostamento dei volumi

Sono disponibili comandi ONTAP specifici per la gestione dello spostamento del volume.

Se si desidera...	Utilizzare questo comando...
Interrompere un'operazione di spostamento del volume attivo.	<code>volume move abort</code>
Mostra lo stato di un volume che si sposta da un aggregato a un altro.	<code>volume move show</code>
Iniziare a spostare un volume da un aggregato a un altro aggregato.	<code>volume move start</code>
Gestire gli aggregati di destinazione per lo spostamento del volume.	<code>volume move target-aggr</code>
Attivare il cutover di un lavoro di spostamento.	<code>volume move trigger-cutover</code>
Modificare la quantità di tempo in cui l'accesso client viene bloccato se l'impostazione predefinita non è adeguata.	<code>volume move start</code> oppure <code>volume move modify</code> con <code>-cutover-window</code> parametro. Il <code>volume move modify</code> è un comando avanzato e il <code>-cutover-window</code> è un parametro avanzato.
Determinare cosa fa il sistema se l'operazione di spostamento del volume non può essere completata durante il periodo di blocco dell'accesso al client.	<code>volume move start</code> oppure <code>volume move modify</code> con <code>-cutover-action</code> parametro. Il <code>volume move modify</code> è un comando avanzato e il <code>-cutover-action</code> è un parametro avanzato.

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Metodi per la copia di un volume

La copia di un volume crea una copia standalone di un volume che è possibile utilizzare per test e altri scopi. Il metodo utilizzato per copiare un volume dipende dal caso d'utilizzo.

Il metodo utilizzato per la copia di un volume dipende dal fatto che si stia copiando un volume nello stesso aggregato o in un aggregato diverso e che si desideri conservare le copie Snapshot del volume originale. La tabella seguente elenca le caratteristiche della copia e i metodi utilizzati per crearla.

Se si desidera copiare un volume...	Il metodo utilizzato è...
Nello stesso aggregato e non si desidera copiare le copie Snapshot dal volume originale.	Creazione di un volume FlexClone del volume originale.
In un altro aggregato e non si desidera copiare le copie Snapshot dal volume originale.	Creazione di un volume FlexClone del volume originale e spostamento del volume in un altro aggregato mediante <code>volume move</code> comando.
Su un altro aggregato e conserva tutte le copie Snapshot dal volume originale.	Replica del volume originale utilizzando SnapMirror e interruzione della relazione SnapMirror per creare una copia del volume in lettura/scrittura.

## Utilizza i volumi FlexClone per creare copie efficienti dei tuoi volumi FlexVol

### Utilizza i volumi FlexClone per creare copie efficienti della panoramica dei volumi FlexVol

I volumi FlexClone sono copie point-in-time scrivibili di un volume FlexVol padre. I volumi FlexClone sono efficienti in termini di spazio perché condividono gli stessi blocchi di dati con i volumi FlexVol di origine per i dati comuni. La copia Snapshot utilizzata per creare un volume FlexClone viene condivisa anche con il volume padre.

È possibile clonare un volume FlexClone esistente per creare un altro volume FlexClone. È inoltre possibile creare un clone di un volume FlexVol contenente LUN e cloni LUN.

È inoltre possibile suddividere un volume FlexClone dal volume di origine. A partire da ONTAP 9.4, per i volumi non garantiti sui sistemi AFF, l'operazione di split per i volumi FlexClone condivide i blocchi fisici e non copia i dati. Pertanto, la suddivisione dei volumi FlexClone sui sistemi AFF è più rapida rispetto all'operazione di suddivisione di FlexClone in altri sistemi FAS in ONTAP 9.4 e versioni successive.

È possibile creare due tipi di volumi FlexClone: Volumi FlexClone in lettura/scrittura e volumi FlexClone per la protezione dei dati. Sebbene sia possibile creare un volume FlexClone in lettura/scrittura di un volume FlexVol normale, è necessario utilizzare solo un volume secondario SnapVault per creare un volume FlexClone per la protezione dei dati.

### Creare un volume FlexClone

È possibile creare un volume FlexClone per la protezione dei dati da un volume di destinazione SnapMirror o da un volume FlexVol padre che è un volume secondario SnapVault. A partire da ONTAP 9.7, è possibile creare un volume FlexClone da un

volume FlexGroup. Una volta creato un volume FlexClone, non è possibile eliminare il volume padre mentre è presente il volume FlexClone.

#### Prima di iniziare

- La licenza FlexClone deve essere installata sul cluster. Questa licenza è inclusa con ["ONTAP uno"](#).
- Il volume che si desidera clonare deve essere in linea.



Il cloning di un volume come volume FlexClone su una SVM diversa non è supportato nelle configurazioni MetroCluster.

#### Creare un volume FlexClone di un FlexVol o FlexGroup

##### Fase

1. Creare un volume FlexClone:

```
volume clone create
```



Durante la creazione di un volume FlexClone di lettura/scrittura dal volume padre di lettura/scrittura, non è necessario specificare la copia Snapshot di base. ONTAP crea una copia Snapshot se non si assegna un nome a una copia Snapshot specifica da utilizzare come copia Snapshot di base per il clone. È necessario specificare la copia Snapshot di base per la creazione di un volume FlexClone quando il volume padre è un volume di protezione dei dati.

##### Esempio

- Il seguente comando crea un volume FlexClone di lettura/scrittura vol1\_clone dal volume padre vol1:

```
volume clone create -vserver vs0 -flexclone vol1_clone -type RW -parent-volume vol1
```

- Il seguente comando crea un volume FlexClone di protezione dei dati vol\_dp\_clone dal volume d'origine dp\_vol utilizzando la copia Snapshot di base snap1:

```
volume clone create -vserver vs1 -flexclone vol_dp_clone -type DP -parent -volume dp_vol -parent-snapshot snap1
```

#### Creare un FlexClone di qualsiasi tipo di SnapLock

A partire da ONTAP 9.13.1, è possibile specificare uno dei tre tipi di SnapLock, `compliance`, `enterprise`, `non-snaplock`. Quando si crea un FlexClone di un volume RW. Per impostazione predefinita, viene creato un volume FlexClone con lo stesso tipo di SnapLock del volume padre. Tuttavia, è possibile eseguire l'override del valore predefinito utilizzando `snaplock-type` Durante la creazione del volume FlexClone.

Utilizzando il `non-snaplock` con il `snaplock-type` È possibile creare un volume FlexClone di tipo non SnapLock da un volume padre SnapLock per fornire un metodo più rapido per riportare i dati online quando necessario.

Scopri di più ["SnapLock"](#).

#### Prima di iniziare

Tenere presente le seguenti limitazioni dei volumi FlexClone quando hanno un tipo di SnapLock diverso da

quello del volume padre.

- Sono supportati solo cloni di tipo RW. I cloni di tipo DP con un tipo SnapLock diverso dal volume padre non sono supportati.
- I volumi con LUN non possono essere clonati utilizzando l'opzione snaplock-type impostata su un valore diverso da 'non snaplock' perché i volumi SnapLock non supportano LUN.
- Non è possibile clonare un volume su un aggregato mirrorato di MetroCluster con un tipo di Compliance SnapLock perché i volumi di conformità SnapLock non sono supportati sugli aggregati mirrorati di MetroCluster.
- I volumi di conformità SnapLock con blocco legale non possono essere clonati con un tipo di SnapLock diverso. La conservazione a fini giudiziari è supportata solo sui volumi di conformità SnapLock.
- Il DR SVM non supporta i volumi SnapLock. Il tentativo di creare un clone SnapLock da un volume in una SVM che fa parte di una relazione DR SVM non riesce.
- Le Best practice di FabricPool consigliano che i cloni mantengano la stessa policy di tiering del padre. Tuttavia, un clone di conformità SnapLock di un volume abilitato a FabricPool non può avere lo stesso criterio di tiering del volume padre. La policy di tiering deve essere impostata su `none`. Tentativo di creare un clone di conformità SnapLock da un'origine con una policy di tiering diversa da `none` non funziona.

## Fasi

1. Creare un volume FlexClone con un tipo di SnapLock: `volume clone create -vserver svm_name -flexclone flexclone_name -type RW [ -snaplock-type {non-snaplock|compliance|enterprise} ]`

Esempio:

```
> volume clone create -vserver vs0 -flexclone voll_clone -type RW  
-snaplock-type enterprise -parent-volume voll1
```

## Separare un volume FlexClone dal volume di origine

È possibile suddividere un volume FlexClone dal padre per rendere il clone un volume FlexVol normale.

L'operazione di suddivisione dei cloni avviene in background. I dati sono accessibili sul clone e sull'immagine principale durante la divisione. A partire da ONTAP 9.4, l'efficienza dello spazio viene preservata. Il processo di suddivisione aggiorna solo i metadati e richiede un io minimo. Non vengono copiati blocchi di dati.

### A proposito di questa attività

- Non è possibile creare nuove copie Snapshot del volume FlexClone durante l'operazione di divisione.
- Un volume FlexClone non può essere diviso dal volume principale se appartiene a una relazione di protezione dei dati o fa parte di un mirror di condivisione del carico.
- Se si porta il volume FlexClone offline mentre è in corso la suddivisione, l'operazione di suddivisione viene sospesa; quando si riporta in linea il volume FlexClone, l'operazione di suddivisione riprende.
- Dopo la divisione, sia il volume FlexVol superiore che il clone richiedono l'allocazione dello spazio completo determinata dalle rispettive garanzie del volume.
- Dopo la divisione di un volume FlexClone dall'immagine principale, non è possibile unire nuovamente i due volumi.

- A partire da ONTAP 9.4, per i volumi non garantiti sui sistemi AFF, l'operazione di split per i volumi FlexClone condivide i blocchi fisici e non copia i dati. Pertanto, la suddivisione dei volumi FlexClone sui sistemi AFF è più rapida rispetto all'operazione di suddivisione di FlexClone in altri sistemi FAS in ONTAP 9.4 e versioni successive. L'operazione di suddivisione FlexClone migliorata sui sistemi AFF offre i seguenti vantaggi:
  - L'efficienza dello storage viene preservata dopo la divisione del clone dal padre.
  - Le copie Snapshot esistenti non vengono eliminate.
  - Il funzionamento è più rapido.
  - Il volume FlexClone può essere suddiviso da qualsiasi punto della gerarchia dei cloni.

### Prima di iniziare

- Devi essere un amministratore del cluster.
- Il volume FlexClone deve essere online all'inizio dell'operazione di divisione.
- Il volume principale deve essere online perché la divisione abbia successo.

### Fasi

1. Determinare la quantità di spazio libero necessaria per completare l'operazione di suddivisione:

```
volume clone show -estimate -vserver vs1 -flexclone clone1 -parent-volume vol1
```

Nell'esempio seguente vengono fornite informazioni sullo spazio libero necessario per separare il volume FlexClone "clone1" dal volume padre "vol1":

```
cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1 -parent-volume vol1
```

Vserver	FlexClone	Split Estimate
vs1	clone1	40.73MB

2. Verificare che l'aggregato contenente il volume FlexClone e il relativo elemento di origine disponga di spazio sufficiente:
  - a. Determinare la quantità di spazio libero nell'aggregato che contiene il volume FlexClone e il relativo elemento di origine:
 

```
storage aggregate show
```
  - b. Se l'aggregato contenente non dispone di spazio libero sufficiente, aggiungere storage all'aggregato:
 

```
storage aggregate add-disks
```
3. Avviare l'operazione di divisione:

```
volume clone split start -vserver vs1 -flexclone clone1 -parent-volume vol1
```

Nell'esempio seguente viene illustrato come avviare il processo di divisione del volume FlexClone "clone1" dal volume padre "vol1":



```
cluster1::> volume clone split start -vserver vs1 -flexclone clone1

Warning: Are you sure you want to split clone volume clone1 in Vserver
vs1 ?
{y|n}: y
[Job 1617] Job is queued: Split clone1.
```

#### 4. Monitorare lo stato dell'operazione di split FlexClone:

```
volume clone split show -vserver vserver_name -flexclone clone_volume_name
```

L'esempio seguente mostra lo stato dell'operazione di split FlexClone su un sistema AFF:

```
cluster1::> volume clone split show -vserver vs1 -flexclone clone1

Inodes
Blocks
-----
Vserver    FlexClone    Processed Total    Scanned    Updated    % Inode
% Block

Complete   Complete
vs1        clone1       0          0        411247    153600     0
37
```

#### 5. Verificare che il volume suddiviso non sia più un volume FlexClone:

```
volume show -volume volume_name -fields clone-volume
```

Il valore di clone-volume L'opzione è "false" per un volume che non è un volume FlexClone.

Nell'esempio riportato di seguito viene illustrato come verificare se il volume "clone1" diviso dal suo padre non è un volume FlexClone.

```
cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
----- **-----**
vs1        clone1 **false**
```

### Determinare lo spazio utilizzato da un volume FlexClone

È possibile determinare lo spazio utilizzato da un volume FlexClone in base alle sue dimensioni nominali e alla quantità di spazio che condivide con il volume FlexVol padre. Quando viene creato un volume FlexClone, tutti i dati vengono condivisi con il volume

padre. Pertanto, anche se le dimensioni nominali del volume FlexVol sono le stesse delle dimensioni del suo padre, utilizza pochissimo spazio libero dall'aggregato.

### A proposito di questa attività

Lo spazio libero utilizzato da un volume FlexClone appena creato è circa il 0.5% delle dimensioni nominali. Questo spazio viene utilizzato per memorizzare i metadati del volume FlexClone.

I nuovi dati scritti nel volume padre o FlexClone non vengono condivisi tra i volumi. L'aumento della quantità di nuovi dati scritti nel volume FlexClone comporta un aumento dello spazio richiesto dal volume FlexClone dall'aggregato contenente.

### Fase

1. Determinare lo spazio fisico effettivo utilizzato dal volume FlexClone utilizzando `volume show` comando.

L'esempio seguente mostra lo spazio fisico totale utilizzato dal volume FlexClone:

```
cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
size,used,available,
percent-used,physical-used,physical-used-percent
vserver      volume      size  available  used    percent-used  physical-
used         physical-used-percent
-----
vs01         clone_vol1  20MB  18.45MB    564KB   7%            196KB
1%
```

### Considerazioni per la creazione di un volume FlexClone da un volume di origine o di destinazione SnapMirror

È possibile creare un volume FlexClone dal volume di origine o di destinazione in una relazione SnapMirror di un volume esistente. Tuttavia, ciò potrebbe impedire il corretto completamento delle future operazioni di replica di SnapMirror.

La replica potrebbe non funzionare perché quando si crea il volume FlexClone, è possibile bloccare una copia Snapshot utilizzata da SnapMirror. In questo caso, SnapMirror interrompe la replica nel volume di destinazione fino a quando il volume FlexClone non viene distrutto o separato dal volume padre. Sono disponibili due opzioni per risolvere questo problema:

- Se si richiede temporaneamente il volume FlexClone e si riesce a contenere un'interruzione temporanea della replica SnapMirror, è possibile creare il volume FlexClone ed eliminarlo o separarlo dal relativo volume padre, se possibile.

La replica di SnapMirror continua normalmente quando il volume FlexClone viene cancellato o separato dal volume padre.

- Se un'interruzione temporanea della replica SnapMirror non è accettabile, è possibile creare una copia Snapshot nel volume di origine di SnapMirror e utilizzarla per creare il volume FlexClone. Se si crea il volume FlexClone dal volume di destinazione, è necessario attendere che la copia Snapshot venga replicata nel volume di destinazione di SnapMirror.

Questo metodo di creazione di una copia Snapshot nel volume di origine di SnapMirror consente di creare il clone senza bloccare una copia Snapshot utilizzata da SnapMirror.

## Utilizzare i file FlexClone e le LUN FlexClone per creare copie efficienti di file e LUN

### Utilizzare i file FlexClone e le LUN FlexClone per creare copie efficienti di file e panoramica delle LUN

I file FlexClone e le LUN FlexClone sono cloni scrivibili ed efficienti in termini di spazio dei file padre e delle LUN padre e contribuiscono a un utilizzo efficiente dello spazio di aggregato fisico. I file FlexClone e i LUN FlexClone sono supportati solo per i volumi FlexVol.

I file FlexClone e le LUN FlexClone utilizzano il 0.4% delle loro dimensioni per memorizzare i metadati. I cloni condividono i blocchi di dati dei file padre e delle LUN padre e occupano uno spazio di storage trascurabile fino a quando i client non scrivono nuovi dati nel file padre o LUN o nel clone.

I client possono eseguire tutte le operazioni di file e LUN sulle entità padre e clone.

È possibile utilizzare diversi metodi per eliminare i file FlexClone e le LUN FlexClone.

### Creare un file FlexClone o un LUN FlexClone

È possibile creare cloni di file e LUN presenti nei volumi FlexVol o FlexClone efficienti in termini di spazio e tempo utilizzando `volume file clone create` comando.

#### Di cosa hai bisogno

- La licenza FlexClone deve essere installata sul cluster. Questa licenza è inclusa con "ONTAP uno".
- Se vengono utilizzati più intervalli di blocchi per la clonazione sotto-LUN o per la clonazione sotto-file, i numeri di blocco non devono sovrapporsi.
- Se si crea un file secondario o un file secondario su volumi con compressione adattiva attivata, gli intervalli di blocchi non devono essere disallineati.

Ciò significa che il numero del blocco iniziale di origine e il numero del blocco iniziale di destinazione devono essere allineati pari o dispari.

#### A proposito di questa attività

A seconda dei privilegi assegnati dall'amministratore del cluster, un amministratore SVM può creare file FlexClone e LUN FlexClone.

È possibile specificare l'impostazione di eliminazione automatica per i file FlexClone e le LUN FlexClone quando si creano e modificano i cloni. Per impostazione predefinita, l'eliminazione automatica è disattivata.

È possibile sovrascrivere un file FlexClone o un LUN FlexClone esistente quando si crea un clone utilizzando `volume file clone create` con il `-overwrite-destination` parametro.

Quando il nodo raggiunge il carico di divisione massimo, il nodo interrompe temporaneamente l'accettazione delle richieste di creazione dei file FlexClone e dei LUN FlexClone ed emette un `EBUSY` messaggio di errore. Quando il carico suddiviso per il nodo scende al di sotto del massimo, il nodo accetta le richieste di creazione di file FlexClone e LUN FlexClone di nuovo. Prima di riprovare la richiesta di creazione, attendere che il nodo disponga della capacità necessaria per creare i cloni.

## Fasi

1. Creare un file FlexClone o un LUN FlexClone utilizzando `volume file clone create` comando.

Nell'esempio seguente viene illustrato come creare un file FlexClone `file1_clone` del file padre `file1_source` nel volume `vol1`:

```
cluster1::> volume file clone create -vserver vs0 -volume vol1 -source  
-path /file1_source -destination-path /file1_clone
```

Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine man.

## Informazioni correlate

["Comandi di ONTAP 9"](#)

### Visualizza la capacità del nodo per la creazione e l'eliminazione di file FlexClone e LUN FlexClone

È possibile verificare se un nodo ha la capacità di ricevere nuove richieste per creare ed eliminare file FlexClone e LUN FlexClone visualizzando il carico suddiviso per il nodo. Se viene raggiunto il carico di divisione massimo, non vengono accettate nuove richieste fino a quando il carico di divisione non scende al di sotto del massimo.

#### A proposito di questa attività

Quando il nodo raggiunge il carico di divisione massimo, viene visualizzato `EBUSY` viene visualizzato un messaggio di errore in risposta alla creazione e all'eliminazione delle richieste. Quando il carico suddiviso per il nodo scende al di sotto del massimo, il nodo accetta le richieste di creare ed eliminare nuovamente i file FlexClone e i LUN FlexClone.

Un nodo può accettare nuove richieste quando il campo carico suddiviso ammesso visualizza la capacità e la richiesta di creazione rientra nella capacità disponibile.

## Fase

1. Visualizza la capacità di un nodo di creare ed eliminare file FlexClone e LUN FlexClone utilizzando `volume file clone split load show` comando.

Nell'esempio seguente, il carico suddiviso viene visualizzato per tutti i nodi nel cluster1. Tutti i nodi del cluster hanno la capacità di creare ed eliminare file FlexClone e LUN FlexClone come indicato dal campo carico suddiviso ammesso:

```
cluster1::> volume file clone split load show
```

Node	Max Split	Current Load	Token Reserved	Allowable Load
node1	15.97TB	0B	100MB	15.97TB
node2	15.97TB	0B	100MB	15.97TB

2 entries were displayed.

## Scopri i risparmi di spazio dovuti ai file FlexClone e alle LUN FlexClone

È possibile visualizzare la percentuale di spazio su disco salvato dalla condivisione a blocchi all'interno di un volume contenente file FlexClone e LUN.

### Fase

1. Per visualizzare il risparmio di spazio ottenuto dai file FlexClone e dalle LUN FlexClone, immettere il seguente comando:

```
df -s volname
```

volname È il nome del volume FlexVol.



Se si esegue `df -s` Su un volume FlexVol abilitato alla deduplica, è possibile visualizzare lo spazio salvato sia dai file di deduplica che da FlexClone e LUN.

### Esempio

L'esempio seguente mostra il risparmio di spazio su un test di un volume FlexClone 1:

```
systemA> df -s test1
```

Filesystem	used	saved	%saved	Vserver
/vol/test1/	4828	5744	54%	vs1

## Metodi per eliminare i file FlexClone e le LUN FlexClone

È possibile utilizzare diversi metodi per eliminare i file FlexClone e le LUN FlexClone. La comprensione dei metodi disponibili consente di pianificare la gestione dei cloni.

Per eliminare i file FlexClone e le LUN FlexClone, è possibile utilizzare i seguenti metodi:

- È possibile configurare un volume FlexVol per eliminare automaticamente i cloni con l'opzione di eliminazione automatica attivata quando lo spazio libero in un volume FlexVol scende al di sotto di una determinata soglia.
- È possibile configurare i client per eliminare i cloni utilizzando NetApp Manageability SDK.
- È possibile utilizzare i client per eliminare i cloni utilizzando i protocolli NAS e SAN.

Il metodo di eliminazione più lento è attivato per impostazione predefinita perché questo metodo non utilizza NetApp Manageability SDK. Tuttavia, è possibile configurare il sistema in modo che utilizzi il metodo di eliminazione più rapida quando si eliminano i file FlexClone utilizzando `volume file clone deletion` comandi.

## Come un volume FlexVol può recuperare spazio libero con l'impostazione di eliminazione automatica

Come un volume FlexVol può recuperare spazio libero con una panoramica delle impostazioni di eliminazione automatica

È possibile attivare l'impostazione di eliminazione automatica di un volume FlexVol per

eliminare automaticamente i file FlexClone e i LUN FlexClone. Attivando l'eliminazione automatica, è possibile recuperare una quantità di spazio libero di destinazione nel volume quando un volume è quasi pieno.

È possibile configurare un volume in modo che avvii automaticamente l'eliminazione dei file FlexClone e dei LUN FlexClone quando lo spazio libero nel volume scende al di sotto di un determinato valore di soglia e interrompa automaticamente l'eliminazione dei cloni quando viene recuperata una quantità di spazio libero di destinazione nel volume. Sebbene non sia possibile specificare il valore di soglia che avvia l'eliminazione automatica dei cloni, è possibile specificare se un clone è idoneo per l'eliminazione ed è possibile specificare la quantità di spazio libero di destinazione per un volume.

Un volume elimina automaticamente i file FlexClone e i LUN FlexClone quando lo spazio libero nel volume scende al di sotto di una determinata soglia e quando vengono soddisfatti i seguenti requisiti:

- La funzione di eliminazione automatica è attivata per il volume che contiene i file FlexClone e i LUN FlexClone.

È possibile attivare la funzione di eliminazione automatica per un volume FlexVol utilizzando `volume snapshot autodelete modify` comando. È necessario impostare `-trigger` parametro a `volume` oppure `snap_reserve` Per eliminare automaticamente i file FlexClone e le LUN FlexClone di un volume.

- La funzione di eliminazione automatica è abilitata per i file FlexClone e le LUN FlexClone.

È possibile attivare l'eliminazione automatica per un file FlexClone o un LUN FlexClone utilizzando `file clone create` con il `-autodelete` parametro. Di conseguenza, è possibile conservare alcuni file FlexClone e LUN FlexClone disattivando l'eliminazione automatica per i cloni e garantendo che altre impostazioni del volume non sovrascrivano l'impostazione del clone.

#### Configurare un volume FlexVol per eliminare automaticamente i file FlexClone e i LUN FlexClone

È possibile abilitare un volume FlexVol per eliminare automaticamente i file FlexClone e i LUN FlexClone con l'eliminazione automatica attivata quando lo spazio libero nel volume scende al di sotto di una determinata soglia.

#### Di cosa hai bisogno

- Il volume FlexVol deve contenere file FlexClone e LUN FlexClone ed essere online.
- Il volume FlexVol non deve essere un volume di sola lettura.

#### Fasi

1. Attivare l'eliminazione automatica dei file FlexClone e dei LUN FlexClone nel volume FlexVol utilizzando `volume snapshot autodelete modify` comando.
  - Per `-trigger` è possibile specificare `volume` oppure `snap_reserve`.
  - Per `-destroy-list` è necessario specificare sempre `lun_clone`, `file_clone` indipendentemente dal fatto che si desideri eliminare un solo tipo di clone. Nell'esempio seguente viene illustrato come attivare il volume vol1 per l'eliminazione automatica dei file FlexClone e dei LUN FlexClone per il recupero dello spazio fino a quando il 25% del volume non è costituito da spazio libero:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume  
vol1 -enabled true -commitment disrupt -trigger volume -target-free  
-space 25 -destroy-list lun_clone,file_clone
```

```
Volume modify successful on volume:vol1
```



Durante l'attivazione dell'eliminazione automatica dei volumi FlexVol, se si imposta il valore di `-commitment` parametro a. `destroy`, Tutti i file FlexClone e le LUN FlexClone con `-autodelete` parametro impostato su `true` potrebbe essere cancellato quando lo spazio libero nel volume scende al di sotto del valore di soglia specificato. Tuttavia, FlexClone Files e FlexClone LUN con `-autodelete` parametro impostato su `false` non verrà eliminato.

2. Verificare che l'eliminazione automatica dei file FlexClone e dei LUN FlexClone sia attivata nel volume FlexVol utilizzando `volume snapshot autodelete show` comando.

L'esempio seguente mostra che il volume `vol1` è abilitato per l'eliminazione automatica di file FlexClone e LUN FlexClone:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1
```

```
Vserver Name: vs1  
Volume Name: vol1  
Enabled: true  
Commitment: disrupt  
Defer Delete: user_created  
Delete Order: oldest_first  
Defer Delete Prefix: (not specified)  
Target Free Space: 25%  
Trigger: volume  
*Destroy List: lun_clone,file_clone*  
Is Constituent Volume: false
```

3. Assicurarsi che l'eliminazione automatica sia attivata per i file FlexClone e le LUN FlexClone nel volume che si desidera eliminare, procedendo come segue:

- a. Attivare l'eliminazione automatica di un file FlexClone o di un LUN FlexClone specifico utilizzando `volume file clone autodelete` comando.

È possibile forzare l'eliminazione automatica di un file FlexClone o di un LUN FlexClone specifico utilizzando `volume file clone autodelete` con il `-force` parametro.

L'esempio seguente mostra che è attivata l'eliminazione automatica del LUN `Lun1_clone` FlexClone contenuto nel volume `vol1`:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path  
/vol/vol1/lun1_clone -enabled true
```

È possibile attivare l'eliminazione automatica quando si creano file FlexClone e LUN FlexClone.

- b. Verificare che il file FlexClone o il LUN FlexClone sia abilitato per l'eliminazione automatica utilizzando `volume file clone show-autodelete` comando.

L'esempio seguente mostra che il LUN lun 1\_clone FlexClone è abilitato per l'eliminazione automatica:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone  
-path vol/vol1/lun1_clone  
Vserver Name: vs1  
Clone Path: vol/vol1/lun1_clone  
**Autodelete Enabled: true**
```

Per ulteriori informazioni sull'utilizzo dei comandi, vedere le rispettive pagine man.

#### Impedire l'eliminazione automatica di un file FlexClone o di un LUN FlexClone specifico

Se si configura un volume FlexVol per eliminare automaticamente i file FlexClone e le LUN FlexClone, qualsiasi clone che soddisfa i criteri specificati potrebbe essere cancellato. Se si desidera conservare file FlexClone o LUN FlexClone specifici, è possibile escluderli dal processo di eliminazione automatica di FlexClone.

#### Di cosa hai bisogno

È necessario installare una licenza FlexClone. Questa licenza è inclusa con ["ONTAP uno"](#).

#### A proposito di questa attività

Quando si crea un file FlexClone o un LUN FlexClone, per impostazione predefinita l'eliminazione automatica del clone viene disattivata. I file FlexClone e i LUN FlexClone con eliminazione automatica disattivata vengono conservati quando si configura un volume FlexVol per eliminare automaticamente i cloni per recuperare spazio sul volume.



Se si imposta `commitment` sul volume a. `try` oppure `disrupt`, È possibile conservare file FlexClone specifici o LUN FlexClone disabilitando l'eliminazione automatica per tali cloni. Tuttavia, se si imposta `commitment` sul volume a. `destroy` e le liste `destroy` includono `lun_clone`, `file_clone`, L'impostazione del volume sovrascrive l'impostazione del clone e tutti i file FlexClone e i LUN FlexClone possono essere cancellati indipendentemente dall'impostazione di eliminazione automatica per i cloni.

#### Fasi

1. Impedire l'eliminazione automatica di un file FlexClone o di un LUN FlexClone specifico utilizzando `volume file clone autodelete` comando.

Nell'esempio seguente viene illustrato come disattivare l'eliminazione automatica per FlexClone LUN lun1\_clone contenuto in vol1:



```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1  
-clone-path lun1_clone -enable false
```

Un file FlexClone o un LUN FlexClone con eliminazione automatica disattivata non può essere cancellato automaticamente per recuperare spazio sul volume.

2. Verificare che l'eliminazione automatica sia disattivata per il file FlexClone o per il LUN FlexClone utilizzando `volume file clone show-autodelete` comando.

L'esempio seguente mostra che l'eliminazione automatica è falsa per il LUN `lun 1_clone` FlexClone:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path  
vol/vol1/lun1_clone  
  
Name: vs1  
vol/vol1/lun1_clone  
Enabled: false  
  
Vserver  
Clone Path:  
Autodelete
```

#### Comandi per la configurazione dell'eliminazione dei file FlexClone

Quando i client eliminano i file FlexClone senza utilizzare NetApp Manageability SDK, è possibile utilizzare `volume file clone deletion` Comandi per consentire un'eliminazione più rapida dei file FlexClone da un volume FlexVol. Le estensioni e le dimensioni minime dei file FlexClone vengono utilizzate per consentire un'eliminazione più rapida.

È possibile utilizzare `volume file clone deletion` Comandi per specificare un elenco di estensioni supportate e un requisito di dimensione minima per i file FlexClone in un volume. Il metodo di eliminazione più rapida viene utilizzato solo per i file FlexClone che soddisfano i requisiti. Per i file FlexClone che non soddisfano i requisiti, viene utilizzato il metodo di eliminazione più lento.

Quando i client eliminano i file FlexClone e le LUN FlexClone da un volume utilizzando NetApp Manageability SDK, i requisiti di estensione e dimensione non si applicano perché viene sempre utilizzato il metodo di eliminazione più veloce.

Per...	Utilizzare questo comando...
Aggiungere un interno all'elenco di interni supportati per il volume	<code>volume file clone deletion add-extension</code>
Modificare le dimensioni minime dei file FlexClone che possono essere cancellati dal volume utilizzando il metodo di eliminazione più rapida	<code>volume file clone deletion modify</code>

Per...	Utilizzare questo comando...
Rimuovere un interno dall'elenco di interni supportati per il volume	<code>volume file clone deletion remove-extension</code>
Visualizzare l'elenco di estensioni supportate e le dimensioni minime dei file FlexClone che i client possono eliminare dal volume utilizzando il metodo di eliminazione più rapida	<code>volume file clone deletion show</code>

Per informazioni dettagliate su questi comandi, consulta la pagina man appropriata.

## Utilizzare qtree per partizionare i volumi FlexVol

### Utilizzare qtree per partizionare la panoramica dei volumi FlexVol

I qtree consentono di suddividere i volumi FlexVol in segmenti più piccoli che è possibile gestire singolarmente. È possibile utilizzare qtree per gestire le quote, lo stile di protezione e gli oplock CIFS.

ONTAP crea un qtree predefinito, denominato *qtree0*, per ogni volume. Se i dati non vengono inseriti in un qtree, risiedono in *qtree0*.

I nomi di qtree non devono contenere più di 64 caratteri.

Impossibile spostare le directory tra qtree. Solo i file possono essere spostati tra i qtree.

Se si creano condivisioni a livello di qtree e di volume sullo stesso pool di FlexVol o SCVMM, i qtree vengono visualizzati come directory nella condivisione di FlexVol. Pertanto, è necessario fare attenzione a non eliminarle accidentalmente.

### Ottenere un percorso di giunzione qtree

È possibile montare un singolo qtree ottenendo il percorso di giunzione o il percorso dello spazio dei nomi del qtree. Il percorso del qtree visualizzato dal comando CLI `qtree show -instance` è del formato `/vol/<volume_name>/<qtree_name>`. Tuttavia, questo percorso non fa riferimento al percorso di giunzione o al percorso dello spazio dei nomi del qtree.

### A proposito di questa attività

È necessario conoscere il percorso di giunzione del volume per ottenere il percorso di giunzione o il percorso dello spazio dei nomi del qtree.

### Fase

1. Utilizzare `vserver volume junction-path` per ottenere il percorso di giunzione di un volume.

Nell'esempio seguente viene visualizzato il percorso di giunzione del volume denominato `vol1` situato sulla macchina virtuale di storage (SVM) denominata `vs0`:

```
cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path  
  
-----  
  
vs0 vol1 /vol1
```

Dal suddetto output, il percorso di giunzione del volume è /vol1. Poiché i qtree sono sempre radicati nel volume, il percorso di giunzione o il percorso dello spazio dei nomi del qtree sarà /vol1/qtree1.

### Restrizioni del nome del qtree

I nomi di qtree non possono superare i 64 caratteri. Inoltre, l'utilizzo di alcuni caratteri speciali nei nomi qtree, come virgole e spazi, può causare problemi con altre funzionalità e deve essere evitato.

["Ulteriori informazioni sul comportamento e sui vincoli della CLI durante la creazione dei nomi dei file".](#)

### Convertire una directory in un qtree

#### Convertire una directory in una panoramica di qtree

Se si dispone di una directory nella directory principale di un volume FlexVol che si desidera convertire in un qtree, è necessario migrare i dati contenuti nella directory in un nuovo qtree con lo stesso nome, utilizzando l'applicazione client.

#### A proposito di questa attività

La procedura da seguire per convertire una directory in un qtree dipende dal client utilizzato. La seguente procedura descrive le attività generali da completare:

#### Fasi

1. Rinominare la directory da creare in un qtree.
2. Creare un nuovo qtree con il nome della directory originale.
3. Utilizzare l'applicazione client per spostare il contenuto della directory nel nuovo qtree.
4. Eliminare la directory ora vuota.



Non è possibile eliminare una directory se associata a una condivisione CIFS esistente.

#### Convertire una directory in un qtree utilizzando un client Windows

Per convertire una directory in un qtree utilizzando un client Windows, rinominare la directory, creare un qtree sul sistema di storage e spostare il contenuto della directory nel qtree.

#### A proposito di questa attività

Per eseguire questa procedura, è necessario utilizzare Esplora risorse. Non è possibile utilizzare l'interfaccia della riga di comando di Windows o l'ambiente dei prompt DOS.

## Fasi

1. Aprire Esplora risorse.
2. Fare clic sulla rappresentazione della cartella della directory che si desidera modificare.



La directory deve risiedere nella directory principale del volume contenente.

3. Dal menu **file**, selezionare **Rinomina** per assegnare a questa directory un nome diverso.
4. Sul sistema storage, utilizzare `volume qtree create` per creare un nuovo qtree con il nome originale della directory.
5. In Esplora risorse, aprire la cartella di directory rinominata e selezionare i file al suo interno.
6. Trascinare questi file nella rappresentazione della cartella del nuovo qtree.



Maggiore è il numero di sottocartelle contenute nella cartella che si sta spostando, maggiore sarà la durata dell'operazione di spostamento.

7. Dal menu **file**, selezionare **Delete** (Elimina) per eliminare la cartella di directory vuota e rinominata.

## Convertire una directory in un qtree utilizzando un client UNIX

Per convertire una directory in un qtree in UNIX, rinominare la directory, creare un qtree sul sistema di storage e spostare il contenuto della directory nel qtree.

## Fasi

1. Aprire una finestra del client UNIX.
2. Utilizzare `mv` per rinominare la directory.

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. Dal sistema storage, utilizzare `volume qtree create` per creare un qtree con il nome originale.

```
system1: volume qtree create /n/user1/vol1/dir1
```

4. Dal client, utilizzare `mv` comando per spostare il contenuto della vecchia directory nel qtree.



Maggiore è il numero di sottodirectory contenute in una directory che si sta spostando, maggiore sarà la durata dell'operazione di spostamento.

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

5. Utilizzare `rmdir` comando per eliminare la vecchia directory ora vuota.

```
client: rmdir /n/user1/vol1/olddir
```

## Al termine

A seconda di come il client UNIX implementa `mv` il comando, la proprietà del file e le autorizzazioni potrebbero non essere conservati. In questo caso, aggiornare i proprietari e le autorizzazioni dei file ai valori precedenti.

## Comandi per la gestione e la configurazione di qtree

È possibile gestire e configurare qtree utilizzando specifici comandi ONTAP.

Se si desidera...	Utilizzare questo comando...
Creare un qtree	<code>volume qtree create</code>
Visualizza un elenco filtrato di qtree	<code>volume qtree show</code>
Eliminare un qtree	<code>volume qtree delete</code>   Il comando <code>qtree volume qtree delete</code> non riesce a meno che il qtree non sia vuoto o il <code>-force true</code> viene aggiunto il flag.
Modificare le autorizzazioni UNIX di un qtree	<code>volume qtree modify -unix-permissions</code>
Modificare l'impostazione degli oplock CIFS di un qtree	<code>volume qtree oplocks</code>
Modificare l'impostazione di sicurezza di un qtree	<code>volume qtree security</code>
Rinominare un qtree	<code>volume qtree rename</code>
Visualizzare le statistiche di un qtree	<code>volume qtree statistics</code>
Ripristinare le statistiche di un qtree	<code>volume qtree statistics -reset</code>



Il `volume rehost` il comando può causare il malfunzionamento di altre operazioni amministrative simultanee destinate a quel volume.

## Creazione di report e applicazione dello spazio logico per i volumi

### Report e applicazione dello spazio logico per la panoramica dei volumi

A partire da ONTAP 9.4, è possibile consentire agli utenti di visualizzare lo spazio logico utilizzato in un volume e la quantità di spazio di storage rimanente. A partire da ONTAP 9.5, è possibile limitare la quantità di spazio logico consumata dagli utenti.

Per impostazione predefinita, il reporting e l'imposizione dello spazio logico sono disattivati.

I seguenti tipi di volume supportano l'applicazione e il reporting dello spazio logico.

Tipo di volume	Il reporting dello spazio è supportato?	L'applicazione dello spazio è supportata?
Volumi FlexVol	Sì, a partire da ONTAP 9.4	Sì, a partire da ONTAP 9.5
Volumi di destinazione di SnapMirror	Sì, a partire da ONTAP 9.8	Sì, a partire da ONTAP 9.13.1
Volumi FlexGroup	Sì, a partire da ONTAP 9.9.1	Sì, a partire da ONTAP 9.9.1
Volumi FlexCache	L'impostazione di origine viene utilizzata nella cache	Non applicabile

### Cosa mostra il reporting dello spazio logico

Quando si attiva il reporting dello spazio logico su un volume, il sistema può visualizzare la quantità di spazio logico utilizzato e disponibile oltre allo spazio totale in un volume. Inoltre, gli utenti sui sistemi client Linux e Windows possono visualizzare lo spazio logico utilizzato e disponibile invece dello spazio fisico utilizzato e fisico disponibile.

Definizioni:

- Lo spazio fisico si riferisce ai blocchi fisici di storage disponibili o utilizzati nel volume.
- Lo spazio logico si riferisce allo spazio utilizzabile in un volume.
- Lo spazio logico utilizzato è lo spazio fisico utilizzato e i risparmi derivanti dalle funzionalità di efficienza dello storage (come deduplica e compressione) configurate.

A partire da ONTAP 9.5, è possibile attivare l'imposizione dello spazio logico insieme al reporting dello spazio.

Quando questa opzione è attivata, il report dello spazio logico visualizza i seguenti parametri con `volume show` comando:

Parametro	Significato
<code>-logical-used</code>	Visualizza solo le informazioni relative al volume o ai volumi con le dimensioni logiche utilizzate specificate. Questo valore include tutto lo spazio risparmiato dalle funzionalità di efficienza dello storage e lo spazio fisicamente utilizzato. Ciò non include la riserva di Snapshot, ma prende in considerazione la fuoriuscita di Snapshot.
<code>-logical-used-by-afs</code>	Visualizza solo le informazioni relative al volume o ai volumi che hanno la dimensione logica specificata utilizzata dal file system attivo. Questo valore differisce da <code>-logical-used</code> Valore in base alla quantità di snapshot che supera la riserva Snapshot.

Parametro	Significato
<code>-logical-available</code>	Quando è attivato solo il reporting dello spazio logico, viene visualizzato solo lo spazio fisico disponibile. Quando sono abilitati sia il reporting dello spazio che l'applicazione, viene visualizzata la quantità di spazio libero attualmente disponibile considerando lo spazio risparmiato dalle funzionalità di efficienza dello storage come utilizzato. Non include la riserva di snapshot.
<code>-logical-used</code> <code>-percent</code>	Visualizza la percentuale della corrente <code>-logical-used</code> Valore con le dimensioni fornite escludendo la riserva Snapshot del volume.  Questo valore può essere superiore al 100%, perché il <code>-logical-used-by-afs</code> il valore include risparmi in termini di efficienza in termini di volume. Il <code>-logical-used-by-afs</code> Il valore di un volume non include la perdita Snapshot come spazio utilizzato. Il <code>-physical-used</code> Il valore di un volume include la perdita Snapshot come spazio utilizzato.
<code>-used</code>	Visualizza la quantità di spazio occupato dai dati dell'utente e dai metadati del file system. È diverso da <code>physical-used</code> spazio calcolato in base alla somma dello spazio riservato alle scritture future e dello spazio salvato dall'efficienza dello storage aggregato. Include Snapshot spill (la quantità di spazio con cui le copie Snapshot superano la riserva di Snapshot). Non include la Snapshot Reserve.

L'abilitazione del reporting dello spazio logico nella CLI consente anche la visualizzazione dei valori di spazio logico utilizzato (%) e spazio logico in System Manager

I sistemi client visualizzano lo spazio logico visualizzato come “used” (utilizzato) sui seguenti display di sistema:

- Output **df** su sistemi Linux
- Dettagli dello spazio in Proprietà utilizzo di Esplora risorse su sistemi Windows.



Se il reporting dello spazio logico è abilitato senza l'imposizione dello spazio logico, il totale visualizzato sui sistemi client può essere superiore allo spazio fornito.

## Che cosa fa l'imposizione dello spazio logico

Quando si attiva l'imposizione dello spazio logico in ONTAP 9.5 e versioni successive, ONTAP conta i blocchi logici utilizzati in un volume per determinare la quantità di spazio ancora disponibile in tale volume. Se non c'è spazio disponibile in un volume, il sistema restituisce un messaggio di errore ENOSPC (spazio esaurito).

L'applicazione dello spazio logico garantisce che gli utenti ricevano una notifica quando un volume è pieno o quasi pieno. L'imposizione dello spazio logico restituisce tre tipi di avvisi per informare l'utente sullo spazio disponibile in un volume:

- `Monitor.vol.full.inc.sav`: Questo avviso viene attivato quando viene utilizzato il 98% dello spazio logico nel volume.
- `Monitor.vol.nearFull.inc.sav`: Questo avviso viene attivato quando viene utilizzato il 95% dello spazio logico nel volume.

- `Vol.log.overalloc.inc.sav`: Questo avviso viene attivato quando lo spazio logico utilizzato nel volume è maggiore della dimensione totale del volume.

Questo avviso indica che l'aggiunta alle dimensioni del volume potrebbe non creare spazio disponibile, poiché tale spazio verrà già consumato dai blocchi logici overallocati.



Lo spazio totale (spazio logico) deve essere uguale allo spazio fornito, escludendo la riserva Snapshot del volume con applicazione dello spazio logico.

Per ulteriori informazioni, vedere ["Configurazione dei volumi per fornire automaticamente più spazio quando sono pieni"](#)

## Abilitare il reporting e l'applicazione dello spazio logico

A partire da ONTAP 9.4, è possibile attivare il reporting dello spazio logico. A partire da 9.5, è possibile abilitare l'applicazione dello spazio logico, o sia il reporting che l'applicazione congiunta.

### A proposito di questa attività

Oltre a consentire il reporting e l'applicazione dello spazio logico a livello di singolo volume, è possibile abilitarli a livello di SVM per ogni volume che supporta tale funzionalità. Se si abilitano le funzionalità di spazio logico per l'intera SVM, è possibile disattivarle anche per singoli volumi.

A partire da ONTAP 9.8, se si attiva la creazione di report dello spazio logico su un volume di origine SnapMirror, questo viene attivato automaticamente sul volume di destinazione dopo il trasferimento.

A partire da ONTAP 9.13.1, se l'opzione di imposizione è attivata su un volume di origine SnapMirror, la destinazione riporta il consumo di spazio logico e ne rispetta l'applicazione, consentendo una migliore pianificazione della capacità.



Se si esegue una release di ONTAP precedente a ONTAP 9.13.1, si deve comprendere che, sebbene l'impostazione di imposizione venga trasferita al volume di destinazione di SnapMirror, il volume di destinazione non supporta l'imposizione. Di conseguenza, la destinazione riporta il consumo di spazio logico, ma non rispetta la sua applicazione.

Scopri di più ["Supporto della release ONTAP per il reporting dello spazio logico"](#).

### Scelte

- Abilitare il reporting dello spazio logico per un volume:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true
```

- Abilitare l'imposizione dello spazio logico per un volume:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-enforcement-logical true
```

- Abilitare insieme il reporting e l'applicazione dello spazio logico per un volume:

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true -is-space-enforcement-logical true
```



- Abilitare il reporting o l'applicazione dello spazio logico per una nuova SVM:

```
vserver create -vserver _svm_name_ -rootvolume root-_volume_name_ -rootvolume
-security-style unix -data-services {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

- Abilitare il reporting o l'imposizione dello spazio logico per una SVM esistente:

```
vserver modify -vserver _svm_name_ {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

## Gestire i limiti di capacità SVM

A partire da ONTAP 9.13.1, è possibile impostare una capacità massima per una VM di storage (SVM). È inoltre possibile configurare gli avvisi quando SVM si avvicina a un livello di capacità di soglia.

### A proposito di questa attività

La capacità su una SVM viene calcolata come somma di FlexVol, volumi FlexGroup, FlexClone e volumi FlexCache. I volumi influiscono sul calcolo della capacità anche se sono limitati, offline o nella coda di ripristino dopo l'eliminazione. Se si dispone di volumi configurati con la crescita automatica, il valore di dimensionamento automatico massimo del volume viene calcolato in base alle dimensioni SVM; senza la crescita automatica, viene calcolata la dimensione effettiva del volume.

La seguente tabella illustra come `autosize-mode` i parametri influiscono sul calcolo della capacità.

<code>autosize-mode off</code>	Il parametro <code>size</code> verrà utilizzato per il calcolo
<code>autosize-mode grow</code>	Il <code>max-autosize</code> il parametro verrà utilizzato per il calcolo
<code>autosize-mode grow-shrink</code>	Il <code>max-autosize</code> il parametro verrà utilizzato per il calcolo

### Prima di iniziare

- Per impostare un limite SVM, è necessario essere un amministratore del cluster.
- I limiti di storage non possono essere configurati per qualsiasi SVM che contiene volumi di protezione dei dati, volumi in una relazione SnapMirror o in una configurazione MetroCluster.
- Quando si esegue la migrazione di una SVM, la SVM di origine non può avere un limite di storage abilitato. Per completare l'operazione di migrazione, disattivare il limite di storage sull'origine, quindi completare la migrazione.
- La capacità SVM è distinta da [quote](#). Le quote non possono superare la dimensione massima.
- Non è possibile impostare un limite di storage quando sono in corso altre operazioni su SVM. Utilizzare `job show vservser svm_name` per visualizzare i lavori esistenti. Provare ad eseguire nuovamente il comando una volta completati i lavori.

### Impatto sulla capacità

Una volta raggiunto il limite di capacità, le seguenti operazioni non vengono eseguite correttamente:


- Creazione di un LUN, uno spazio dei nomi o un volume

- Clonare un LUN, uno spazio dei nomi o un volume
- Modifica di un LUN, di uno spazio dei nomi o di un volume
- Aumento delle dimensioni di un LUN, di uno spazio dei nomi o di un volume
- Espansione di un LUN, di uno spazio dei nomi o di un volume
- Eseguire il rehosting di un LUN, di uno spazio dei nomi o di un volume

## Impostare un limite di capacità su una nuova SVM

### System Manager

#### Fasi

1. Selezionare **Storage > Storage VM**.
2. Selezionare  Per creare la SVM.
3. Assegnare un nome alla SVM e selezionare un protocollo **Access**.
4. In **Storage VM settings**, selezionare **Enable maximum Capacity limit**.

Fornire una dimensione massima della capacità per SVM.

5. Selezionare **Salva**.

### CLI

#### Fasi

1. Creare la SVM. Per impostare un limite di storage, fornire un `storage-limit` valore. Per impostare un avviso di soglia per il limite di storage, fornire un valore percentuale per `-storage-limit -threshold-alert`.

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} -storage
-limit value [GiB|TiB] -storage-limit-threshold-alert percentage [-ipspace
IPspace_name] [-language <language>] [-snapshot-policy
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

Se non si fornisce un valore di soglia, per impostazione predefinita viene attivato un avviso quando la SVM raggiunge la capacità del 90%. Per disattivare l'avviso di soglia, fornire un valore pari a zero.

2. Verificare che la SVM sia stata creata correttamente:

```
vserver show -vserver vserver_name
```

3. Se si desidera disattivare il limite di storage, modificare la SVM con `-storage-limit` parametro impostato su zero:

```
vserver modify -vserver vserver_name -storage-limit 0
```


## Impostare o modificare un limite di capacità su una SVM esistente

È possibile impostare un limite di capacità e un avviso di soglia su una SVM esistente o disattivare un limite di capacità.

Una volta impostato il limite di capacità, non è possibile modificarlo su un valore inferiore alla capacità attualmente allocata.

## System Manager

### Fasi

1. Selezionare **Storage > Storage VM**.
2. Selezionare la SVM che si desidera modificare. Accanto al nome della SVM, selezionare  Quindi **Modifica**.
3. Per attivare un limite di capacità, selezionare la casella accanto a **Enable Capacity Limit** (attiva limite di capacità). Inserire un valore per la **capacità massima** e un valore percentuale per la **soglia di avviso**.

Se si desidera disattivare il limite di capacità, deselezionare la casella accanto a **Enable Capacity Limit** (attiva limite di capacità).

4. Selezionare **Salva**.

### CLI

#### Fasi

1. Sul cluster che ospita la SVM, eseguire il `vserver modify` comando. Fornire un valore numerico per `-storage-limit` e un valore percentuale per `-storage-limit-threshold-alert`.

```
vserver modify -vserver vserver_name -storage-limit value [GiB|TiB]
-storage-limit-threshold-alert percentage
```

Se non si fornisce un valore di soglia, viene visualizzato un avviso predefinito al 90% della capacità. Per disattivare l'avviso di soglia, fornire un valore pari a zero.

2. Se si desidera disattivare il limite di storage, modificare la SVM con `-storage-limit` impostare su zero:

```
vserver modify -vserver vserver_name -storage-limit 0
```

## Raggiungimento dei limiti di capacità

Una volta raggiunta la capacità massima o la soglia di avviso, consultare `vserver.storage.threshold` Messaggi EMS o utilizzare la pagina **Insights** di System Manager per informazioni sulle possibili azioni. Le possibili risoluzioni includono:

- Modifica dei limiti di capacità massima SVM
- Eliminazione della coda di recovery dei volumi per liberare spazio
- Elimina snapshot per fornire spazio al volume

## Ulteriori informazioni

- [Misurazioni della capacità in System Manager](#)
- [Monitorare la capacità in System Manager](#)

# Utilizzare le quote per limitare o tenere traccia dell'utilizzo delle risorse

## Panoramica del processo di quota

### Processo di quota

Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree. Le quote vengono applicate a un volume o qtree FlexVol specifico.

Le quote possono essere morbide o difficili. Le quote morbide fanno sì che ONTAP invii una notifica quando vengono superati i limiti specificati, mentre le quote rigide impediscono il successo di un'operazione di scrittura quando vengono superati i limiti specificati.

Quando ONTAP riceve una richiesta di scrittura su un volume FlexVol da parte di un utente o di un gruppo di utenti, verifica se le quote sono attivate su tale volume per l'utente o il gruppo di utenti e determina quanto segue:

- Se verrà raggiunto il limite massimo

In caso affermativo, l'operazione di scrittura non riesce quando viene raggiunto il limite massimo e viene inviata la notifica della quota rigida.

- Se il limite di tolleranza verrà violato

In caso affermativo, l'operazione di scrittura riesce quando il limite di tolleranza viene superato e viene inviata la notifica della quota di tolleranza.

- Se un'operazione di scrittura non supera il limite di tolleranza

In caso affermativo, l'operazione di scrittura ha esito positivo e non viene inviata alcuna notifica.

### Differenze tra quote rigide, morbide e di soglia

Le quote rigide impediscono le operazioni mentre le quote morbide attivano le notifiche.

Le quote rigide impongono un limite massimo alle risorse di sistema; qualsiasi operazione che comporterebbe il superamento del limite fallisce. Le seguenti impostazioni creano le quote rigide:

- Parametro disk limit
- Parametro limite file

Le quote morbide inviano un messaggio di avviso quando l'utilizzo delle risorse raggiunge un determinato livello, ma non influiscono sulle operazioni di accesso ai dati, in modo da poter intraprendere le azioni appropriate prima che la quota venga superata. Le seguenti impostazioni creano quote soft:

- Soglia per il parametro Disk Limit
- Parametro Soft Disk Limit
- Parametro di limite dei file soft

Le quote Threshold e Soft Disk consentono agli amministratori di ricevere più di una notifica su una quota. In genere, gli amministratori impostano il valore Threshold for Disk Limit (soglia per limite disco) su un valore solo leggermente inferiore al limite del disco, in modo che la soglia fornisca un "avviso finale" prima che la scrittura

inizi a non riuscire.

### Informazioni sulle notifiche delle quote

Le notifiche delle quote sono messaggi inviati al sistema di gestione degli eventi (EMS) e configurati anche come trap SNMP.

Le notifiche vengono inviate in risposta ai seguenti eventi:

- Viene raggiunta una quota rigida; in altre parole, si tenta di superarla
- Viene superata una quota soft
- Una quota soft non viene più superata

Le soglie sono leggermente diverse dalle altre quote morbide. Le soglie attivano le notifiche solo quando vengono superate, non quando non vengono più superate.

Le notifiche delle quote rigide sono configurabili utilizzando il comando di modifica della quota del volume. È possibile disattivarle completamente e modificarne la frequenza, ad esempio per impedire l'invio di messaggi ridondanti.

Le notifiche delle quote non sono configurabili perché è improbabile che generino messaggi ridondanti e il loro unico scopo è la notifica.

La seguente tabella elenca gli eventi che le quote inviano al sistema EMS:

Quando ciò si verifica...	Questo evento viene inviato al sistema EMS...
Viene raggiunto un limite massimo in una quota ad albero	<code>wafl.quota.qtree.exceeded</code>
Viene raggiunto un limite massimo in una quota utente sul volume	<code>wafl.quota.user.exceeded</code> (Per utenti UNIX) <code>wafl.quota.user.exceeded.win</code> (Per utenti Windows)
Viene raggiunto un limite massimo in una quota utente su un qtree	<code>wafl.quota.userQtree.exceeded</code> (Per utenti UNIX) <code>wafl.quota.userQtree.exceeded.win</code> (Per utenti Windows)
Viene raggiunto un limite massimo in una quota di gruppo sul volume	<code>wafl.quota.group.exceeded</code>
Viene raggiunto un limite massimo in una quota di gruppo su un qtree	<code>wafl.quota.groupQtree.exceeded</code>
Viene superato un limite di tolleranza, compresa una soglia	<code>quota.softlimit.exceeded</code>
Non viene più superato un limite di tolleranza	<code>quota.softlimit.normal</code>

Nella tabella seguente sono elencati i trap SNMP generati dalle quote:

Quando ciò si verifica...	Questa trap SNMP viene inviata...
Viene raggiunto un limite massimo	QuotaExceed
Viene superato un limite di tolleranza, compresa una soglia	QuotaExceed e softQuotaExceed
Non viene più superato un limite di tolleranza	QuotaNormal e softQuotaNormal



Le notifiche contengono numeri di ID qtree piuttosto che nomi qtree. È possibile correlare i nomi di qtree ai numeri ID utilizzando `volume qtree show -id` comando.

### Perché utilizzare le quote

È possibile utilizzare le quote per limitare l'utilizzo delle risorse nei volumi FlexVol, fornire notifiche quando l'utilizzo delle risorse raggiunge livelli specifici o tenere traccia dell'utilizzo delle risorse.

Specificare una quota per i seguenti motivi:

- Per limitare la quantità di spazio su disco o il numero di file che possono essere utilizzati da un utente o un gruppo o che possono essere contenuti da un qtree
- Per tenere traccia della quantità di spazio su disco o del numero di file utilizzati da un utente, un gruppo o un qtree, senza imporre alcun limite
- Per avvisare gli utenti quando l'utilizzo del disco o del file è elevato

Utilizza le quote predefinite, esplicite, derivate e tracciate per gestire l'utilizzo del disco nel modo più efficiente.

### Quali sono le regole delle quote, le policy delle quote e le quote

Le quote sono definite in regole di quota specifiche per i volumi FlexVol. Queste regole di quota vengono raccolte in una policy di quota di una macchina virtuale di storage (SVM) e attivate su ciascun volume della SVM.

Una regola di quota è sempre specifica per un volume. Le regole di quota non hanno alcun effetto fino a quando le quote non vengono attivate sul volume definito nella regola di quota.

Un criterio di quota è un insieme di regole di quota per tutti i volumi di una SVM. Le policy di quota non sono condivise tra le SVM. Una SVM può disporre di un massimo di cinque criteri di quota, che consentono di disporre di copie di backup dei criteri di quota. Una policy di quota viene assegnata a una SVM in qualsiasi momento.

Una quota è la restrizione effettiva che ONTAP applica o il monitoraggio effettivo che ONTAP esegue. Una regola di quota determina sempre almeno una quota e potrebbe comportare molte quote derivate aggiuntive. L'elenco completo delle quote applicate è visibile solo nei report delle quote.

L'attivazione è il processo di attivazione di ONTAP per la creazione di quote applicate dall'attuale set di regole di quota nel criterio di quota assegnato. L'attivazione avviene volume per volume. La prima attivazione delle quote su un volume viene chiamata inizializzazione. Le attivazioni successive sono chiamate reinizializzazione.

o ridimensionamento, a seconda dell'ambito delle modifiche.




Quando si inizializzano o si ridimensionano le quote su un volume, si attivano le regole di quota nel criterio di quota attualmente assegnato alla SVM.

### Destinazioni e tipi di quota

Le quote hanno un tipo: Possono essere utente, gruppo o albero. Le destinazioni di quota specificano l'utente, il gruppo o il qtree per cui vengono applicati i limiti di quota.

La tabella seguente elenca i tipi di target di quota, i tipi di quote a cui ciascun target di quota è associato e il modo in cui ciascun target di quota è rappresentato:

Destinazione della quota	Tipo di quota	Come viene rappresentato il target	Note
utente	quota utente	Nome utente UNIX UID UNIX  File o directory il cui UID corrisponde all'utente  Nome utente Windows in formato precedente a Windows 2000  SID di Windows  File o directory con un ACL di proprietà del SID dell'utente	Le quote utente possono essere applicate a un volume o qtree specifico.
gruppo	quota di gruppo	Nome del gruppo UNIX GID  Un file o una directory il cui GID corrisponde al gruppo	Le quote di gruppo possono essere applicate a un volume o qtree specifico.   ONTAP non applica quote di gruppo basate sugli ID Windows.
qtree	quota ad albero	nome del qtree	Le quote ad albero vengono applicate a un particolare volume e non influiscono sui qtree di altri volumi.
""	quota di preventivi utente  quota ad albero	Virgolette doppie ("")	Una destinazione di quota di "" indica una <i>quota predefinita</i> . Per le quote predefinite, il tipo di quota è determinato dal valore del campo tipo.

### Come funzionano le quote predefinite

È possibile utilizzare le quote predefinite per applicare una quota a tutte le istanze di un determinato tipo di quota. Ad esempio, una quota utente predefinita influisce su tutti gli utenti del sistema per il volume FlexVol o qtree specificato. Inoltre, le quote predefinite consentono di modificare facilmente le quote.

È possibile utilizzare le quote predefinite per applicare automaticamente un limite a un ampio set di destinazioni di quota senza dover creare quote separate per ciascuna destinazione. Ad esempio, se si desidera limitare la maggior parte degli utenti a 10 GB di spazio su disco, è possibile specificare una quota utente predefinita di 10 GB di spazio su disco invece di creare una quota per ciascun utente. Se si dispone di utenti specifici per i quali si desidera applicare un limite diverso, è possibile creare quote esplicite per tali utenti. (Quote esplicite—quote con una destinazione specifica o un elenco di destinazioni—override quote predefinite.)

Inoltre, le quote predefinite consentono di utilizzare il ridimensionamento anziché la reinizializzazione quando si desidera che le modifiche delle quote abbiano effetto. Ad esempio, se si aggiunge una quota utente esplicita a un volume che ha già una quota utente predefinita, è possibile attivare la nuova quota ridimensionando.

Le quote predefinite possono essere applicate a tutti e tre i tipi di destinazione delle quote (utenti, gruppi e qtree).

Le quote predefinite non hanno necessariamente limiti specifici; una quota predefinita può essere una quota di controllo.

Una quota è indicata da una destinazione che è una stringa vuota ("" ) o un asterisco (\*), a seconda del contesto:

- Quando si crea una quota utilizzando `volume quota policy rule create`, impostazione di `-target` parametro su una stringa vuota ("" ) crea una quota predefinita.
- In `volume quota policy rule create` il comando `-qtree parameter` specifica il nome del qtree a cui si applica la regola di quota. Questo parametro non è applicabile alle regole del tipo di struttura. Per le regole di tipo utente o gruppo a livello di volume, questo parametro deve contenere "".
- Nell'output di `volume quota policy rule show` viene visualizzata una quota predefinita con una stringa vuota ("" ) come destinazione.
- Nell'output di `volume quota report` Viene visualizzata una quota predefinita con un asterisco (\*) come identificatore di ID e quota.

### Esempio di quota utente predefinita

La seguente regola di quota utilizza una quota utente predefinita per applicare un limite di 50 MB a ciascun utente per vol1:



```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default			Volume: vol1	
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Soft Files Limit	Soft Files Limit
Threshold							
-----	-----	-----	-----	-----	-----	-----	-----
user	""	""	off	50MB	-	-	-

Se un utente del sistema immette un comando che richiederebbe ai dati di quell'utente più di 50 MB in vol1 (ad esempio, scrivendo su un file da un editor), il comando non riesce.

### Modalità di utilizzo delle quote esplicite

È possibile utilizzare le quote esplicite per specificare una quota per una destinazione di quota specifica o per eseguire l'override di una quota predefinita per una destinazione specifica.

Una quota esplicita specifica un limite per un particolare utente, gruppo o qtree. Una quota esplicita sostituisce qualsiasi quota predefinita esistente per la stessa destinazione.

Quando si aggiunge una quota utente esplicita per un utente che ha una quota utente derivata, è necessario utilizzare la stessa impostazione di mappatura utente della quota utente predefinita. In caso contrario, quando si ridimensionano le quote, la quota utente esplicita viene rifiutata perché viene considerata una nuova quota.

Le quote esplicite influiscono solo sulle quote predefinite allo stesso livello (volume o qtree). Ad esempio, una quota utente esplicita per un qtree non influisce sulla quota utente predefinita per il volume che contiene tale qtree. Tuttavia, la quota utente esplicita per il qtree sovrascrive (sostituisce i limiti definiti da) la quota utente predefinita per quel qtree.

### Esempi di quote esplicite

Le seguenti regole di quota definiscono una quota utente predefinita che limita tutti gli utenti in vol1 a 50MB di spazio. Tuttavia, a un utente, jsmith, è consentito 80MB di spazio, a causa della quota esplicita (mostrata in grassetto):

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith" -qtree "" -disk-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	""	""	off	50MB	-	-	-
user	jsmith	""	off	80MB	-	-	-

La seguente regola di quota limita l'utente specificato, rappresentato da quattro ID, a 550MB GB di spazio su disco e 10.000 file nel volume vol1:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "
jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" -qtree "" -disk
-limit 550m -file-limit 10000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	"jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544"	""	off	550MB	-	10000	-

La seguente regola di quota limita il gruppo eng1 a 150MB di spazio su disco e un numero illimitato di file nel qtree proj1:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type group -target "eng1" -qtree "proj1" -disk-limit
150m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol2
```

Vserver: vs0			Policy: default			Volume: vol2	
					Soft		Soft
			User	Disk	Disk	Files	Files
Type	Target	Qtree	Mapping	Limit	Limit	Limit	Limit
Threshold							
-----	-----	-----	-----	-----	-----	-----	-----
-----							
group	eng1	proj1	off	150MB	-	-	-
-							

La seguente regola di quota limita il qtree proj1 nel volume vol2 a 750MB di spazio su disco e 75.000 file:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type tree -target "proj1" -disk-limit 750m -file
-limit 75000
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol2
```

Vserver: vs0			Policy: default			Volume: vol2	
					Soft		Soft
			User	Disk	Disk	Files	Files
Type	Target	Qtree	Mapping	Limit	Limit	Limit	Limit
Threshold							
-----	-----	-----	-----	-----	-----	-----	-----
-----							
tree	proj1	""	-	750MB	-	75000	-
-							

### Come funzionano le quote derivate

Una quota imposta come risultato di una quota predefinita, invece di una quota esplicita (una quota con una destinazione specifica), viene definita *quota derivata*.

Il numero e la posizione delle quote derivate dipendono dal tipo di quota:

- Una quota ad albero predefinita di un volume crea quote ad albero predefinite derivate per ogni qtree del volume.
- Una quota utente o di gruppo predefinita crea una quota utente o di gruppo derivata per ogni utente o gruppo che possiede un file allo stesso livello (volume o qtree).

- Una quota di gruppo o utente predefinita di un volume crea una quota di gruppo o utente predefinita derivata su ogni qtree che dispone anche di una quota ad albero.

Le impostazioni, compresi i limiti e la mappatura utente, delle quote derivate sono le stesse delle impostazioni delle quote predefinite corrispondenti. Ad esempio, una quota tree predefinita con un limite di 20 GB su un volume crea quote tree derivate con limiti di 20 GB sui qtree del volume. Se una quota predefinita è una quota di rilevamento (senza limiti), anche le quote derivate stanno tracciando le quote.

Per visualizzare le quote derivate, è possibile generare un report delle quote. Nel report, una quota derivata di un utente o di un gruppo è indicata da un identificatore di quota vuoto o asterisco (\*). Una quota ad albero derivata, tuttavia, dispone di un identificatore di quota; per identificare una quota ad albero derivata, è necessario cercare una quota ad albero predefinita sul volume con gli stessi limiti.

Le quote esplicite interagiscono con le quote derivate nei seguenti modi:

- Le quote derivate non vengono create se esiste già una quota esplicita per la stessa destinazione.
- Se esiste una quota derivata quando si crea una quota esplicita per una destinazione, è possibile attivare la quota esplicita ridimensionando invece di dover eseguire un'inizializzazione della quota completa.

### **Modalità di utilizzo delle quote di rilevamento**

Il tracciamento delle quote genera report sull'utilizzo di dischi e file e non limita l'utilizzo delle risorse. Quando si utilizzano le quote di rilevamento, la modifica dei valori delle quote è meno disgregativa, perché è possibile ridimensionare le quote anziché disattivarle e riattivarle.

Per creare una quota di controllo, omettere i parametri Disk Limit (limite disco) e Files Limit (limite file). In questo modo, ONTAP deve monitorare l'utilizzo di dischi e file per la destinazione a quel livello (volume o qtree), senza imporre alcun limite. Le quote di monitoraggio sono indicate nell'output di `show` e il report delle quote con un trattino ("-") per tutti i limiti. ONTAP crea automaticamente quote di rilevamento quando si utilizza l'interfaccia utente di Gestione sistema per creare quote esplicite (quote con destinazioni specifiche). Quando si utilizza la CLI, l'amministratore dello storage crea quote di tracciamento oltre a quote esplicite.

È inoltre possibile specificare una *quota di rilevamento predefinita*, che si applica a tutte le istanze della destinazione. Le quote di rilevamento predefinite consentono di tenere traccia dell'utilizzo di tutte le istanze di un tipo di quota (ad esempio, tutti i qtree o tutti gli utenti). Inoltre, consentono di utilizzare il ridimensionamento anziché la reinizializzazione quando si desidera che le modifiche delle quote abbiano effetto.

### **Esempi**

L'output di una regola di traccia mostra le quote di traccia in essere per un qtree, un utente e un gruppo, come mostrato nell'esempio seguente per una regola di traccia a livello di volume:

Vserver: vs0			Policy: default			Volume: fv1		
			User	Disk	Soft	Files	Soft	
Type	Target	Qtree	Mapping	Limit	Disk Limit	Files Limit	Files Limit	Threshold
-----	-----	-----	-----	-----	-----	-----	-----	-----
tree	""	""	-	-	-	-	-	-
user	""	""	off	-	-	-	-	-
group	""	""	-	-	-	-	-	-

### Modalità di applicazione delle quote

La comprensione delle modalità di applicazione delle quote consente di configurare le quote e di impostare i limiti previsti.

Ogni volta che si tenta di creare un file o di scrivere dati in un file in un volume FlexVol con le quote attivate, i limiti di quota vengono controllati prima di procedere con l'operazione. Se l'operazione supera il limite di dischi o di file, l'operazione viene impedita.

I limiti di quota vengono controllati nel seguente ordine:

1. La quota tree per quel qtree (questo controllo non è rilevante se il file viene creato o scritto in qtree0).
2. La quota utente per l'utente proprietario del file sul volume
3. La quota di gruppo per il gruppo proprietario del file sul volume
4. La quota utente per l'utente proprietario del file sul qtree (questo controllo non è rilevante se il file viene creato o scritto su qtree0).
5. La quota di gruppo per il gruppo proprietario del file sul qtree (questo controllo non è rilevante se il file viene creato o scritto su qtree0).

La quota con il limite minimo potrebbe non essere quella che viene superata per prima. Ad esempio, se una quota utente per il volume vol1 è di 100 GB, E la quota utente per qtree q2 contenuta nel volume vol1 è di 20 GB, il limite di volume potrebbe essere raggiunto per primo se quell'utente ha già scritto più di 80 GB di dati nel volume vol1 (ma al di fuori di qtree q2).

### Considerazioni per l'assegnazione dei criteri di quota

Un criterio di quota è un raggruppamento delle regole di quota per tutti i volumi FlexVol di una SVM. Quando si assegnano i criteri di quota, è necessario tenere presente alcune considerazioni.

- Una SVM ha una policy di quota assegnata in qualsiasi momento. Quando viene creata una SVM, viene creata una policy di quota vuota e assegnata alla SVM. Questo criterio di quota predefinito ha il nome "default", a meno che non venga specificato un nome diverso al momento della creazione della SVM.
- Una SVM può avere fino a cinque policy di quota. Se una SVM dispone di cinque criteri di quota, non è possibile creare un nuovo criterio di quota per la SVM fino a quando non si elimina un criterio di quota esistente.
- Quando è necessario creare una regola di quota o modificare le regole di quota per un criterio di quota, è possibile scegliere uno dei seguenti approcci:

- Se si utilizza un criterio di quota assegnato a una SVM, non è necessario assegnare il criterio di quota alla SVM.
- Se si utilizza un criterio di quota non assegnato e si assegna quindi il criterio di quota a SVM, è necessario disporre di un backup del criterio di quota a cui è possibile ripristinare, se necessario.

Ad esempio, è possibile creare una copia del criterio di quota assegnato, modificarne la copia, assegnarla alla SVM e rinominare il criterio di quota originale.

- È possibile rinominare un criterio di quota anche quando è assegnato a SVM.

## Come funzionano le quote con utenti e gruppi

### Panoramica sul funzionamento delle quote con utenti e gruppi

Quando si specifica un utente o un gruppo come destinazione di una quota, i limiti imposti da tale quota vengono applicati a tale utente o gruppo. Tuttavia, alcuni gruppi e utenti speciali vengono gestiti in modo diverso. Esistono diversi modi per specificare gli ID per gli utenti, a seconda dell'ambiente in uso.

### Come specificare gli utenti UNIX per le quote

È possibile specificare un utente UNIX per una quota utilizzando uno dei tre formati: Il nome utente, l'UID o un file o una directory di proprietà dell'utente.

Per specificare un utente UNIX per una quota, è possibile utilizzare uno dei seguenti formati:

- Il nome utente, ad esempio jsmith.



Non è possibile utilizzare un nome utente UNIX per specificare una quota se tale nome include una barra rovesciata ( @ ) o un simbolo " ". Questo perché ONTAP considera i nomi che contengono questi caratteri come nomi Windows.

- UID, ad esempio 20.
- Il percorso di un file o di una directory di proprietà dell'utente, in modo che l'UID del file corrisponda all'utente.



Se si specifica un nome di file o di directory, è necessario selezionare un file o una directory che durerà fino a quando l'account utente rimane nel sistema.

Se si specifica un nome di file o directory per l'UID, ONTAP non applica una quota a tale file o directory.

### Modalità di specifica degli utenti Windows per le quote

È possibile specificare un utente Windows per una quota utilizzando uno dei tre formati seguenti: Il nome di Windows in formato precedente a Windows 2000, il SID o un file o una directory di proprietà del SID dell'utente.

Per specificare un utente Windows per una quota, è possibile utilizzare uno dei seguenti formati:

- Il nome di Windows in formato precedente a Windows 2000.
- L'ID di protezione (SID), come visualizzato da Windows in forma di testo, ad esempio S-1-5-32-544.
- Il nome di un file o di una directory che ha un ACL di proprietà del SID dell'utente.

Se si specifica un nome di file o di directory, è necessario selezionare un file o una directory che durerà fino a quando l'account utente rimane nel sistema.

Affinché ONTAP ottenga il SID dall'ACL, l'ACL deve essere valido.



Se il file o la directory esiste in un qtree di stile UNIX o se il sistema di storage utilizza la modalità UNIX per l'autenticazione dell'utente, ONTAP applica la quota utente all'utente il cui **UID**, non SID, corrisponde a quello del file o della directory.

Se si specifica un nome di file o directory per identificare un utente per una quota, ONTAP non applica una quota a tale file o directory.

### In che modo le quote predefinite di utenti e gruppi creano quote derivate

Quando si creano quote utente o gruppo predefinite, le quote utente o gruppo derivate corrispondenti vengono create automaticamente per ogni utente o gruppo proprietario di file allo stesso livello.

Le quote di utenti e gruppi derivati vengono create nei seguenti modi:

- Una quota utente predefinita su un volume FlexVol crea quote utente derivate per ogni utente che possiede un file in qualsiasi punto del volume.
- Una quota utente predefinita su un qtree crea quote utente derivate per ogni utente che possiede un file nel qtree.
- Una quota di gruppo predefinita su un volume FlexVol crea quote di gruppo derivate per ogni gruppo che possiede un file in qualsiasi punto del volume.
- Una quota di gruppo predefinita su un qtree crea quote di gruppo derivate per ogni gruppo che possiede un file nel qtree.

Se un utente o un gruppo non possiede file al livello di una quota utente o di gruppo predefinita, le quote derivate non vengono create per l'utente o il gruppo. Ad esempio, se viene creata una quota utente predefinita per qtree proj1 e l'utente jsmith possiede file su un qtree diverso, non viene creata alcuna quota utente derivata per jsmith.

Le quote derivate hanno le stesse impostazioni delle quote predefinite, inclusi limiti e mappatura utente. Ad esempio, se una quota utente predefinita ha un limite di 50 MB di disco e la mappatura utente è attivata, anche le quote derivate risultanti hanno un limite di 50 MB di disco e la mappatura utente è attivata.

Tuttavia, non esistono limiti nelle quote derivate per tre utenti e gruppi speciali. Se i seguenti utenti e gruppi possiedono file al livello di una quota utente o di gruppo predefinita, viene creata una quota derivata con la stessa impostazione di mappatura utente della quota utente o di gruppo predefinita, ma si tratta solo di una quota di controllo (senza limiti):

- Utente root UNIX (UID 0)
- Gruppo root UNIX (GID 0)
- Gruppo BUILTIN/Administrators di Windows

Poiché le quote per i gruppi Windows vengono registrate come quote utente, una quota derivata per questo gruppo è una quota utente derivata da una quota utente predefinita, non una quota di gruppo predefinita.

### Esempio di quote utente derivate

Se si dispone di un volume in cui tre utenti (root, jsmith e bob) possiedono file e si crea una quota utente predefinita sul volume, ONTAP crea automaticamente tre quote utente derivate. Pertanto, dopo aver reinizializzato le quote sul volume, nel report delle quote vengono visualizzate quattro nuove quote:

```
cluster1::> volume quota report
Vserver: vs1
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
Specifier				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
vol1		user	*	0B	50MB	0	-	*
vol1		user	root	5B	-	1	-	
vol1		user	jsmith	30B	50MB	10	-	*
vol1		user	bob	40B	50MB	15	-	*

4 entries were displayed.

La prima nuova riga è la quota utente predefinita creata, identificabile dall'asterisco (\*) come ID. Le altre nuove righe sono le quote utente derivate. Le quote derivate per jsmith e bob hanno lo stesso limite di 50 MB di disco della quota predefinita. La quota derivata per l'utente root è una quota di monitoraggio senza limiti.

### Modalità di applicazione delle quote all'utente root

L'utente root (UID=0) sui client UNIX è soggetto a quote ad albero, ma non a quote utente o di gruppo. Ciò consente all'utente root di intraprendere azioni per conto di altri utenti che altrimenti sarebbero impediti da una quota.

Quando root esegue un cambiamento di proprietà di file o directory o un'altra operazione (come UNIX `chown` Comando) per conto di un utente con meno privilegi, ONTAP controlla le quote in base al nuovo proprietario, ma non segnala errori o interrompe l'operazione, anche se vengono superate le restrizioni di quota rigida del nuovo proprietario. Ciò può essere utile quando un'azione amministrativa, come il ripristino dei dati persi, comporta il superamento temporaneo delle quote.



Una volta eseguito il trasferimento di proprietà, tuttavia, un sistema client segnala un errore di spazio su disco se l'utente tenta di allocare più spazio su disco mentre la quota viene ancora superata.

### Come funzionano le quote con gruppi speciali di Windows

Le quote vengono applicate al gruppo Everyone e al gruppo BUILTIN/Administrators in modo diverso rispetto agli altri gruppi Windows.

Il seguente elenco descrive cosa accade se la destinazione della quota è un ID speciale del gruppo Windows:



- Se la destinazione della quota è il gruppo Everyone, un file il cui ACL indica che il proprietario è Everyone viene conteggiato sotto il SID per Everyone.
- Se la destinazione della quota è BUILTIN/Administrators, la voce viene considerata una quota utente, solo per il monitoraggio.

Non è possibile imporre restrizioni a BUILTIN/Administrators.

Se un membro di BUILTIN/Administrators crea un file, il file è di proprietà di BUILTIN/Administrators e viene conteggiato sotto il SID per BUILTIN/Administrators, non il SID personale dell'utente.



ONTAP non supporta le quote di gruppo basate sugli ID di gruppo Windows. Se si specifica un ID gruppo Windows come destinazione della quota, la quota viene considerata come quota utente.

### Modalità di applicazione delle quote agli utenti con ID multipli

Un utente può essere rappresentato da più ID. È possibile impostare una singola quota utente per tale utente specificando un elenco di ID come destinazione della quota. Un file di proprietà di uno qualsiasi di questi ID è soggetto alla limitazione della quota utente.

Si supponga che un utente disponga dell'UID UNIX 20 e dell'id Windows corp. john\_smith e Engineering. Per questo utente, è possibile specificare una quota in cui la destinazione della quota è un elenco degli ID UID e Windows. Quando l'utente scrive nel sistema di storage, viene applicata la quota specificata, indipendentemente dal fatto che la scrittura abbia origine da UID 20, dall'azienda o dal tecnico.



Regole di quota separate sono considerate destinazioni separate, anche se gli ID appartengono allo stesso utente. Ad esempio, per lo stesso utente è possibile specificare una quota che limiti UID 20 a 1 GB di spazio su disco e un'altra quota che limiti corp/john\_smith a 2 GB di spazio su disco, anche se entrambi gli ID rappresentano lo stesso utente. ONTAP applica le quote separatamente a UID 20 e a john smith.

In questo caso, non viene applicato alcun limite ai tecnici, anche se vengono applicati limiti agli altri ID utilizzati dallo stesso utente.

### Come ONTAP determina gli ID utente in un ambiente misto

Se si dispone di utenti che accedono allo storage ONTAP da client Windows e UNIX, per determinare la proprietà del file vengono utilizzate sia la protezione di Windows che quella di UNIX. Diversi fattori determinano se ONTAP utilizza un ID UNIX o Windows quando si applicano le quote utente.

Se lo stile di protezione del volume qtree o FlexVol che contiene il file è solo NTFS o UNIX, lo stile di protezione determina il tipo di ID utilizzato durante l'applicazione delle quote utente. Per i qtree con lo stile di sicurezza misto, il tipo di ID utilizzato è determinato dalla presenza o meno di un ACL nel file.

La seguente tabella riassume il tipo di ID utilizzato:

Stile di sicurezza	ACL	Nessun ACL
UNIX	ID UNIX	ID UNIX

Stile di sicurezza	ACL	Nessun ACL
Misto	ID Windows	ID UNIX
NTFS	ID Windows	ID Windows

### Come funzionano le quote con più utenti

Quando si inserisce più utenti nella stessa destinazione di quota, i limiti di quota definiti da tale quota non vengono applicati a ciascun utente; in questo caso, i limiti di quota vengono condivisi tra tutti gli utenti elencati nella destinazione di quota.

A differenza dei comandi per la gestione degli oggetti, come volumi e qtree, non è possibile rinominare una destinazione di quota, inclusa una quota multiutente. Ciò significa che, dopo aver definito una quota multiutente, non è possibile modificare gli utenti nella destinazione della quota e non è possibile aggiungere utenti a una destinazione o rimuovere utenti da una destinazione. Se si desidera aggiungere o rimuovere un utente da una quota multiutente, è necessario eliminare la quota contenente tale utente e definire una nuova regola di quota con l'insieme di utenti nella destinazione.



Se si combinano quote utente separate in una quota multiutente, è possibile attivare la modifica ridimensionando le quote. Tuttavia, se si desidera rimuovere utenti da una destinazione di quota con più utenti o aggiungere utenti a una destinazione che ha già più utenti, è necessario reinizializzare le quote prima che la modifica abbia effetto.

### Esempio di più utenti in una regola di quota

Nell'esempio seguente, nella voce quota sono elencati due utenti. I due utenti possono utilizzare fino a 80MB GB di spazio in combinazione. Se uno usa 75MB, l'altro può usare solo 5MB.

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
Threshold							
-----	-----	-----	-----	-----	-----	-----	-----
-----							
user	"jsmith,chen"	""	off	80MB	-	-	-
-							

### Come collegare i nomi UNIX e Windows per le quote

In un ambiente misto, gli utenti possono accedere come utenti Windows o UNIX. È

possibile configurare le quote per riconoscere che l'id UNIX e l'ID Windows di un utente rappresentano lo stesso utente.

Le quote per il nome utente Windows vengono mappate a un nome utente UNIX o viceversa, quando vengono soddisfatte entrambe le seguenti condizioni:

- Il `user-mapping` il parametro è impostato su "on" nella regola di quota per l'utente.
- I nomi utente sono stati mappati con `vserver name-mapping` comandi.

Quando un nome UNIX e Windows vengono mappati insieme, vengono trattati come la stessa persona per determinare l'utilizzo delle quote.

#### Come funzionano le quote con i qtree

È possibile creare quote con un qtree come destinazione; queste quote sono denominate *quote albero*. È inoltre possibile creare quote utente e di gruppo per un qtree specifico. Inoltre, le quote per un volume FlexVol vengono talvolta ereditate dai qtree contenuti in tale volume.

#### Come funzionano le quote ad albero

##### Panoramica sul funzionamento delle quote ad albero

È possibile creare una quota con un qtree come destinazione per limitare le dimensioni del qtree di destinazione. Queste quote sono anche denominate *quote albero*.

Quando si applica una quota a un qtree, il risultato è simile a una partizione del disco, con la differenza che è possibile modificare la dimensione massima del qtree in qualsiasi momento modificando la quota. Quando si applica una quota ad albero, ONTAP limita lo spazio su disco e il numero di file nel qtree, indipendentemente dai proprietari. Nessun utente, inclusi root e membri del gruppo BUILTIN/Administrators, può scrivere nel qtree se l'operazione di scrittura causa il superamento della quota tree.



La dimensione della quota non garantisce una quantità specifica di spazio disponibile. La dimensione della quota può essere superiore alla quantità di spazio libero disponibile per il qtree. È possibile utilizzare `volume quota report` per determinare la quantità effettiva di spazio disponibile nel qtree.

#### Come funzionano le quote utente e di gruppo con i qtree

Le quote della struttura limitano le dimensioni complessive del qtree. Per impedire a singoli utenti o gruppi di utilizzare l'intero qtree, specificare una quota utente o di gruppo per tale qtree.

##### Esempio di quota utente in un qtree

Si supponga di disporre delle seguenti regole di quota:

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
Threshold							
user	""	""	off	50MB	-	-	-
45MB							
user	jsmith	""	off	80MB	-	-	-
75MB							

Si noti che un determinato utente, kjones, occupa troppo spazio in un qtree critico, proj1, che risiede nel vol1. È possibile limitare lo spazio di questo utente aggiungendo la seguente regola di quota:

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "kjones" -qtree "proj1" -disk
-limit 20m -threshold 15m
```

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1
```

Vserver: vs0			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
Threshold							
user	""	""	off	50MB	-	-	-
45MB							
user	jsmith	""	off	80MB	-	-	-
75MB							
user	kjones	proj1	off	20MB	-	-	-
15MB							

### Come le quote ad albero predefinite su un volume FlexVol creano quote ad albero derivate

Quando si crea una quota tree predefinita su un volume FlexVol, le quote tree derivate corrispondenti vengono create automaticamente per ogni qtree di quel volume.

Queste quote derivate hanno gli stessi limiti della quota ad albero predefinita. Se non esistono quote aggiuntive, i limiti hanno i seguenti effetti:

- Gli utenti possono utilizzare lo spazio in un qtree pari a quello assegnato per l'intero volume (a condizione che non superino il limite per il volume utilizzando lo spazio nella root o in un altro qtree).
- Ciascuno dei qtree può crescere per consumare l'intero volume.

L'esistenza di una quota ad albero predefinita su un volume continua a influire su tutti i nuovi qtree aggiunti al volume. Ogni volta che viene creato un nuovo qtree, viene creata anche una quota di albero derivata.

Come tutte le quote derivate, le quote derivate dell'albero presentano i seguenti comportamenti:

- Vengono creati solo se la destinazione non dispone già di una quota esplicita.
- Vengono visualizzati nei report delle quote ma non quando si visualizzano le regole delle quote con `volume quota policy rule show` comando.

### Esempio di quote di albero derivate

Si dispone di un volume con tre qtree (proj1, proj2 e proj3) e l'unica quota ad albero è una quota esplicita sul qtree proj1 che limita le sue dimensioni del disco a 10 GB. Se si crea una quota ad albero predefinita sul volume e si reinizializzano le quote sul volume, il report delle quote ora contiene quattro quote ad albero:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
vol1	proj1	tree	1	0B	10GB	1	-	proj1
vol1		tree	*	0B	20GB	0	-	*
vol1	proj2	tree	2	0B	20GB	1	-	proj2
vol1	proj3	tree	3	0B	20GB	1	-	proj3
...								

La prima riga mostra la quota esplicita originale sul qtree proj1. Tale quota rimane invariata.

La seconda riga mostra la nuova quota ad albero predefinita sul volume. L'asterisco (\*) specifier di quota indica che si tratta di una quota predefinita. Questa quota è il risultato della regola di quota creata.

Le ultime due righe mostrano le nuove quote di albero derivate per i qtree proj2 e proj3. ONTAP ha creato automaticamente queste quote come risultato della quota ad albero predefinita sul volume. Queste quote derivate della struttura hanno lo stesso limite di 20 GB di disco della quota predefinita della struttura nel volume. ONTAP non ha creato una quota tree derivata per il qtree proj1 perché il qtree proj1 aveva già una quota esplicita.

### In che modo le quote utente predefinite su un volume FlexVol influiscono sulle quote per i qtree di quel volume

Se viene definita una quota utente predefinita per un volume FlexVol, viene creata automaticamente una quota utente predefinita per ogni qtree contenuto in quel volume per il quale esiste una quota ad albero esplicita o derivata.

Se esiste già una quota utente predefinita sul qtree, questa rimane inalterata quando viene creata la quota utente predefinita sul volume.

Le quote utente predefinite create automaticamente sui qtree hanno gli stessi limiti della quota utente predefinita creata per il volume.

Una quota utente esplicita per un qtree sovrascrive (sostituisce i limiti applicati da) la quota utente predefinita creata automaticamente, così come sovrascrive una quota utente predefinita su quel qtree creata da un amministratore.

#### **Come le modifiche al qtree influiscono sulle quote**

##### **Panoramica delle modalità con cui le modifiche al qtree influiscono sulle quote**

Quando si elimina, rinomina o si modifica lo stile di sicurezza di un qtree, le quote applicate da ONTAP potrebbero cambiare, a seconda delle quote correnti applicate.

##### **Come l'eliminazione di un qtree influisce sulle quote dell'albero**

Quando si elimina un qtree, tutte le quote applicabili a tale qtree, siano esse esplicite o derivate, non vengono più applicate da ONTAP.

La persistenza delle regole di quota dipende dalla posizione in cui si elimina il qtree:

- Se si elimina un qtree utilizzando ONTAP, le regole di quota per quel qtree vengono automaticamente eliminate, incluse le regole di quota albero e le regole di quota utente e gruppo configurate per quel qtree.
- Se si elimina un qtree utilizzando il client CIFS o NFS, è necessario eliminare qualsiasi regola di quota per quel qtree per evitare di ottenere errori quando si reinizializzano le quote. Se si crea un nuovo qtree con lo stesso nome di quello eliminato, le regole di quota esistenti non vengono applicate al nuovo qtree fino a quando non si reinizializzano le quote.

##### **Il modo in cui la ridenominazione di un qtree influisce sulle quote**

Quando si rinomina un qtree utilizzando ONTAP, le regole di quota per quel qtree vengono aggiornate automaticamente. Se si rinomina un qtree utilizzando il client CIFS o NFS, è necessario aggiornare le regole di quota per tale qtree.



Se si rinomina un qtree utilizzando il client CIFS o NFS e non si aggiornano le regole di quota per quel qtree con il nuovo nome prima di reinizializzare le quote, le quote non verranno applicate al qtree e le quote esplicite per il qtree— includendo le quote ad albero e le quote utente o di gruppo per il qtree—potrebbe essere convertito in quote derivate.

##### **In che modo la modifica dello stile di sicurezza di un qtree influisce sulle quote degli utenti**

È possibile applicare Access Control List (ACL) su qtree utilizzando NTFS o stili di protezione misti, ma non utilizzando lo stile di protezione UNIX. Pertanto, la modifica dello stile di protezione di un qtree potrebbe influire sul calcolo delle quote. Dopo aver modificato lo stile di sicurezza di un qtree, è necessario reinizializzare le quote.

Se si modifica lo stile di sicurezza di un qtree da NTFS o misto a UNIX, tutti gli ACL dei file in quel qtree vengono ignorati e l'utilizzo del file viene addebitato in base agli ID utente UNIX.

Se si modifica lo stile di protezione di un qtree da UNIX a misto o NTFS, gli ACL precedentemente nascosti diventano visibili. Inoltre, tutti gli ACL ignorati diventano nuovamente efficaci e le informazioni utente NFS

vengono ignorate. Se in precedenza non esisteva alcun ACL, le informazioni NFS continuano a essere utilizzate nel calcolo della quota.



Per assicurarsi che gli utilizzi delle quote per gli utenti UNIX e Windows vengano calcolati correttamente dopo aver modificato lo stile di protezione di un qtree, è necessario reinizializzare le quote per il volume che contiene tale qtree.

### Esempio

Nell'esempio seguente viene illustrato come una modifica dello stile di protezione di un qtree comporta l'addebito a un utente diverso dell'utilizzo di un file nel qtree specifico.

Supponiamo che la sicurezza NTFS sia attiva su qtree A e che un ACL dia all'utente Windows corp/joe la proprietà di un file da 5 MB. User corp/joe ha un costo di 5 MB di spazio su disco per qtree A.

Ora si cambia lo stile di sicurezza di qtree A da NTFS a UNIX. Una volta reinizializzate le quote, l'utente di Windows non addebita più questo file all'utente UNIX corrispondente all'UID del file. L'UID potrebbe essere un utente UNIX mappato a corp/joe o all'utente root.

### Modalità di attivazione delle quote

#### Panoramica delle modalità di attivazione delle quote

Le nuove quote e le modifiche alle quote non hanno effetto fino a quando non vengono attivate. Sapere come funziona l'attivazione delle quote può aiutarti a gestire le quote in modo meno disgregabile.

È possibile attivare le quote a livello di volume.

Le quote vengono attivate tramite *inizializzazione* (attivazione) o mediante *ridimensionamento*. La disattivazione e la riattivazione delle quote viene chiamata reinizializzazione.

La durata del processo di attivazione e il suo impatto sull'applicazione delle quote dipendono dal tipo di attivazione:

- Il processo di inizializzazione comprende due parti: A. `quota on job` e una scansione delle quote dell'intero file system del volume. La scansione inizia dopo `quota on` processo completato correttamente. La scansione delle quote può richiedere del tempo; maggiore è il numero di file presenti nel volume, maggiore sarà il tempo necessario. Fino al termine della scansione, l'attivazione della quota non viene completata e le quote non vengono applicate.
- Il processo di ridimensionamento richiede solo un `quota resize` lavoro. Il ridimensionamento richiede meno tempo rispetto all'inizializzazione di una quota perché non comporta una scansione di quota. Durante un processo di ridimensionamento, le quote continuano ad essere applicate.

Per impostazione predefinita, il `quota on` e `quota resize` i lavori vengono eseguiti in background, consentendo di utilizzare contemporaneamente altri comandi.

Gli errori e gli avvisi del processo di attivazione vengono inviati al sistema di gestione degli eventi. Se si utilizza `-foreground` con il `volume quota on` oppure `volume quota resize` il comando non viene restituito fino al completamento del processo; ciò è utile se si esegue una reinizializzazione da uno script. Per visualizzare gli errori e gli avvisi in un secondo momento, è possibile utilizzare `volume quota show` con il `-instance` parametro.

L'attivazione della quota persiste tra gli arresti e si riavvia. Il processo di attivazione delle quote non influisce

sulla disponibilità dei dati del sistema di storage.

### Quando è possibile utilizzare il ridimensionamento

Poiché il ridimensionamento delle quote è più rapido dell'inizializzazione delle quote, è necessario utilizzare il ridimensionamento quando possibile. Tuttavia, il ridimensionamento funziona solo per alcuni tipi di modifiche delle quote.

È possibile ridimensionare le quote quando si apportano i seguenti tipi di modifiche alle regole di quota:

- Modifica di una quota esistente.

Ad esempio, la modifica dei limiti di una quota esistente.

- Aggiunta di una quota per una destinazione di quota per la quale esiste una quota predefinita o una quota di rilevamento predefinita.
- Eliminazione di una quota per la quale è specificata una quota predefinita o una quota di tracciamento predefinita.
- Combinazione di quote utente separate in un'unica quota multiutente.



Dopo aver apportato modifiche estese alle quote, è necessario eseguire una reinizializzazione completa per garantire che tutte le modifiche abbiano effetto.



Se si tenta di ridimensionare e non tutte le modifiche delle quote possono essere incorporate utilizzando un'operazione di ridimensionamento, ONTAP emette un avviso. Dal report delle quote è possibile determinare se il sistema storage sta monitorando l'utilizzo del disco per un determinato utente, gruppo o qtree. Se viene visualizzata una quota nel report delle quote, significa che il sistema di storage sta monitorando lo spazio su disco e il numero di file di proprietà della destinazione della quota.

### Esempio di modifiche alle quote che possono essere rese effettive ridimensionando

Alcune modifiche delle regole di quota possono essere rese effettive ridimensionando. Prendere in considerazione le seguenti quote:

#Quota	Target	type	disk	files	thold	sdisk	sfile
#-----	----		----	-----	-----	-----	-----
*		user@/vol/vol2	50M	15K			
*		group@/vol/vol2	750M	85K			
*		tree@/vol/vol2	-	-			
jdoe		user@/vol/vol2/	100M	75K			
kbuck		user@/vol/vol2/	100M	75K			

Si supponga di apportare le seguenti modifiche:

- Aumentare il numero di file per la destinazione utente predefinita.
- Aggiungere una nuova quota utente per un nuovo utente, boris, che richiede un limite di dischi superiore alla quota utente predefinita.
- Eliminare la voce di quota esplicita dell'utente kbuck; il nuovo utente ora necessita solo dei limiti di quota



predefiniti.

Tali modifiche comportano le seguenti quote:

```
#Quota Target type          disk  files thold  sdisk  sfile
#-----
*          user@/vol/vol2    50M   25K
*          group@/vol/vol2  750M   85K
*          tree@/vol/vol2    -      -
jdoe       user@/vol/vol2/   100M   75K
boris      user@/vol/vol2/   100M   75K
```

Il ridimensionamento attiva tutte queste modifiche; non è necessaria una reinizializzazione della quota completa.

### Quando è richiesta una reinizializzazione della quota completa

Sebbene il ridimensionamento delle quote sia più rapido, è necessario eseguire una reinizializzazione completa delle quote se si apportano modifiche di piccole o grandi dimensioni alle quote.

È necessario eseguire una reinizializzazione della quota completa nei seguenti casi:

- Si crea una quota per una destinazione che non ha in precedenza una quota (né una quota esplicita né una derivata da una quota predefinita).
- Lo stile di sicurezza di un qtree viene modificato da UNIX a misto o NTFS.
- Lo stile di protezione di un qtree viene modificato da misto o NTFS a UNIX.
- Gli utenti vengono rimossi da una destinazione di quota con più utenti o aggiunti a una destinazione che ha già più utenti.
- Le quote vengono modificate in modo esteso.

### Esempio di modifiche delle quote che richiedono l'inizializzazione

Supponiamo di avere un volume che contiene tre qtree e che le uniche quote nel volume siano tre quote ad albero esplicite. Si decide di apportare le seguenti modifiche:

- Aggiungere un nuovo qtree e creare una nuova quota ad albero.
- Aggiungere una quota utente predefinita per il volume.

Entrambe le modifiche richiedono un'inizializzazione della quota completa. Il ridimensionamento non rende effettive le quote.

### Come visualizzare le informazioni sulle quote

### Come visualizzare una panoramica delle informazioni sulle quote

È possibile utilizzare i report sulle quote per visualizzare dettagli quali la configurazione di regole e policy sulle quote, le quote applicate e configurate e gli errori che si verificano durante il ridimensionamento e la reinizializzazione delle quote.

La visualizzazione delle informazioni sulle quote è utile in situazioni come le seguenti:

- Configurazione delle quote, ad esempio per configurare le quote e verificare le configurazioni
- Risposta alle notifiche che lo spazio su disco o i limiti di file saranno presto raggiunti o che sono stati raggiunti
- Rispondere alle richieste di più spazio

### Come utilizzare il report delle quote per visualizzare le quote in vigore

A causa dei diversi modi in cui le quote interagiscono, sono in vigore più quote rispetto a quelle create esplicitamente. Per visualizzare le quote in vigore, è possibile visualizzare il report delle quote.

I seguenti esempi mostrano i report delle quote per diversi tipi di quote applicate su un volume FlexVol vol1 e un qtree q1 contenuto in tale volume:

#### Esempio senza quote utente specificate per il qtree

In questo esempio, esiste un qtree, q1, contenuto nel volume vol1. L'amministratore ha creato tre quote:

- Un limite predefinito di quota della struttura su vol1 di 400MB
- Un limite di quota utente predefinito su vol1 di 100MB
- Un limite di quota utente esplicito su vol1 di 200MB per l'utente jsmith

Le regole di quota per questi contingenti sono simili a quelle dell'esempio seguente:

```
cluster1::*> volume quota policy rule show -vserver vs1 -volume vol1
```

Vserver: vs1			Policy: default		Volume: vol1		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
tree	""	""	-	400MB	-	-	-
user	""	""	off	100MB	-	-	-
user	jsmith	""	off	200MB	-	-	-

Il rapporto sulle quote per queste quote è simile al seguente esempio:

```
cluster1::> volume quota report
Vserver: vs1
```

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
vol1	-	tree	*	0B	400MB	0	-	*
vol1	-	user	*	0B	100MB	0	-	*
vol1	-	user	jsmith	150B	200MB	7	-	jsmith
vol1	q1	tree	1	0B	400MB	6	-	q1
vol1	q1	user	*	0B	100MB	0	-	
vol1	q1	user	jsmith	0B	100MB	5	-	
vol1	-	user	root	0B	0MB	1	-	
vol1	q1	user	root	0B	0MB	8	-	

Le prime tre righe del report di quota visualizzano le tre quote specificate dall'amministratore. Poiché due di queste quote sono quote predefinite, ONTAP crea automaticamente le quote derivate.

La quarta riga visualizza la quota tree derivata dalla quota tree predefinita per ogni qtree in vol1 (in questo esempio, solo q1).

La quinta riga visualizza la quota utente predefinita creata per il qtree in seguito all'esistenza della quota utente predefinita sul volume e sulla quota del qtree.

La sesta riga visualizza la quota utente derivata creata per jsmith sul qtree perché esiste una quota utente predefinita per il qtree (riga 5) e l'utente jsmith possiede i file su quel qtree. Si noti che il limite applicato all'utente jsmith nel qtree Q1 non è determinato dal limite di quota utente esplicito (200MB). Questo perché il limite di quota utente esplicito si trova sul volume, quindi non influisce sui limiti per il qtree. Il limite di quota utente derivato per il qtree è invece determinato dalla quota utente predefinita per il qtree (100MB).

Le ultime due righe visualizzano più quote utente derivate dalle quote utente predefinite sul volume e sul qtree. È stata creata una quota utente derivata per l'utente root sia sul volume che sul qtree, in quanto l'utente root possedeva file sia sul volume che sul qtree. Poiché l'utente root riceve un trattamento speciale in termini di quote, le quote derivate monitorano solo le quote.

### Esempio con le quote utente specificate per il qtree

Questo esempio è simile a quello precedente, ad eccezione del fatto che l'amministratore ha aggiunto due quote nel qtree.

Esiste ancora un volume, vol1 e un qtree, q1. L'amministratore ha creato le seguenti quote:

- Un limite predefinito di quota della struttura su vol1 di 400MB
- Un limite di quota utente predefinito su vol1 di 100MB
- Un limite di quota utente esplicito su vol1 per l'utente jsmith di 200MB
- Limite di quota utente predefinito per il qtree Q1 di 50MB
- Un limite di quota utente esplicito sul qtree Q1 per l'utente jsmith di 75MB

Le regole di quota per queste quote sono le seguenti:

```
cluster1::> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1                      Policy: default                      Volume: vol1
                                     Soft                                     Soft
                                     Disk                                     Files
Type  Target  Qtree  User      Disk      Disk      Files      Files
-----  -----  -----  Mapping   Limit     Limit     Limit     Limit
-----  -----  -----  -----
tree   ""      ""      -          400MB     -         -         -
-
user   ""      ""      off        100MB     -         -         -
-
user   ""      q1      off        50MB      -         -         -
-
user   jsmith  ""      off        200MB     -         -         -
-
user   jsmith  q1      off        75MB      -         -         -
-
```

Il report delle quote per queste quote è simile al seguente:

```
cluster1::> volume quota report

Vserver: vs1
                                     -----Disk-----  -----Files-----  Quota
Volume  Tree    Type  ID      Used  Limit   Used  Limit
Specifier
-----  -----  -----  -----  -----  -----  -----  -----
vol1    -       tree  *       0B    400MB   0      -      *
vol1    -       user  *       0B    100MB   0      -      *
vol1    -       user  jsmith  2000B 200MB   7      -      jsmith
vol1    q1      user  *       0B    50MB    0      -      *
vol1    q1      user  jsmith  0B     75MB    5      -      jsmith
vol1    q1      tree  1       0B    400MB   6      -      q1
vol1    -       user  root    0B     0MB     2      -      -
vol1    q1      user  root    0B     0MB     1      -      -
```

Le prime cinque righe del report delle quote visualizzano le cinque quote create dall'amministratore. Poiché alcune di queste quote sono quote predefinite, ONTAP crea automaticamente quote derivate.

La sesta riga visualizza la quota tree derivata dalla quota tree predefinita per ogni qtree in vol1 (in questo esempio, solo q1).

Le ultime due righe visualizzano le quote utente derivate dalle quote utente predefinite sul volume e sul qtree. È stata creata una quota utente derivata per l'utente root sia sul volume che sul qtree, in quanto l'utente root possedeva file sia sul volume che sul qtree. Poiché l'utente root riceve un trattamento speciale in termini di quote, le quote derivate monitorano solo le quote.

Non sono state create altre quote predefinite o derivate per i seguenti motivi:

- Una quota utente derivata non è stata creata per l'utente jsmith anche se l'utente possiede file sia sul volume che sul qtree, perché l'utente dispone già di quote esplicite a entrambi i livelli.
- Non sono state create quote utente derivate per altri utenti perché nessun altro utente possiede file sul volume o sul qtree.
- La quota utente predefinita sul volume non ha creato una quota utente predefinita sul qtree perché il qtree aveva già una quota utente predefinita.

### **Perché le quote applicate differiscono dalle quote configurate**

Le quote applicate differiscono dalle quote configurate perché le quote derivate vengono applicate senza essere configurate, ma le quote configurate vengono applicate solo dopo che sono state inizializzate correttamente. La comprensione di queste differenze consente di confrontare le quote applicate visualizzate nei report delle quote con quelle configurate.

Le quote applicate, visualizzate nei report delle quote, potrebbero differire dalle regole delle quote configurate per i seguenti motivi:

- Le quote derivate vengono applicate senza essere configurate come regole di quota; ONTAP crea automaticamente le quote derivate in risposta alle quote predefinite.
- Le quote potrebbero non essere state reinizializzate su un volume dopo la configurazione delle regole di quota.
- È possibile che si siano verificati errori durante l'inizializzazione delle quote su un volume.

### **Utilizzare il report delle quote per determinare il limite delle quote di scrittura in un file specifico**

È possibile utilizzare il comando del report quota volume con un percorso di file specifico per determinare quali limiti di quota influiscono sulle operazioni di scrittura in un file. In questo modo è possibile capire quale quota impedisce un'operazione di scrittura.

#### **Fase**

1. Utilizzare il comando volume quota report con il parametro -path.

#### **Esempio di visualizzazione delle quote che influiscono su un file specifico**

L'esempio seguente mostra il comando e l'output per determinare quali quote sono in vigore per le scritture nel file 1, che risiede nel qtree q1 nel volume FlexVol vol2:

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
Volume Specifier								
-----	-----	-----	-----	-----	-----	-----	-----	
vol2	q1	tree	jsmith	1MB	100MB	2	10000	q1
vol2	q1	group	eng	1MB	700MB	2	70000	
vol2		group	eng	1MB	700MB	6	70000	*
vol2		user	corp\jsmith					
				1MB	50MB	1	-	*
vol2	q1	user	corp\jsmith					
				1MB	50MB	1	-	

5 entries were displayed.

## Comandi per la visualizzazione delle informazioni sulle quote

È possibile utilizzare i comandi per visualizzare un report delle quote contenente le quote applicate e l'utilizzo delle risorse, visualizzare informazioni sullo stato delle quote e sugli errori o sui criteri delle quote e sulle regole delle quote.



È possibile eseguire i seguenti comandi solo sui volumi FlexVol.

Se si desidera...	Utilizzare questo comando...
Visualizza informazioni sulle quote applicate	<code>volume quota report</code>
Visualizzare l'utilizzo delle risorse (spazio su disco e numero di file) delle destinazioni di quota	<code>volume quota report</code>
Determinare quali limiti di quota sono interessati quando è consentita la scrittura su un file	<code>volume quota report con -path parametro</code>
Visualizzare lo stato della quota, ad esempio on, off, e. initializing	<code>volume quota show</code>
Consente di visualizzare informazioni sulla registrazione dei messaggi di quota	<code>volume quota show con -logmsg parametro</code>
Visualizza gli errori che si verificano durante l'inizializzazione e il ridimensionamento delle quote	<code>volume quota show con -instance parametro</code>
Visualizza informazioni sulle policy di quota	<code>volume quota policy show</code>

Se si desidera...	Utilizzare questo comando...
Consente di visualizzare informazioni sulle regole delle quote	<code>volume quota policy rule show</code>
Visualizzare il nome del criterio di quota assegnato a una macchina virtuale di storage (SVM, precedentemente noto come Vserver)	<code>vserver show</code> con <code>-instance</code> parametro

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Quando utilizzare i comandi di visualizzazione della regola dei criteri di quota del volume e dei rapporti di quota del volume

Sebbene entrambi i comandi mostrino informazioni sulle quote, il `volume quota policy rule show` visualizza rapidamente le regole di quota configurate durante il `volume quota report command`, che consuma più tempo e risorse, visualizza le quote applicate e l'utilizzo delle risorse.

Il `volume quota policy rule show` il comando è utile per i seguenti scopi:

- Controllare la configurazione delle regole di quota prima di attivarle

Questo comando visualizza tutte le regole di quota configurate, indipendentemente dal fatto che le quote siano state inizializzate o ridimensionate.

- Visualizzazione rapida delle regole di quota senza influire sulle risorse di sistema

Poiché non visualizza l'utilizzo di dischi e file, questo comando non comporta un uso intensivo di risorse come un report delle quote.

- Visualizzare le regole di quota in un criterio di quota non assegnato a SVM.

Il `volume quota report` il comando è utile per i seguenti scopi:

- Visualizzare le quote applicate, incluse le quote derivate
- Visualizzare lo spazio su disco e il numero di file utilizzati da ogni quota in vigore, comprese le destinazioni interessate dalle quote derivate

(Per le quote predefinite, l'utilizzo viene visualizzato come "0" perché l'utilizzo viene monitorato rispetto alla quota derivata risultante).

- Determinare quali limiti di quota influiscono quando è consentita la scrittura su un file

Aggiungere il `-path` al `volume quota report` comando.



Il report delle quote è un'operazione che richiede un uso intensivo delle risorse. Se viene eseguito su molti volumi FlexVol nel cluster, il completamento potrebbe richiedere molto tempo. Un modo più efficiente sarebbe quello di visualizzare il report delle quote per un particolare volume in una SVM.

## Differenza di utilizzo dello spazio visualizzata da un report delle quote e da una panoramica del client UNIX

Il valore dello spazio su disco utilizzato visualizzato in un report di quota per un volume o qtree FlexVol può essere diverso dal valore visualizzato da un client UNIX per lo stesso volume o qtree. La differenza nei valori di utilizzo è dovuta alla differenza nei metodi seguita dal report di quota e dai comandi UNIX per il calcolo dei blocchi di dati nel volume o nel qtree.

Ad esempio, se un volume contiene un file con blocchi di dati vuoti (su cui i dati non vengono scritti), il report delle quote per il volume non conta i blocchi di dati vuoti durante la segnalazione dell'utilizzo dello spazio. Tuttavia, quando il volume viene montato su un client UNIX e il file viene visualizzato come output di `ls` i blocchi di dati vuoti sono inclusi anche nell'utilizzo dello spazio. Pertanto, il `ls` il comando visualizza una dimensione del file più elevata rispetto all'utilizzo dello spazio visualizzato dal report delle quote.

Allo stesso modo, i valori di utilizzo dello spazio mostrati in un report di quota possono anche differire dai valori visualizzati come risultato di comandi UNIX come `df` e `du`.

### In che modo un report sulle quote tiene conto dello spazio su disco e dell'utilizzo dei file

Il numero di file utilizzati e la quantità di spazio su disco specificata in un report di quota per un volume FlexVol o un qtree dipendono dal numero di blocchi di dati utilizzati corrispondente a ogni inode nel volume o nel qtree.

Il numero di blocchi include i blocchi diretti e indiretti utilizzati per i file regolari e di flusso. I blocchi utilizzati per directory, ACL (Access Control List), directory di flusso e metafile non vengono contabilizzati nel report delle quote. Nel caso di file sparse UNIX, i blocchi di dati vuoti non sono inclusi nel report delle quote.

Il sottosistema quota è progettato per considerare e includere solo aspetti controllabili dall'utente del file system. Directory, ACL e spazio di snapshot sono tutti esempi di spazio escluso dai calcoli delle quote. Le quote vengono utilizzate per imporre limiti, non garanzie, e funzionano solo sul file system attivo. La contabilità delle quote non conta determinati costrutti di file system, né tiene conto dell'efficienza dello storage (come compressione o deduplica).

### Il modo in cui il comando `ls` tiene conto dell'utilizzo dello spazio

Quando si utilizza `ls` Comando per visualizzare il contenuto di un volume FlexVol montato su un client UNIX, le dimensioni del file visualizzato nell'output potrebbero essere inferiori o superiori all'utilizzo dello spazio visualizzato nel report delle quote per il volume, a seconda del tipo di blocchi di dati per il file.

L'output di `ls` il comando visualizza solo le dimensioni di un file e non include i blocchi indiretti utilizzati dal file. Anche i blocchi vuoti del file vengono inclusi nell'output del comando.

Pertanto, se un file non ha blocchi vuoti, la dimensione visualizzata da `ls` il comando potrebbe essere inferiore all'utilizzo del disco specificato da un report di quota a causa dell'inclusione di blocchi indiretti nel report di quota. Al contrario, se il file contiene blocchi vuoti, le dimensioni visualizzate da `ls` il comando potrebbe essere superiore all'utilizzo del disco specificato dal report delle quote.

L'output di `ls` il comando visualizza solo le dimensioni di un file e non include i blocchi indiretti utilizzati dal file. Anche i blocchi vuoti del file vengono inclusi nell'output del comando.



## Esempio della differenza tra l'utilizzo dello spazio rappresentato dal comando ls e un report di quota

Il seguente report sulle quote mostra un limite di 10 MB per un qtree q1:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1	q1	tree	user1	10MB	10MB	1	-	q1
...								

Un file presente nello stesso qtree può avere una dimensione che supera il limite di quota quando viene visualizzato da un client UNIX utilizzando `ls` comando, come illustrato nell'esempio seguente:

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x  1 user1 nfsuser  **27M** Apr 09  2013 file1
```

## Il modo in cui il comando df tiene conto della dimensione del file

Il modo in cui in `df` il comando segnala che l'utilizzo dello spazio dipende da due condizioni: se le quote sono attivate o disattivate per il volume che contiene il qtree e se viene rilevato l'utilizzo delle quote all'interno del qtree.

Quando vengono attivate le quote per il volume che contiene l'utilizzo di qtree e quota all'interno del qtree, viene registrato l'utilizzo dello spazio riportato da `df` command è uguale al valore specificato dal report di quota. In questa situazione, l'utilizzo delle quote esclude i blocchi utilizzati da directory, ACL, directory di flusso e metafile.

Quando le quote non sono attivate sul volume o quando il qtree non ha una regola di quota configurata, l'utilizzo dello spazio riportato include i blocchi utilizzati da directory, ACL, directory di flusso e metafile per l'intero volume, inclusi altri qtree all'interno del volume. In questa situazione, l'utilizzo dello spazio riportato da `df` il comando è maggiore del valore previsto riportato quando vengono monitorate le quote.

Quando si esegue `df` dal punto di montaggio di un qtree per il quale viene registrato l'utilizzo della quota, l'output del comando mostra lo stesso utilizzo dello spazio del valore specificato dal report della quota. Nella maggior parte dei casi, quando la regola di quota ad albero ha un limite per il disco rigido, la dimensione totale indicata da `df` il comando equivale al limite del disco e lo spazio disponibile equivale alla differenza tra il limite del disco di quota e l'utilizzo della quota.

Tuttavia, in alcuni casi, lo spazio disponibile riportato da `df` il comando potrebbe essere uguale allo spazio disponibile nel volume nel suo complesso. Questo può verificarsi quando non è configurato alcun limite di dischi rigidi per il qtree. A partire da ONTAP 9.9.1, può verificarsi anche quando lo spazio disponibile nel volume nel suo complesso è inferiore allo spazio di quota ad albero rimanente. Quando si verifica una di queste condizioni, la dimensione totale indicata da `df` Command è un numero sintetizzato uguale alla quota utilizzata all'interno del qtree più lo spazio disponibile nel volume FlexVol.



Questa dimensione totale non corrisponde né al limite del disco qtree né alla dimensione del volume configurato. Può anche variare in base all'attività di scrittura all'interno di altri qtree o all'attività di efficienza dello storage in background.

### Esempio di utilizzo dello spazio rappresentato da df e un report di quota

Il seguente report di quota mostra un limite di 1 GB per qtree alice, 2 GB per qtree bob e nessun limite per qtree project1:

```
C1_vsim1::> quota report -vserver vs0
Vserver: vs0
```

Volume	Tree	Type	ID	-----Disk-----	-----Files-----	Quota		
Specifier				Used	Limit	Used	Limit	
vol2	alice	tree	1	502.0MB	1GB	2	-	alice
vol2	bob	tree	2	1003MB	2GB	2	-	bob
vol2	project1	tree	3	200.8MB	-	2	-	
project1								
vol2		tree	*	0B	-	0	-	*

4 entries were displayed.

Nell'esempio seguente, l'output di df Il comando sui qtree alice e BOB riporta lo stesso spazio utilizzato del report di quota e la stessa dimensione totale (in termini di blocchi 1 M) del limite di dischi. Questo perché le regole di quota per qtree alice e BOB hanno un limite di disco definito e lo spazio disponibile del volume (1211 MB) è maggiore dello spazio di quota ad albero rimanente per qtree alice (523 MB) e qtree Bob (1045 MB).

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem            1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2    1024      502      523   50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem            1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2    2048    1004     1045   50% /mnt/vol2
```

Nell'esempio seguente, l'output di df Il comando sul progetto qtree 1 riporta lo stesso spazio utilizzato del report delle quote, ma la dimensione totale viene sintetizzata aggiungendo lo spazio disponibile nel volume nel suo complesso (1211 MB) all'utilizzo delle quote del progetto qtree 1 (201 MB) per un totale di 1412 MB. Questo perché la regola di quota per il progetto qtree 1 non ha limiti di disco.

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem            1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1412    201      1211  15% /mnt/vol2
```

Nell'esempio seguente viene illustrato l'output di `df` il comando sul volume nel suo complesso riporta lo stesso spazio disponibile del proietto1.



```
linux-client1 [~]$ df -m /mnt/vol2
Filesystem            1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2919  1709      1211  59% /mnt/vol2
```

### Come il comando `du` tiene conto dell'utilizzo dello spazio

Quando si esegue `du` Comando per controllare l'utilizzo dello spazio su disco per un volume `qtree` o `FlexVol` montato su un client UNIX, il valore di utilizzo potrebbe essere superiore al valore visualizzato da un report di quota per il `qtree` o il volume.

L'output di `du` il comando contiene l'utilizzo combinato dello spazio di tutti i file attraverso la struttura di directory a partire dal livello della directory in cui viene emesso il comando. Perché il valore di utilizzo visualizzato da `du` il comando include anche i blocchi di dati per le directory, è superiore al valore visualizzato da un report di quota.

### Esempio della differenza tra l'utilizzo dello spazio rappresentato dal comando `du` e un report di quota

Il seguente report sulle quote mostra un limite di 10 MB per un `qtree` `q1`:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
vol1	q1	tree	user1	10MB	10MB	1	-	q1
...								

Nell'esempio seguente, l'utilizzo dello spazio su disco come output di `du` il comando mostra un valore superiore che supera il limite di quota:

```
[user1@lin-sys1 q1]$ du -sh
**11M**      q1
```

### Esempi di configurazione delle quote

Questi esempi aiutano a comprendere come configurare le quote e leggere i report delle

quote.

Per gli esempi seguenti, si supponga di disporre di un sistema storage che include un SVM, vs1, con un volume, vol1. Per iniziare a impostare le quote, creare un nuovo criterio di quota per SVM con il seguente comando:

```
cluster1::>volume quota policy create -vserver vs1 -policy-name
quota_policy_vs1_1
```

Poiché il criterio di quota è nuovo, viene assegnato a SVM:

```
cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
```

### Esempio 1: Quota utente predefinita

Si decide di imporre un limite massimo di 50 MB per ciascun utente nel vol1:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB
-qtrees ""
```

Per attivare la nuova regola, inizializza le quote sul volume:

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

Per visualizzare il report delle quote, immettere il seguente comando:

```
cluster1::>volume quota report
```

Il report delle quote risultante è simile al report seguente:

```
Vserver: vs1
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
Specifier								
-----	-----	-----	-----	-----	-----	-----	-----	
vol1		user	*	0B	50MB	0	-	*
vol1		user	jsmith	49MB	50MB	37	-	*
vol1		user	root	0B	-	1	-	

La prima riga mostra la quota utente predefinita creata, compreso il limite di dischi. Come tutte le quote predefinite, questa quota utente predefinita non visualizza informazioni sull'utilizzo di disco o file. Oltre alla

quota creata, vengono visualizzate altre due quote, una per ogni utente che attualmente possiede file su vol1. Queste quote aggiuntive sono quote utente derivate automaticamente dalla quota utente predefinita. La quota utente derivata per l'utente jsmith ha lo stesso limite di 50 MB di disco della quota utente predefinita. La quota utente derivata per l'utente root è una quota di monitoraggio (senza limiti).

Se un utente del sistema (diverso dall'utente root) tenta di eseguire un'azione che utilizza più di 50 MB in vol1 (ad esempio, la scrittura su un file da un editor), l'azione non riesce.

### Esempio 2: Quota utente esplicita che sovrascrive una quota utente predefinita

Se è necessario fornire più spazio nel volume vol1 all'utente jsmith, immettere il seguente comando:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit 80MB
-qtrees ""
```

Si tratta di una quota utente esplicita, in quanto l'utente è esplicitamente elencato come destinazione della regola di quota.

Si tratta di una modifica a un limite di quota esistente, in quanto modifica il limite di disco della quota utente derivata per l'utente jsmith sul volume. Pertanto, non è necessario reinizializzare le quote sul volume per attivare la modifica.

Per ridimensionare le quote:

```
cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground
```

Le quote rimangono attive durante il ridimensionamento e il processo di ridimensionamento è breve.

Il report delle quote risultante è simile al report seguente:

```
cluster1::> volume quota report
Vserver: vs1
```

Volume	Tree	Type	ID	----Disk----		----Files----		Quota
				Used	Limit	Used	Limit	
Specifier								
-----	-----	-----	-----	-----	-----	-----	-----	
vol1		user	*	0B	50MB	0	-	*
vol1		user	jsmith	50MB	80MB	37	-	jsmith
vol1		user	root	0B	-	1	-	

3 entries were displayed.

La seconda riga mostra ora un limite di 80 MB di disco e un identificatore di quota di jsmith.

Pertanto, jsmith può utilizzare fino a 80 MB di spazio su vol1, anche se tutti gli altri utenti sono ancora limitati a 50 MB.

### Esempio 3: Soglie

Si supponga di voler ricevere una notifica quando gli utenti raggiungono un massimo di 5 MB dei limiti dei dischi. Per creare una soglia di 45 MB per tutti gli utenti e una soglia di 75 MB per jsmith, modificare le regole di quota esistenti:

```
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target "" -qtree "" -threshold
45MB
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -qtree ""
-threshold 75MB
```

Poiché le dimensioni delle regole esistenti vengono modificate, è possibile ridimensionare le quote sul volume per attivare le modifiche. Attendere il completamento del processo di ridimensionamento.

Per visualizzare il report delle quote con le soglie, aggiungere `-thresholds` al `volume quota report` comando:

```
cluster1::>volume quota report -thresholds
Vserver: vs1
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
				(Thold)				
Specifier								
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1		user	*	0B	50MB (45MB)	0	-	*
vol1		user	jsmith	59MB	80MB (75MB)	55	-	jsmith
vol1		user	root	0B	- ( -)	1	-	

3 entries were displayed.

Le soglie vengono visualizzate tra parentesi nella colonna Disk Limit (limite disco).

### Esempio 4: Quote su qtree

Supponiamo di dover partizionare dello spazio per due progetti. È possibile creare due qtree, denominati proj1 e proj2, per ospitare questi progetti all'interno di vol1.

Attualmente, gli utenti possono utilizzare lo spazio di un qtree pari a quello assegnato per l'intero volume (a condizione che non superino il limite del volume utilizzando lo spazio nella directory principale o in un altro qtree). Inoltre, ciascuno dei qtree può crescere per consumare l'intero volume. Se si desidera garantire che nessuna delle due dimensioni di qtree superi i 20 GB, è possibile creare una quota ad albero predefinita sul volume:

```
cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume voll -type tree -target "" -disk-limit 20GB
```

Si noti che il tipo corretto è *tree*, non *qtree*.

Poiché si tratta di una nuova quota, non è possibile attivarla ridimensionandola. Reinizializzare le quote sul volume:

```
cluster1:>>volume quota off -vserver vs1 -volume voll
cluster1:>>volume quota on -vserver vs1 -volume voll -foreground
```



È necessario attendere circa cinque minuti prima di riattivare le quote su ciascun volume interessato, in quanto si tenta di attivarle quasi immediatamente dopo l'esecuzione di `volume quota off` il comando potrebbe causare errori. In alternativa, è possibile eseguire i comandi per reinizializzare le quote per un volume dal nodo che contiene il volume specifico.

Le quote non vengono applicate durante il processo di reinizializzazione, che richiede più tempo del processo di ridimensionamento.

Quando si visualizza un report delle quote, sono presenti diverse nuove righe: Alcune righe sono per le quote ad albero e altre per le quote utente derivate.

Le nuove righe seguenti si riferiscono alle quote della struttura:

Volume	Tree	Type	ID	-----Disk-----	-----Files-----	Quota	
Specifier				Used	Limit	Used	Limit
-----	-----	-----	-----	-----	-----	-----	-----
...							
voll		tree	*	0B	20GB	0	- *
voll	proj1	tree	1	0B	20GB	1	- proj1
voll	proj2	tree	2	0B	20GB	1	- proj2
...							

La quota ad albero predefinita creata viene visualizzata nella prima nuova riga, con un asterisco (\*) nella colonna ID. In risposta alla quota tree predefinita su un volume, ONTAP crea automaticamente quote tree derivate per ogni qtree del volume. Questi sono mostrati nelle righe in cui proj1 e proj2 appaiono nella colonna Tree.

Le seguenti nuove righe si riferiscono alle quote utente derivate:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
...								
vol1	proj1	user	*	0B	50MB	0	-	
vol1	proj1	user	root	0B	-	1	-	
vol1	proj2	user	*	0B	50MB	0	-	
vol1	proj2	user	root	0B	-	1	-	
...								

Le quote utente predefinite su un volume vengono ereditate automaticamente per tutti i qtree contenuti in quel volume, se le quote sono attivate per i qtree. Quando è stata aggiunta la prima quota qtree, sono state attivate le quote sui qtree. Pertanto, sono state create quote utente predefinite derivate per ogni qtree. Questi sono indicati nelle righe in cui ID è asterisco (\*).

Poiché l'utente root è il proprietario di un file, quando sono state create quote utente predefinite per ciascuno dei qtree, sono state create anche quote di rilevamento speciali per l'utente root su ciascuno dei qtree. Questi vengono visualizzati nelle righe in cui ID è root.

#### Esempio 5: Quota utente su un qtree

Si decide di limitare gli utenti a meno spazio nel qtree proj1 di quanto non ricevano nel volume nel suo complesso. Si desidera evitare che utilizzino più di 10 MB nel qtree proj1. Pertanto, si crea una quota utente predefinita per il qtree:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 10MB
-qtree proj1
```

Si tratta di una modifica a una quota esistente, in quanto modifica la quota utente predefinita per il qtree proj1 derivato dalla quota utente predefinita sul volume. Pertanto, è possibile attivare la modifica ridimensionando le quote. Una volta completato il processo di ridimensionamento, è possibile visualizzare il report delle quote.

Nel report delle quote viene visualizzata la seguente nuova riga che mostra la nuova quota utente esplicita per il qtree:

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1	proj1	user	*	0B	10MB	0	-	*

Tuttavia, all'utente jsmith viene impedito di scrivere più dati nel qtree proj1 perché la quota creata per eseguire l'override della quota utente predefinita (per fornire più spazio) era sul volume. Una volta aggiunta una quota



utente predefinita nel qtree proj1, tale quota viene applicata e limita lo spazio degli utenti in tale qtree, incluso jsmith. Per fornire più spazio all'utente jsmith, aggiungere una regola di quota utente esplicita per il qtree con un limite di 80 MB di disco per sovrascrivere la regola di quota utente predefinita per il qtree:

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit 80MB
-qtree proj1
```

Poiché si tratta di una quota esplicita per la quale esiste già una quota predefinita, la modifica viene attivata ridimensionando le quote. Una volta completato il processo di ridimensionamento, viene visualizzato un report delle quote.

Nel report delle quote viene visualizzata la seguente nuova riga:

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
Specifier								
-----	-----	-----	-----	-----	-----	-----	-----	
-----								
vol1	proj1	user	jsmith	61MB	80MB	57	-	jsmith

Il report finale sulle quote è simile al seguente:

```
cluster1::>volume quota report
Vserver: vs1

Volume  Tree      Type  ID      ----Disk----  ----Files-----  Quota
Specifier                                     Used  Limit    Used  Limit
-----
vol1      tree      *      0B      20GB      0      -      *
vol1      user      *      0B      50MB      0      -      *
vol1      user      jsmith 70MB     80MB     65      -      jsmith
vol1      proj1     tree    1      0B      20GB     1      -      proj1
vol1      proj1     user    *      0B      10MB     0      -      *
vol1      proj1     user    root   0B      -        1      -      -
vol1      proj2     tree    2      0B      20GB     1      -      proj2
vol1      proj2     user    *      0B      50MB     0      -      -
vol1      proj2     user    root   0B      -        1      -      -
vol1      proj2     user    root   0B      -        3      -      -
vol1      proj1     user    jsmith 61MB     80MB     57      -      jsmith
11 entries were displayed.
```

L'utente jsmith deve rispettare i seguenti limiti di quota per la scrittura in un file in proj1:

1. La quota tree per il qtree proj1.
2. La quota utente sul qtree proj1.
3. La quota utente sul volume.

## Impostare le quote su una SVM

Per impostare le quote su una nuova macchina virtuale per lo storage (SVM, precedentemente nota come Vserver), è necessario creare un criterio di quota, aggiungere regole di policy di quota al criterio, assegnare il criterio alla SVM e inizializzare le quote su ciascun volume FlexVol sulla SVM.

### Fasi

1. Immettere il comando `vserver show -instance` Per visualizzare il nome del criterio di quota predefinito creato automaticamente al momento della creazione di SVM.

Se non è stato specificato un nome al momento della creazione della SVM, il nome è "predefinito". È possibile utilizzare `vserver quota policy rename` per assegnare un nome al criterio predefinito.



È inoltre possibile creare una nuova policy utilizzando `volume quota policy create` comando.

2. Utilizzare `volume quota policy rule create` Comando per creare *una qualsiasi* delle seguenti regole di quota per ciascun volume sulla SVM:
  - Regole di quota predefinite per tutti gli utenti
  - Regole di quota esplicite per utenti specifici
  - Regole di quota predefinite per tutti i gruppi
  - Regole di quota esplicite per gruppi specifici
  - Regole di quota predefinite per tutti i qtree
  - Regole di quota esplicite per qtree specifici
3. Utilizzare `volume quota policy rule show` per verificare che le regole di quota siano configurate correttamente.
4. Se si sta lavorando a una nuova policy, utilizzare `vserver modify` Per assegnare il nuovo criterio a SVM.
5. Utilizzare `volume quota on` Per inizializzare le quote su ciascun volume della SVM.

È possibile monitorare il processo di inizializzazione nei seguenti modi:

- Quando si utilizza `volume quota on` è possibile aggiungere il comando `-foreground` parametro per eseguire la quota sul lavoro in primo piano. (Per impostazione predefinita, il processo viene eseguito in background).

Quando il lavoro viene eseguito in background, è possibile monitorarne l'avanzamento utilizzando `job show` comando.

- È possibile utilizzare `volume quota show` per monitorare lo stato dell'inizializzazione della quota.

6. Utilizzare `volume quota show -instance` comando per verificare la presenza di errori di

inizializzazione, come ad esempio le regole di quota che non sono riuscite a inizializzare.

7. Utilizzare `volume quota report` per visualizzare un report delle quote in modo da garantire che le quote applicate corrispondano alle aspettative.

## Modificare (o ridimensionare) i limiti di quota

Quando si apportano modifiche alle dimensioni delle quote esistenti, è possibile ridimensionare le quote su tutti i volumi interessati, il che è più rapido rispetto alla reinizializzazione delle quote su tali volumi.

### A proposito di questa attività

Si dispone di una macchina virtuale per lo storage (SVM, precedentemente nota come Vserver) con quote applicate e si desidera modificare i limiti di dimensione delle quote esistenti o aggiungere o eliminare quote per destinazioni che hanno già quote derivate.

### Fasi

1. Utilizzare `vserver show` con il `-instance` Parametro per determinare il nome del criterio attualmente assegnato a SVM.
2. Modificare le regole di quota eseguendo una delle seguenti operazioni:
  - Utilizzare `volume quota policy rule modify` comando per modificare i limiti dei dischi o dei file delle regole di quota esistenti.
  - Utilizzare `volume quota policy rule create` comando per creare regole di quota esplicite per le destinazioni (utenti, gruppi o qtree) che dispongono attualmente di quote derivate.
  - Utilizzare `volume quota policy rule delete` comando per eliminare regole di quota esplicite per destinazioni (utenti, gruppi o qtree) che hanno anche quote predefinite.
3. Utilizzare `volume quota policy rule show` per verificare che le regole di quota siano configurate correttamente.
4. Utilizzare `volume quota resize` su ogni volume in cui sono state modificate le quote, per attivare le modifiche su ciascun volume.

È possibile monitorare il processo di ridimensionamento in uno dei seguenti modi:

- Quando si utilizza `volume quota resize` è possibile aggiungere il comando `-foreground` parametro per eseguire il lavoro di ridimensionamento in primo piano. (Per impostazione predefinita, il processo viene eseguito in background).

Quando il lavoro viene eseguito in background, è possibile monitorarne l'avanzamento utilizzando `job show` comando.

- È possibile utilizzare `volume quota show` comando per monitorare lo stato di ridimensionamento.

5. Utilizzare `volume quota show -instance` comando per verificare la presenza di errori di ridimensionamento, come ad esempio le regole di quota che non sono riuscite a ridimensionare.

In particolare, controllare gli errori “new Definition” che si verificano quando si ridimensionano le quote dopo l'aggiunta di una quota esplicita per una destinazione che non dispone già di una quota derivata.

6. Utilizzare `volume quota report` per visualizzare un report delle quote in modo da garantire che le quote applicate corrispondano ai requisiti.

## Reinizializzare le quote dopo aver apportato modifiche estese

Quando si apportano modifiche estese alle quote esistenti, ad esempio aggiungendo o eliminando le quote per le destinazioni che non dispongono di quote applicate, è necessario apportare le modifiche e reinizializzare le quote su tutti i volumi interessati.

### A proposito di questa attività

Si dispone di una macchina virtuale di storage (SVM) con quote applicate e si desidera apportare modifiche che richiedono una reinizializzazione completa delle quote.

### Fasi

1. Utilizzare `vserver show` con il `-instance` Parametro per determinare il nome del criterio attualmente assegnato a SVM.
2. Modificare le regole di quota eseguendo una delle seguenti operazioni:

Se si desidera...	Quindi...
Creare nuove regole di quota	Utilizzare <code>volume quota policy rule create</code> comando
Modificare le impostazioni delle regole di quota esistenti	Utilizzare <code>volume quota policy rule modify</code> comando
Eliminare le regole di quota esistenti	Utilizzare <code>volume quota policy rule delete</code> comando

3. Utilizzare `volume quota policy rule show` per verificare che le regole di quota siano configurate correttamente.
4. Reinizializzare le quote su ciascun volume in cui sono state modificate le quote disattivando le quote e attivando le quote per tali volumi.
  - a. Utilizzare `volume quota off` su ciascun volume interessato per disattivare le quote su tale volume.
  - b. Utilizzare `volume quota on` su ciascun volume interessato per attivare le quote su tale volume.



È necessario attendere circa cinque minuti prima di riattivare le quote su ciascun volume interessato, in quanto si tenta di attivarle quasi immediatamente dopo l'esecuzione di `volume quota off` il comando potrebbe causare errori.

In alternativa, è possibile eseguire i comandi per reinizializzare le quote per un volume dal nodo che contiene il volume specifico.

È possibile monitorare il processo di inizializzazione in uno dei seguenti modi:

- Quando si utilizza `volume quota on` è possibile aggiungere il comando `-foreground` parametro per eseguire la quota sul lavoro in primo piano. (Per impostazione predefinita, il processo viene eseguito in background).

Quando il lavoro viene eseguito in background, è possibile monitorarne l'avanzamento utilizzando `job show` comando.

- È possibile utilizzare `volume quota show` per monitorare lo stato dell'inizializzazione della quota.

5. Utilizzare `volume quota show -instance` comando per verificare la presenza di errori di inizializzazione, come ad esempio le regole di quota che non sono riuscite a inizializzare.

6. Utilizzare `volume quota report` per visualizzare un report delle quote in modo da garantire che le quote applicate corrispondano alle aspettative.

### Comandi per gestire le regole di quota e le policy di quota

È possibile utilizzare `volume quota policy rule` comandi per configurare le regole di quota e utilizzare `volume quota policy` e alcuni `vserver` comandi per configurare i criteri di quota.



È possibile eseguire i seguenti comandi solo sui volumi FlexVol.

#### Comandi per la gestione delle regole di quota

Se si desidera...	Utilizzare questo comando...
Creare una nuova regola di quota	<code>volume quota policy rule create</code>
Eliminare una regola di quota esistente	<code>volume quota policy rule delete</code>
Modificare una regola di quota esistente	<code>volume quota policy rule modify</code>
Visualizza informazioni sulle regole di quota configurate	<code>volume quota policy rule show</code>

#### Comandi per la gestione dei criteri di quota

Se si desidera...	Utilizzare questo comando...
Duplicare un criterio di quota e le regole di quota in esso contenute	<code>volume quota policy copy</code>
Creare un nuovo criterio di quota vuoto	<code>volume quota policy create</code>
Eliminazione di un criterio di quota esistente non assegnato a una macchina virtuale di storage (SVM)	<code>volume quota policy delete</code>
Rinominare un criterio di quota	<code>volume quota policy rename</code>
Visualizza informazioni sui criteri di quota	<code>volume quota policy show</code>
Assegnare un criterio di quota a una SVM	<code>vserver modify -quota-policy <i>policy_name</i></code>

Se si desidera...	Utilizzare questo comando...
Visualizza il nome del criterio di quota assegnato a una SVM	<code>vserver show</code>

Vedere ["Riferimento al comando ONTAP"](#) per ogni comando per ulteriori informazioni.

### Comandi per attivare e modificare le quote

È possibile utilizzare `volume quota` comandi per modificare lo stato delle quote e configurare la registrazione dei messaggi delle quote.

Se si desidera...	Utilizzare questo comando...
Attivare le quote (dette anche <i>inizializzazione</i> )	<code>volume quota on</code>
Ridimensionare le quote esistenti	<code>volume quota resize</code>
Disattivare le quote	<code>volume quota off</code>
Modificare la registrazione dei messaggi delle quote, attivare le quote, disattivare le quote o ridimensionare le quote esistenti	<code>volume quota modify</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Utilizza la deduplica, la compressione dei dati e la compattazione dei dati per aumentare l'efficienza dello storage

**Utilizza la deduplica, la compressione dei dati e la compattazione dei dati per migliorare la panoramica dell'efficienza dello storage**

È possibile eseguire la deduplica, la compressione dei dati e la compattazione dei dati insieme o in modo indipendente per ottenere risparmi di spazio ottimali su un volume FlexVol. La deduplica elimina i blocchi di dati duplicati. La compressione dei dati comprime i blocchi di dati per ridurre la quantità di storage fisico richiesta. La compattazione dei dati memorizza più dati in meno spazio per aumentare l'efficienza dello storage.



A partire da ONTAP 9.2, tutte le funzionalità di efficienza dello storage inline, come la deduplica inline e la compressione inline, sono attivate per impostazione predefinita sui volumi AFF.

### Abilitare la deduplica su un volume

È possibile attivare la deduplica su un volume FlexVol per ottenere l'efficienza dello storage. È possibile attivare la deduplica post-processo su tutti i volumi e la deduplica inline su volumi che risiedono su aggregati AFF o Flash Pool.

Se si desidera attivare la deduplica inline su altri tipi di volumi, consultare l'articolo della Knowledge base ["Come attivare la deduplica inline del volume su aggregati non AFF \(All Flash FAS\)"](#).

### Di cosa hai bisogno

Per un volume FlexVol, è necessario aver verificato che esiste spazio libero sufficiente per i metadati di deduplica in volumi e aggregati. I metadati di deduplica richiedono una quantità minima di spazio libero nell'aggregato. Questa quantità è pari al 3% della quantità totale di dati fisici per tutti i volumi FlexVol deduplicati o i componenti dei dati all'interno dell'aggregato. Ogni volume o componente di dati FlexVol deve avere il 4% della quantità totale di dati fisici di spazio libero, per un totale del 7%.



A partire da ONTAP 9.2, la deduplica inline è attivata per impostazione predefinita sui sistemi AFF.

### Scelte

- Utilizzare `volume efficiency on` per attivare la deduplica post-processo.

Il seguente comando abilita la deduplica post-elaborazione sul volume VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```

- Utilizzare `volume efficiency on` seguito dal comando `volume efficiency modify` con il `-inline-deduplication` opzione impostata su `true` per abilitare la deduplica post-processo e la deduplica inline.

I seguenti comandi consentono la deduplica post-processo e la deduplica inline sul volume VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -inline-dedupe true
```

- Utilizzare `volume efficiency on` seguito dal comando `volume efficiency modify` con il `-inline-deduplication` opzione impostata su `true` e a. `-policy` opzione impostata su `inline-only` per attivare solo la deduplica inline.

I seguenti comandi consentono solo la deduplica inline sul volume VolA:

```
volume efficiency on -vserver vs1 -volume VolA
```

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only -inline-dedupe true
```

### Al termine

Verificare che l'impostazione sia stata modificata visualizzando le impostazioni di efficienza del volume:

```
volume efficiency show -instance
```

### Disattivare la deduplica su un volume

È possibile disattivare la deduplica post-processo e la deduplica inline in modo indipendente su un volume.

### Di cosa hai bisogno

Interrompere qualsiasi operazione di efficienza del volume attualmente attiva sul volume: `volume efficiency stop`

### A proposito di questa attività

Se è stata attivata la compressione dei dati sul volume, eseguire `volume efficiency off` il comando disattiva la compressione dei dati.

### Scelte

- Utilizzare `volume efficiency off` comando per disattivare la deduplica post-processo e la deduplica inline.

Il seguente comando disattiva sia la deduplica post-processo che la deduplica inline sul volume Vola:

```
volume efficiency off -vserver vs1 -volume VolA
```

- Utilizzare `volume efficiency modify` con il `-policy` opzione impostata su `inline only` per disattivare la deduplica post-processo, ma la deduplica inline rimane attivata.

Il seguente comando disattiva la deduplica post-processo, ma la deduplica inline rimane attivata sul volume Vola:

```
volume efficiency modify -vserver vs1 -volume VolA -policy inline-only
```

- Utilizzare `volume efficiency modify` con il `-inline-deduplication` opzione impostata su `false` per disattivare solo la deduplica inline.

Il seguente comando disattiva solo la deduplica inline sul volume Vola:

```
volume efficiency modify -vserver vs1 -volume VolA -inline-deduplication false
```

### Gestire la deduplica automatica in background a livello di volume sui sistemi AFF

A partire da ONTAP 9.3, la deduplica in background a livello di volume può essere gestita per essere eseguita automaticamente utilizzando un predefinito `auto` Policy AFF. Non è richiesta alcuna configurazione manuale delle pianificazioni. Il `auto policy` esegue la deduplica continua in background.

Il `auto` la policy viene impostata per tutti i volumi appena creati e per tutti i volumi aggiornati che non sono stati configurati manualmente per la deduplica in background. È possibile modificare il criterio in `default` o qualsiasi altro criterio per disattivare la funzione.

Se un volume si sposta da un sistema non AFF a un sistema AFF, l' `auto` il criterio è attivato per impostazione predefinita nel nodo di destinazione. Se un volume si sposta da un nodo AFF a un nodo non AFF, il `auto` il criterio sul nodo di destinazione viene sostituito da `inline-only policy` per impostazione predefinita.

Su AFF, il sistema monitora tutti i volumi con `auto policy` e deprioritizza il volume che ha meno risparmi o sovrascritture frequenti. I volumi sordinati non partecipano più alla deduplica automatica in background. La registrazione delle modifiche sui volumi con priorità disattivata viene disattivata e i metadati sul volume vengono troncati.

Gli utenti possono promuovere il volume sassegnato dalla priorità per partecipare nuovamente a una deduplica automatica in background utilizzando `volume efficiency promote` comando disponibile a livello di



privilegio avanzato.

## Gestione della deduplica inline a livello aggregato sui sistemi AFF

La deduplica a livello di aggregato elimina i blocchi duplicati nei volumi appartenenti allo stesso aggregato. A partire da ONTAP 9.2, è possibile eseguire la deduplica a livello aggregato inline sui sistemi AFF. La funzione è attivata per impostazione predefinita per tutti i volumi appena creati e tutti i volumi aggiornati con la deduplica inline del volume attivata.

### A proposito di questa attività

L'operazione di deduplica elimina i blocchi duplicati prima che i dati vengano scritti su disco. Solo i volumi con `space guarantee` impostare su `none` può partecipare alla deduplica inline a livello di aggregato. Questa è l'impostazione predefinita sui sistemi AFF.



La deduplica inline a livello di aggregato viene talvolta definita deduplica inline tra volumi diversi.

### Fase

1. Gestire la deduplica inline a livello aggregato sui sistemi AFF:

Se si desidera...	Utilizzare questo comando
Consente la deduplica inline a livello di aggregato	<code>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe true</code>
Disattiva la deduplica inline a livello di aggregato	<code>volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe false</code>
Visualizzare lo stato della deduplica inline a livello di aggregato	<code>volume efficiency config -volume vol_name</code>

### Esempi

Il seguente comando visualizza lo stato della deduplica inline a livello di aggregato:

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver:                                vs0
Volume:                                choke0_wfit_8020_03_0
Schedule:                               -
Policy:                                 choke_VE_policy
Compression:                            true
Inline Compression:                      true
Inline Dedupe:                           true
Data Compaction:                         true
Cross Volume Inline Deduplication:       false
```

### Gestire la deduplica in background a livello aggregato sui sistemi AFF

La deduplica a livello di aggregato elimina i blocchi duplicati nei volumi appartenenti allo stesso aggregato. A partire da ONTAP 9.3, è possibile eseguire la deduplica a livello aggregato in background sui sistemi AFF. La funzione è attivata per impostazione predefinita per tutti i volumi appena creati e tutti i volumi aggiornati con la deduplica in background del volume attivata.

#### A proposito di questa attività

L'operazione viene attivata automaticamente quando viene compilata una percentuale sufficiente del registro delle modifiche. Nessuna pianificazione o policy è associata all'operazione.

A partire da ONTAP 9.4, gli utenti di AFF possono anche eseguire lo scanner di deduplica a livello aggregato per eliminare i duplicati dei dati esistenti nei volumi dell'aggregato. È possibile utilizzare `storage aggregate efficiency cross-volume-dedupe start` con il `-scan-old-data=true` opzione per avviare lo scanner:

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

La scansione della deduplica può richiedere molto tempo. Potrebbe essere necessario eseguire l'operazione in ore non di punta.



La deduplica in background a livello di aggregato viene talvolta definita deduplica in background tra volumi.

#### Fase

- 1. Gestire la deduplica in background a livello aggregato sui sistemi AFF:

Se si desidera...	Utilizzare questo comando
Abilitare la deduplica in background a livello aggregato	<code>volume efficiency modify -vserver &lt;vserver_name&gt; -volume &lt;vol_name&gt; -cross-volume-background-dedupe true</code>
Disattiva la deduplica in background a livello di aggregato	<code>volume efficiency modify -vserver &lt;vserver_name&gt; -volume &lt;vol_name&gt; -cross-volume-background-dedupe false</code>
Visualizzare lo stato della deduplica di background a livello aggregato	<code>aggregate efficiency cross-volume-dedupe show</code>

### Panoramica dell'efficienza dello storage sensibile alla temperatura

ONTAP offre vantaggi in termini di efficienza dello storage sensibili alla temperatura, valutando la frequenza di accesso ai dati del volume e mappando tale frequenza al grado di compressione applicato a tali dati. Per i dati cold a cui si accede raramente, i blocchi di

dati più grandi vengono compressi, mentre per i dati hot, a cui si accede frequentemente e che vengono sovrascritti più spesso, i blocchi di dati più piccoli vengono compressi, rendendo il processo più efficiente.

L'efficienza dello storage sensibile alla temperatura (TSSE) viene introdotta in ONTAP 9.8 e attivata automaticamente sui volumi AFF appena creati con thin provisioning. È possibile abilitare l'efficienza dello storage sensibile alla temperatura sui volumi AFF esistenti e sui volumi DP non AFF con thin provisioning.

### **Introduzione delle modalità "predefinite" ed "efficienti"**

A partire da ONTAP 9.10.1, sono state introdotte due modalità di efficienza dello storage a livello di volume solo per i sistemi AFF, *default* e *Efficient*. Le due modalità consentono di scegliere tra la compressione file (predefinita), che è la modalità predefinita per la creazione di nuovi volumi AFF, o l'efficienza dello storage sensibile alla temperatura (efficiente), che consente l'efficienza dello storage sensibile alla temperatura. Con ONTAP 9.10.1, ["l'efficienza dello storage sensibile alla temperatura deve essere impostata in modo esplicito"](#) per attivare la compressione adattativa automatica. Tuttavia, altre funzionalità di efficienza dello storage, come la compattazione dei dati, la pianificazione della deduplica automatica, la deduplica inline, la deduplica inline tra volumi e la deduplica in background tra volumi, sono attivate per impostazione predefinita sulle piattaforme AFF sia per le modalità predefinite che per quelle efficienti.

Entrambe le modalità di efficienza dello storage (predefinite ed efficienti) sono supportate negli aggregati abilitati per FabricPool e con tutti i tipi di policy di tiering.

### **Efficienza dello storage sensibile alla temperatura abilitata sulle piattaforme C-Series**

L'efficienza dello storage sensibile alla temperatura è attivata per impostazione predefinita sulle piattaforme AFF C-Series e durante la migrazione dei volumi da una piattaforma non TSSE a una piattaforma C-Series abilitata a TSSE utilizzando lo spostamento del volume o SnapMirror con le seguenti release installate sulla destinazione:

- ONTAP 9.12.1P4 e versioni successive
- ONTAP 9.13.1 e versioni successive

Per ulteriori informazioni, vedere ["Comportamento in termini di efficienza dello storage con lo spostamento dei volumi e le operazioni SnapMirror"](#).

Tuttavia, per i volumi esistenti, l'efficienza dello storage sensibile alla temperatura non viene attivata automaticamente ["modificare la modalità di efficienza dello storage"](#) manualmente per passare alla modalità efficiente.



Una volta impostata la modalità di efficienza dello storage su efficiente, non sarà più possibile modificarla.

### **Efficienza dello storage migliorata grazie al confezionamento sequenziale di blocchi fisici contigui**

A partire da ONTAP 9.13.1, l'efficienza dello storage sensibile alla temperatura aggiunge un impacchettamento sequenziale di blocchi fisici contigui per migliorare ulteriormente l'efficienza dello storage. I volumi con efficienza dello storage sensibile alla temperatura attivata dispongono automaticamente del packing sequenziale attivato quando si aggiornano i sistemi a ONTAP 9.13.1. Una volta attivato il packing sequenziale, è necessario ["reimballare manualmente i dati esistenti"](#).

### **Considerazioni sull'upgrade**

Quando si esegue l'aggiornamento a ONTAP 9.10.1 e versioni successive, ai volumi esistenti viene assegnata una modalità di efficienza dello storage basata sul tipo di compressione attualmente attivata sui volumi. Durante un aggiornamento, ai volumi con compressione attivata viene assegnata la modalità predefinita e ai

volumi con efficienza dello storage sensibile alla temperatura attivata viene assegnata la modalità efficiente. Se la compressione non è attivata, la modalità di efficienza dello storage rimane vuota.

### Comportamento in termini di efficienza dello storage con lo spostamento dei volumi e le operazioni SnapMirror

Il modo in cui l'efficienza dello storage si comporta su un volume quando si esegue un'operazione di spostamento del volume o SnapMirror e ciò che accade quando si esegue un'interruzione di SnapMirror e si attiva manualmente l'efficienza dello storage sensibile alla temperatura dipende dal tipo di efficienza sul volume di origine.

La seguente tabella descrive il comportamento di un volume di origine e di un volume di destinazione quando si esegue uno spostamento del volume o un'operazione SnapMirror con diversi tipi di efficienza dello storage, nonché il comportamento quando si attiva manualmente l'efficienza dello storage sensibile alla temperatura (TSSE).

Efficienza del volume di origine	Comportamento predefinito del volume di destinazione			Comportamento predefinito dopo l'attivazione manuale di TSSE (dopo l'interruzione di SnapMirror)		
	Tipo di efficienza dello storage	Nuove scritture	Compressione dati a freddo	Tipo di efficienza dello storage	Nuove scritture	Compressione dati a freddo
Nessuna efficienza dello storage (probabile FAS)	Compressione del file	La compressione del file viene tentata inline sui dati appena scritti	Nessuna compressione dei dati a freddo, i dati rimangono così come sono	TSSE con algoritmo cold data scan come ZSTD	viene tentata la compressione inline 8k in formato TSSE	<b>File dati compressi:</b> N/A.  <b>Dati non compressi:</b> Tentativo di compressione di 32K dopo il raggiungimento dei giorni di soglia  <b>Dati appena scritti:</b> Tentativo di compressione di 32K dopo il raggiungimento dei giorni di soglia
Nessuna efficienza dello storage (probabile FAS)	Compressione dei file su piattaforme e C-Series che utilizzano ONTAP 9.11.1P10 o ONTAP 9.12.1P3	Nessuna compressione dati Cold abilitata per TSSE	<b>File dati compressi:</b> N/A.	TSSE con algoritmo cold data scan come ZSTD	Compressione inline 8K	<b>File dati compressi:</b> N/A.  <b>Dati non compressi:</b> Tentativo di compressione di 32K dopo il raggiungimento dei giorni di soglia  <b>Dati appena scritti:</b> Tentativo di compressione di 32K dopo il raggiungimento dei giorni di soglia

Nessuna efficienza dello storage (probabile FAS)	TSSE su piattaforme e C-Series che utilizzano ONTAP 9.12.1P4 e versioni successive o ONTAP 9.13.1 e versioni successive	Viene tentata la compressione inline 8K in formato TSSE	<b>File dati compressi:</b> N/A.  <b>Dati non compressi:</b> Tentativo di compressione di 32K dopo il raggiungimento dei giorni di soglia  <b>Dati appena scritti:</b> Tentativo di compressione di 32K dopo il raggiungimento dei giorni di soglia	TSSE con algoritmo cold data scan come ZSTD	Viene tentata la compressione inline 8K in formato TSSE	<b>File dati compressi:</b> N/A.  <b>Dati non compressi:</b> Tentativo di compressione di 32K dopo il raggiungimento dei giorni di soglia  <b>Dati appena scritti:</b> Tentativo di compressione di 32K dopo il raggiungimento dei giorni di soglia
Gruppo di compressione del file	Uguale all'origine	La compressione del file viene tentata inline sui dati appena scritti	Nessuna compressione dei dati a freddo, i dati rimangono così come sono	TSSE con algoritmo cold data scan come ZSTD	viene tentata la compressione inline 8k in formato TSSE	<b>File dati compressi:</b> Non compressi  <b>Dati non compressi:</b> Viene tentata una compressione di 32K dopo che sono stati raggiunti i giorni di soglia  <b>Dati appena scritti:</b> Viene tentata una compressione di 32K dopo il raggiungimento della soglia dei giorni
Scansione dei dati TSSE cold	TSSE che utilizza lo stesso algoritmo di compressione del volume di origine (LZOPro→LZOPro e ZSTD→ZSTD)	Tentativo di compressione inline 8K in formato TSSE	Tentativo di compressione di 32K con LzoPro dopo il raggiungimento di un livello di freddo basato su giorni di soglia sia sui dati esistenti che sui dati appena scritti.	TSSE è attivato. NOTA: L'algoritmo di scansione dei dati cold LZOPro può essere modificato in ZSTD.	Viene tentata la compressione inline 8K in formato TSSE	Viene tentata una compressione di 32K dopo che la temperatura dei giorni di soglia è stata soddisfatta sia sui dati esistenti che sui dati appena scritti.

### Impostare la modalità di efficienza dello storage durante la creazione del volume

A partire da ONTAP 9.10.1, è possibile impostare la modalità di efficienza dello storage quando si crea un nuovo volume AFF. Utilizzando il parametro `-storage-efficiency-mode`, è possibile specificare se il volume utilizza la modalità efficient o la modalità performance predefinita. Le due modalità consentono di scegliere tra la compressione file (predefinita), ovvero la modalità predefinita quando vengono creati nuovi volumi AFF, o l'efficienza dello storage sensibile alla temperatura (efficiente), che consente l'efficienza


dello storage sensibile alla temperatura. Il `-storage-efficiency-mode` Il parametro non è supportato su volumi non AFF o su volumi di protezione dei dati.

## Fasi

È possibile eseguire questa attività utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

### System Manager

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per aumentare l'efficienza dello storage utilizzando la funzione di efficienza dello storage sensibile alla temperatura. L'efficienza dello storage basata sulle performance è attivata per impostazione predefinita.

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Individuare il volume su cui si desidera attivare o disattivare l'efficienza dello storage e fare clic su .
3. Fare clic su **Modifica > volumi** e scorrere fino a **efficienza archiviazione**.
4. Selezionare **Enable Higher Storage Efficiency** (attiva efficienza dello storage superiore)

### CLI

#### Creare un nuovo volume utilizzando la modalità efficiente

Per impostare la modalità di efficienza dello storage sensibile alla temperatura durante la creazione di un nuovo volume, è possibile utilizzare `-storage-efficiency-mode` con il valore `efficient`.

1. Creare un nuovo volume con la modalità di efficienza attivata:

```
volume create -vserver <vserver name> -volume <volume name> -aggregate  
<aggregate name> -size <volume size> -storage-efficiency-mode efficient
```

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1  
-storage-efficiency-mode efficient -size 10g
```

#### Creare un nuovo volume utilizzando la modalità performance

La modalità performance viene impostata per impostazione predefinita quando si creano nuovi volumi AFF con efficienza dello storage. Sebbene non sia necessario, è possibile utilizzare facoltativamente il default valore con `-storage-efficiency-mode` Quando si crea un nuovo volume AFF.

1. Creare un nuovo volume utilizzando la modalità di efficienza dello storage per le performance, "default":

```
volume create -vserver <vserver name> -volume <volume name> -aggregate  
<aggregate name> -size <volume size> -storage-efficiency-mode default
```

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1 -storage  
-efficiency-mode default -size 10g
```

## Modificare la soglia di compressione dei dati inattivi del volume

È possibile modificare la frequenza con cui ONTAP esegue una scansione dei dati a

freddo modificando la soglia di freddo sui volumi utilizzando l'efficienza dello storage sensibile alla temperatura.

### Prima di iniziare

È necessario essere un amministratore di cluster o SVM e utilizzare il livello di privilegio avanzato CLI di ONTAP.

### A proposito di questa attività

La soglia di freddo può essere compresa tra 1 e 60 giorni. La soglia predefinita è 14 giorni.

### Fasi

1. Impostare il livello di privilegio:

```
set -privilege advanced
```

2. Modificare la compressione dei dati inattivi su un volume:

```
volume efficiency inactive-data-compression modify -vserver <vserver_name>  
-volume <volume_name> -threshold-days <integer>
```

Per ulteriori informazioni su, consulta la pagina man ["modifica della compressione dei dati inattivi"](#).

### Controllare la modalità di efficienza del volume

È possibile utilizzare `volume-efficiency-show` Comando su un volume AFF per verificare se l'efficienza è impostata e per visualizzare la modalità di efficienza corrente.

### Fase

1. Controllare la modalità di efficienza su un volume:

```
volume efficiency show -vserver <vserver name> -volume <volume name> -fields  
storage-efficiency-mode
```

### Modificare la modalità di efficienza del volume

A partire da ONTAP 9.10.1, sono state introdotte due modalità di efficienza dello storage a livello di volume solo per i sistemi AFF, *default* e *Efficient*. Le due modalità consentono di scegliere tra la compressione file (predefinita), che è la modalità predefinita per la creazione di nuovi volumi AFF, o l'efficienza dello storage sensibile alla temperatura (efficiente), che consente l'efficienza dello storage sensibile alla temperatura. È possibile utilizzare `volume efficiency modify` Comando per modificare la modalità di efficienza dello storage impostata su un volume AFF. È possibile modificare la modalità da *default* a *efficient* in alternativa, è possibile impostare una modalità di efficienza quando l'efficienza del volume non è già impostata.

### Fasi

1. Modificare la modalità di efficienza del volume:

```
volume efficiency modify -vserver <vserver name> -volume <volume name>
```

```
-storage-efficiency-mode <default|efficient>
```

## Riduzione dell'impatto dei volumi con o senza efficienza dello storage sensibile alla temperatura

A partire da ONTAP 9.11.1, è possibile utilizzare `volume show-footprint` comando per visualizzare i risparmi di impatto fisico sui volumi "Grazie all'efficienza dello storage sensibile alla temperatura (TSSE)". A partire da ONTAP 9.13.1, è possibile utilizzare lo stesso comando per visualizzare i risparmi di impatto fisico sui volumi non abilitati con TSSE.

### Fase

1. Scopri i risparmi sull'impatto dei volumi:

```
volume show-footprint
```

### Esempio di output con TSSE attivato

```
Vserver : vs0
Volume  : vol_tsse_75_per_compress
```

Feature	Used	Used%
-----	-----	-----
Volume Data Footprint	10.15GB	13%
Volume Guarantee	0B	0%
Flexible Volume Metadata	64.25MB	0%
Delayed Frees	235.0MB	0%
File Operation Metadata	4KB	0%
 Total Footprint	 10.45GB	 13%
 Footprint Data Reduction	 6.85GB	 9%
Auto Adaptive Compression	6.85GB	9%
Effective Total Footprint	3.59GB	5%



## Output di esempio senza TSSE abilitato

```
Vserver : vs0
Volume  : vol_file_cg_75_per_compress

Feature                                Used      Used%
-----
Volume Data Footprint                  5.19GB     7%
Volume Guarantee                       0B         0%
Flexible Volume Metadata               32.12MB    0%
Delayed Frees                          90.17MB    0%
File Operation Metadata                 4KB        0%

Total Footprint                        5.31GB     7%

Footprint Data Reduction                1.05GB     1%
    Data Compaction                    1.05GB     1%
Effective Total Footprint               4.26GB     5%
```

## Abilitare la compressione dei dati su un volume

È possibile attivare la compressione dei dati su un volume FlexVol per ottenere risparmi di spazio utilizzando `volume efficiency modify` comando. È inoltre possibile assegnare un tipo di compressione al volume, se non si desidera utilizzare il tipo di compressione predefinito.

### Di cosa hai bisogno

È necessario aver attivato la deduplica sul volume.



- La deduplica deve essere abilitata e non deve essere eseguita sul volume.
- Lo scanner di compressione deve essere utilizzato per comprimere i dati esistenti sui volumi presenti nelle piattaforme AFF.

### "Attivazione della deduplica su un volume"

#### A proposito di questa attività

- Negli aggregati HDD e Flash Pool, è possibile attivare la compressione inline e post-process o solo la compressione post-process su un volume.

Se si abilitano entrambi, è necessario attivare la compressione post-elaborazione sul volume prima di attivare la compressione inline.

- Nelle piattaforme AFF, è supportata solo la compressione inline.

Prima di attivare la compressione inline, è necessario attivare la compressione post-elaborazione sul volume. Tuttavia, poiché la compressione post-processo non è supportata nelle piattaforme AFF, non viene eseguita alcuna compressione post-processo su tali volumi e viene generato un messaggio EMS che informa che la compressione post-processo è stata saltata.

- L'efficienza dello storage sensibile alla temperatura è stata introdotta in ONTAP 9.8. Con questa funzione, l'efficienza dello storage viene applicata in base al fatto che i dati siano caldi o freddi. Per i dati cold, vengono compressi blocchi di dati più grandi e per i dati hot, che vengono sovrascritti più spesso, vengono compressi blocchi di dati più piccoli, rendendo il processo più efficiente. L'efficienza dello storage sensibile alla temperatura viene attivata automaticamente sui volumi AFF appena creati con thin provisioning.
- Il tipo di compressione viene assegnato automaticamente in base alla piattaforma dell'aggregato:

Piattaforma/aggregati	Tipo di compressione
AFF	Compressione adattiva
Aggregati di Flash Pool	Compressione adattiva
Aggregati di HDD	Compressione secondaria

## Scelte

- Utilizzare `volume efficiency modify` per attivare la compressione dei dati con il tipo di compressione predefinito.

Il seguente comando abilita la compressione post-elaborazione sul volume VolA di SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
```

Il seguente comando abilita sia la compressione post-processo che quella inline sul volume VolA di SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true -inline  
-compression true
```

- Utilizzare `volume efficiency modify` al livello di privilegio avanzato per abilitare la compressione dei dati con un tipo di compressione specifico.
  - a. Utilizzare `set -privilege advanced` per impostare il livello di privilegio su avanzato.
  - b. Utilizzare `volume efficiency modify` comando per assegnare un tipo di compressione a un volume.

Il seguente comando abilita la compressione post-elaborazione e assegna il tipo di compressione adattativa al volume VolA di SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true  
-compression-type adaptive
```

Il seguente comando abilita sia la compressione post-processo che quella inline e assegna il tipo di compressione adattiva al volume VolA di SVM vs1:

```
volume efficiency modify -vserver vs1 -volume VolA -compression true  
-compression-type adaptive -inline-compression true
```

- a. Utilizzare `set -privilege admin` per modificare il livello di privilegio in admin.

## Passare dalla compressione secondaria alla compressione adattativa

È possibile passare dalla compressione secondaria alla compressione adattativa in base alla quantità di dati letti. La compressione adattativa è preferibile quando il sistema è dotato di un elevato volume di letture casuali e sono richieste prestazioni più elevate. La compressione secondaria è preferibile quando i dati vengono scritti in sequenza e sono richiesti risparmi di compressione più elevati.

### A proposito di questa attività

Il tipo di compressione predefinito viene selezionato in base agli aggregati e alla piattaforma.

### Fasi

1. Disattivare la compressione dei dati sul volume:

```
volume efficiency modify
```

Il seguente comando disattiva la compressione dei dati sul volume vol1:

```
volume efficiency modify -compression false -inline-compression false -volume vol1
```

2. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

3. Decomprimere i dati compressi:

```
volume efficiency undo
```

Il seguente comando decompresse i dati compressi sul volume vol1:

```
volume efficiency undo -vserver vs1 -volume vol1 -compression true
```



È necessario verificare di disporre di spazio sufficiente nel volume per ospitare i dati decompressi.

4. Verificare che lo stato dell'operazione sia inattivo:

```
volume efficiency show
```

Il seguente comando visualizza lo stato di un'operazione di efficienza sul volume vol1:

```
volume efficiency show -vserver vs1 -volume vol1
```

5. Attivare la compressione dei dati, quindi impostare il tipo di compressione:

```
volume efficiency modify
```

Il seguente comando abilita la compressione dei dati e imposta il tipo di compressione come compressione secondaria sul volume vol1:

```
volume efficiency modify -vserver vs1 -volume vol1 -compression true
```

`-compression-type secondary`



Questa fase attiva solo la compressione secondaria sul volume; i dati sul volume non vengono compressi.

- Per comprimere i dati esistenti sui sistemi AFF, è necessario eseguire lo scanner di compressione in background.
- Per comprimere i dati esistenti su aggregati di Flash Pool o HDD, è necessario eseguire la compressione in background.

6. Passare al livello di privilegio admin:

```
set -privilege admin
```

7. Opzionale: Abilitare la compressione inline:

```
volume efficiency modify
```

Il seguente comando abilita la compressione inline sul volume vol1:

```
volume efficiency modify -vserver vs1 -volume vol1 -inline-compression true
```

## Disattiva la compressione dei dati su un volume

È possibile disattivare la compressione dei dati su un volume utilizzando `volume efficiency modify` comando.

### A proposito di questa attività

Se si desidera disattivare la compressione post-elaborazione, è necessario prima disattivare la compressione inline sul volume.

### Fasi

1. Interrompere qualsiasi operazione di efficienza del volume attualmente attiva sul volume:

```
volume efficiency stop
```

2. Disattivare la compressione dei dati:

```
volume efficiency modify
```

I dati compressi esistenti rimarranno compressi sul volume. Solo le nuove scritture che arrivano nel volume non vengono compresse.

### Esempi

Il seguente comando disattiva la compressione inline sul volume Vola:

```
volume efficiency modify -vserver vs1 -volume VolA -inline-compression false
```

Il seguente comando disattiva sia la compressione post-processo che la compressione inline sul volume Vola:

```
volume efficiency modify -vserver vs1 -volume VolA -compression false -inline
```

```
-compression false
```

## Gestire la compattazione dei dati inline per i sistemi AFF

È possibile controllare la compattazione dei dati inline sui sistemi AFF a livello di volume utilizzando `volume efficiency modify` comando. La compattazione dei dati è attivata per impostazione predefinita per tutti i volumi sui sistemi AFF.

### Di cosa hai bisogno

La compattazione dei dati richiede che la garanzia di spazio del volume sia impostata su `none`. Questa è l'impostazione predefinita per i sistemi AFF.



La garanzia di spazio predefinita per i volumi di protezione dei dati non AFF è impostata su `NONE`.

### Fasi

1. Per verificare l'impostazione della garanzia di spazio per il volume:

```
volume show -vserver vs1 -volume vol1 -fields space-guarantee
```

2. Per consentire la compaction dei dati:

```
volume efficiency modify -vserver vs1 -volume vol1 -data  
-compaction true
```

3. Per disattivare la compattazione dei dati:

```
volume efficiency modify -vserver vs1 -volume vol1 -data  
-compaction false
```

4. Per visualizzare lo stato di compattazione dei dati:

```
volume efficiency show -instance
```

### Esempi

```
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data-compaction  
true cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data  
-compaction false
```

## Consentire la compaction dei dati inline per i sistemi FAS

È possibile controllare la compattazione dei dati inline sui sistemi FAS con aggregati di Flash Pool (ibridi) o HDD a livello di volume o aggregato utilizzando `volume efficiency` comando della shell del cluster. La compattazione dei dati è disattivata per impostazione predefinita per i sistemi FAS.

### A proposito di questa attività

Se si abilita la compaction dei dati a livello di aggregato, la compaction dei dati viene attivata su qualsiasi nuovo volume creato con una garanzia di spazio del volume di `none` nell'aggregato. L'abilitazione della compaction dei dati su un volume su un aggregato HDD utilizza risorse CPU aggiuntive.

## Fasi

1. Passare al livello di privilegio avanzato:  
`set -privilege advanced`
2. Controllare lo stato di compattazione dei dati dei volumi e degli aggregati per il nodo desiderato:  
`volume efficiency show -volume volume_name +`
3. Consentire la compaction dei dati sul volume:  
`volume efficiency modify -volume volume_name -data-compaction true`



Se la compattazione dei dati è impostata su `false` per un aggregato o un volume, la compattazione non riesce. L'abilitazione della compaction non compatta i dati esistenti; solo le nuove scritture nel sistema vengono compattate. Il `volume efficiency start` Command contiene ulteriori informazioni su come comprimere i dati esistenti (in ONTAP 9.1 e versioni successive). [+http://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr/GUID-5CB10C70-AC11-41C0-8C16-B4D0DF916E9B.html](http://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr/GUID-5CB10C70-AC11-41C0-8C16-B4D0DF916E9B.html)["Comandi di ONTAP 9"^]

4. Visualizza le statistiche di compattazione:  
`volume efficiency show -volume volume_name`

## Efficienza dello storage inline attivata per impostazione predefinita sui sistemi AFF

Le funzionalità di efficienza dello storage sono attualmente attivate per impostazione predefinita su tutti i volumi creati di recente sui sistemi AFF. A partire da ONTAP 9.2, tutte le funzionalità di efficienza dello storage inline sono attivate per impostazione predefinita su tutti i volumi esistenti e creati di recente su tutti i sistemi AFF.

Le funzionalità di efficienza dello storage includono deduplica inline, deduplica cross-volume inline e compressione inline e sono attivate per impostazione predefinita sui sistemi AFF, come mostrato nella tabella.



Il comportamento di compattazione dei dati sui volumi AFF non è stato modificato in ONTAP 9.2, poiché è già attivato per impostazione predefinita.

Condizioni di volume	Funzionalità di efficienza dello storage attivate per impostazione predefinita in ONTAP 9.2		
	Deduplica inline	Deduplica cross-volume inline	Compressione inline
Aggiornamento del cluster alla versione 9.2	Sì	Sì	Sì
Transizione da ONTAP 7-Mode a Clustered ONTAP	Sì	Sì	Sì
Spostamento del volume	Sì	Sì	Sì
Volumi con thick provisioning	Sì	No	Sì

Condizioni di volume	Funzionalità di efficienza dello storage attivate per impostazione predefinita in ONTAP 9.2		
Volumi crittografati	Sì	No	Sì

Le seguenti eccezioni si applicano a una o più funzionalità di efficienza dello storage inline:

- Solo i volumi di lettura/scrittura possono supportare l'abilitazione dell'efficienza dello storage inline predefinita.
- L'attivazione della compressione inline non consente di abilitare i volumi con risparmi di compressione.
- I volumi con deduplica post-processo attivata non sono in grado di attivare la compressione inline.
- Nei volumi in cui l'efficienza del volume è disattivata, il sistema esegue l'override delle impostazioni dei criteri di efficienza del volume esistenti e la imposta per attivare la policy di solo inline.

### Consentire la visualizzazione dell'efficienza dello storage

Utilizzare `storage aggregate show-efficiency` comando per visualizzare le informazioni sull'efficienza dello storage di tutti gli aggregati del sistema.

Il `storage aggregate show-efficiency` command dispone di tre viste diverse che possono essere richiamate passando le opzioni dei comandi.

#### Vista predefinita

La vista predefinita visualizza il rapporto complessivo per ciascuno degli aggregati.

```
cluster1::> storage aggregate show-efficiency
```

#### Vista dettagliata

Richiamare la vista dettagliata con `-details` opzione di comando. Questa vista visualizza quanto segue:

- Rapporto di efficienza globale per ciascuno degli aggregati.
- Rapporto complessivo senza copie Snapshot.
- Suddivisione del rapporto per le seguenti tecnologie di efficienza: Deduplica dei volumi, compressione dei volumi, copie Snapshot, cloni, compattazione dei dati, e deduplica in linea aggregata.

```
cluster1::> storage aggregate show-efficiency -details
```

#### Vista avanzata

La vista avanzata è simile alla vista dettagliata e visualizza i dettagli utilizzati sia logici che fisici.

È necessario eseguire questo comando al livello di privilegio avanzato. Passare ai privilegi avanzati utilizzando `set -privilege advanced` comando.

Il prompt dei comandi diventa `cluster::*>`.

```
cluster1::> set -privilege advanced
```

Richiamare la vista avanzata con `-advanced` opzione di comando.

```
cluster1::*> storage aggregate show-efficiency -advanced
```

Per visualizzare i rapporti per un singolo aggregato, richiamare singolarmente `-aggregate aggregate_name` comando. Questo comando può essere eseguito a livello di amministratore, nonché a livello di privilegi avanzati.

```
cluster1::> storage aggregate show-efficiency -aggregate aggr1
```

## Creare una policy di efficienza dei volumi per eseguire operazioni di efficienza

### Creare una policy di efficienza dei volumi per eseguire operazioni di efficienza

È possibile creare una policy di efficienza dei volumi per eseguire la deduplica o la compressione dei dati seguita dalla deduplica su un volume per una durata specifica e specificare la pianificazione dei processi utilizzando `volume efficiency policy create` comando.

#### Prima di iniziare

È necessario aver creato una pianificazione cron utilizzando `job schedule cron create` comando. Per ulteriori informazioni sulla gestione delle pianificazioni cron, vedere ["Riferimento per l'amministrazione del sistema"](#).

#### A proposito di questa attività

Un amministratore SVM con ruoli predefiniti non può gestire le policy di deduplica. Tuttavia, l'amministratore del cluster può modificare i privilegi assegnati a un amministratore SVM utilizzando ruoli personalizzati. Per ulteriori informazioni sulle funzionalità di amministratore di SVM, vedere ["Autenticazione amministratore e RBAC"](#).



È possibile eseguire operazioni di deduplica o compressione dei dati a un orario pianificato, oppure creando una pianificazione con una durata specifica, oppure specificando una percentuale di soglia, che attende che i nuovi dati superino la soglia e quindi attiva l'operazione di deduplica o compressione dei dati. Questo valore di soglia è la percentuale del numero totale di blocchi utilizzati nel volume. Ad esempio, se si imposta il valore di soglia su un volume su 20% quando il numero totale di blocchi utilizzati sul volume è 50%, la deduplica dei dati o la compressione dei dati si attiva automaticamente quando i nuovi dati scritti sul volume raggiungono il 10% (20% dei blocchi utilizzati al 50%). Se necessario, è possibile ottenere il numero totale di blocchi utilizzati da `df` output del comando.

#### Fasi

1. Utilizzare `volume efficiency policy create` per creare una policy di efficienza dei volumi.

#### Esempi

Il seguente comando crea una policy di efficienza del volume denominata `pol1` che attiva un'operazione di efficienza giornaliera:

```
volume efficiency policy create -vserver vs1 -policy pol1 -schedule daily
```

Il seguente comando crea una policy di efficienza del volume denominata `pol2` che attiva un'operazione di efficienza quando la percentuale di soglia raggiunge il 20%:



```
volume efficiency policy create -vserver vs1 -policy pol2 -type threshold -start  
-threshold-percent 20%
```

### Assegnare una policy di efficienza del volume a un volume

È possibile assegnare una policy di efficienza a un volume per eseguire operazioni di deduplica o compressione dei dati utilizzando `volume efficiency modify` comando.

#### A proposito di questa attività

Se un criterio di efficienza viene assegnato a un volume secondario SnapVault, viene preso in considerazione solo l'attributo di priorità di efficienza del volume quando si eseguono operazioni di efficienza del volume. Le pianificazioni dei processi vengono ignorate e l'operazione di deduplica viene eseguita quando vengono effettuati aggiornamenti incrementali al volume secondario SnapVault.

#### Fase

1. Utilizzare `volume efficiency modify` comando per assegnare un criterio a un volume.

#### Esempio

Il seguente comando assegna al volume Vola la policy di efficienza del volume denominata `new_policy`:

```
volume efficiency modify -vserver vs1 -volume VolA -policy new_policy
```

### Modificare una policy di efficienza dei volumi

È possibile modificare una policy di efficienza dei volumi per eseguire la deduplica e la compressione dei dati per una durata diversa o modificare la pianificazione dei processi utilizzando `volume efficiency policy modify` comando.

#### Fase

1. Utilizzare `volume efficiency policy modify` comando per modificare una policy di efficienza dei volumi.

#### Esempi

Il seguente comando modifica la policy di efficienza del volume denominata `policy 1` da eseguire ogni ora:

```
volume efficiency policy modify -vserver vs1 -policy policy1 -schedule hourly
```

Il seguente comando modifica una policy di efficienza del volume denominata `pol2` in `threshold 30%`:

```
volume efficiency policy modify -vserver vs1 -policy pol1 -type threshold -start  
-threshold-percent 30%
```

### Visualizza una policy di efficienza dei volumi

È possibile visualizzare il nome, la pianificazione, la durata e la descrizione della policy di efficienza del volume utilizzando `volume efficiency policy show` comando.

#### A proposito di questa attività

Quando si esegue `volume efficiency policy show` in base all'ambito del cluster, i criteri con ambito del cluster non vengono visualizzati. Tuttavia, è possibile visualizzare i criteri con ambito cluster nel contesto della macchina virtuale di storage (SVM).

## Fase

1. Utilizzare `volume efficiency policy show` comando per visualizzare informazioni su una policy di efficienza dei volumi.

L'output dipende dai parametri specificati. Per ulteriori informazioni sulla visualizzazione della vista dettagliata e di altri parametri, consulta la pagina man di questo comando.

## Esempi

Il seguente comando visualizza le informazioni relative ai criteri creati per SVM vs1: `volume efficiency policy show -vserver vs1`

Il seguente comando visualizza i criteri per i quali la durata è impostata su 10 ore: `volume efficiency policy show -duration 10`

## Disassociare una policy di efficienza dei volumi da un volume

È possibile disassociare una policy di efficienza dei volumi da un volume per interrompere l'esecuzione di ulteriori operazioni di deduplica e compressione dei dati basate su pianificazione sul volume. Una volta disassociata una policy di efficienza dei volumi, è necessario attivarla manualmente.

## Fase

1. Utilizzare `volume efficiency modify` comando per disassociare una policy di efficienza dei volumi da un volume.

## Esempio

Il seguente comando disassocia la policy di efficienza del volume dal volume VolA: `volume efficiency modify -vserver vs1 -volume VolA -policy -`

## Eliminare una policy di efficienza dei volumi

È possibile eliminare una policy di efficienza dei volumi utilizzando `volume efficiency policy delete` comando.

## Di cosa hai bisogno

È necessario assicurarsi che il criterio che si desidera eliminare non sia associato ad alcun volume.



Non è possibile eliminare il *inline-only* e il *default* criterio di efficienza predefinito.

## Fase

1. Utilizzare `volume efficiency policy delete` comando per eliminare una policy di efficienza dei volumi.

## Esempio

Il seguente comando elimina una policy di efficienza dei volumi denominata policy 1: `volume efficiency policy delete -vserver vs1 -policy policy1`

## Gestione manuale delle operazioni di efficienza dei volumi

### Panoramica manuale delle operazioni di gestione dell'efficienza dei volumi

Puoi gestire il modo in cui le operazioni di efficienza vengono eseguite su un volume eseguendo manualmente le operazioni di efficienza.

È inoltre possibile controllare il funzionamento delle operazioni di efficienza in base alle seguenti condizioni:

- Utilizzare i checkpoint o meno
- Eseguire operazioni di efficienza sui dati esistenti o solo sui nuovi dati
- Arrestare le operazioni di efficienza, se necessario

È possibile utilizzare `volume efficiency show` comando con `schedule` come valore per `-fields` per visualizzare la pianificazione assegnata ai volumi.

### Eseguire manualmente le operazioni di efficienza

È possibile eseguire manualmente le operazioni di efficienza su un volume utilizzando `volume efficiency start` comando.

#### Di cosa hai bisogno

A seconda dell'operazione di efficienza che si desidera eseguire manualmente, è necessario aver attivato la deduplica o sia la compressione dei dati che la deduplica su un volume.

#### A proposito di questa attività

Quando l'efficienza dello storage sensibile alla temperatura è abilitata su un volume, la deduplica viene eseguita inizialmente seguita dalla compressione dei dati.

La deduplica è un processo in background che consuma le risorse di sistema mentre è in esecuzione. Se i dati non cambiano spesso in un volume, si consiglia di eseguire la deduplica con minore frequenza. Più operazioni di deduplica simultanee eseguite su un sistema storage comportano un maggiore consumo di risorse di sistema.

È possibile eseguire un massimo di otto operazioni simultanee di deduplica o compressione dei dati per nodo. Se vengono pianificate ulteriori operazioni di efficienza, le operazioni vengono inserite nella coda.

A partire da ONTAP 9.13.1, se l'efficienza dello storage sensibile alla temperatura è abilitata su un volume, è possibile eseguire l'efficienza del volume sui dati esistenti per sfruttare il packing sequenziale per migliorare ulteriormente l'efficienza dello storage.

### Esegui l'efficienza manualmente

#### Fase

1. Avviare l'operazione di efficienza su un volume: `volume efficiency start`

#### Esempio

Il seguente comando consente di avviare manualmente solo la deduplica o la deduplica seguita dalla compressione logica e dalla compressione container sul volume Vola

```
volume efficiency start -vserver vs1 -volume VolA
```

## Reimballare i dati esistenti

Per sfruttare il pacchetto sequenziale di dati introdotto in ONTAP 9.13.1 sui volumi con l'efficienza dello storage sensibile alla temperatura attivata, è possibile reimballare i dati esistenti. Per utilizzare questo comando, è necessario essere in modalità avanzata con privilegi.

### Fase

1. Impostare il livello di privilegio: `set -privilege advanced`
2. Reimballare i dati esistenti: `volume efficiency inactive-data-compression start -vserver vserver_name -volume volume_name -scan-mode extended_recompression`

### Esempio

```
volume efficiency inactive-data-compression start -vserver vs1 -volume  
voll1 -scan-mode extended_recompression
```

## Utilizza i checkpoint per riprendere le operazioni di efficienza

I checkpoint vengono utilizzati internamente per registrare il processo di esecuzione di un'operazione di efficienza. Quando un'operazione di efficienza viene arrestata per qualsiasi motivo (ad esempio, arresto del sistema, interruzione del sistema, riavvio o perché l'ultima operazione di efficienza non è riuscita o è stata arrestata) ed esistono dati del punto di verifica, l'operazione di efficienza può riprendere dall'ultimo file del punto di verifica.

Viene creato un checkpoint:

- in ogni fase o sottostage dell'operazione
- quando si esegue `sis stop` comando
- alla scadenza della durata

## Riprendere un'operazione di efficienza interrotta

Se un'operazione di efficienza viene arrestata a causa di un arresto del sistema, di un'interruzione del sistema o di un riavvio, è possibile riprendere l'operazione di efficienza dallo stesso punto utilizzando `volume efficiency start` comando con l'opzione `checkpoint`. Ciò consente di risparmiare tempo e risorse senza dover riavviare l'operazione di efficienza fin dall'inizio.

## A proposito di questa attività

Se è stata attivata solo la deduplica sul volume, la deduplica viene eseguita sui dati. Se sono state attivate sia la deduplica che la compressione dei dati su un volume, la compressione dei dati viene eseguita per prima, seguita dalla deduplica.

È possibile visualizzare i dettagli del checkpoint di un volume utilizzando `volume efficiency show` comando.

Per impostazione predefinita, le operazioni di efficienza riprendono dai checkpoint. Tuttavia, se un checkpoint corrispondente a un'operazione di efficienza precedente (la fase in cui `volume efficiency start` il comando `-scan-old-data` viene eseguito) ha più di 24 ore, quindi l'operazione di efficienza non riprende automaticamente dal checkpoint precedente. In questo caso, l'operazione di efficienza inizia dall'inizio. Tuttavia, se si sa che non si sono verificate modifiche significative nel volume dall'ultima scansione, è possibile forzare la continuazione dal checkpoint precedente utilizzando `-use-checkpoint` opzione.

## Fase

1. Utilizzare `volume efficiency start` con il `-use-checkpoint` opzione per riprendere un'operazione efficiente.

Il seguente comando consente di riprendere un'operazione di efficienza sui nuovi dati del volume Vola:

```
volume efficiency start -vserver vs1 -volume VolA -use-checkpoint true
```

Il seguente comando consente di riprendere un'operazione di efficienza sui dati esistenti sul volume Vola:

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true -use-checkpoint true
```

## Eeguire manualmente le operazioni di efficienza sui dati esistenti

È possibile eseguire manualmente le operazioni di efficienza sui dati presenti nei volumi di efficienza dello storage non sensibili alla temperatura prima di abilitare la deduplica, la compressione dei dati o la compattazione dei dati con le versioni di ONTAP precedenti a ONTAP 9.8. È possibile eseguire queste operazioni utilizzando `volume efficiency start -scan-old-data` comando.

## A proposito di questa attività

Il `-compression` l'opzione non funziona con `-scan-old-data` sui volumi di efficienza dello storage sensibili alla temperatura. La compressione dei dati inattiva viene eseguita automaticamente sui dati preesistenti per volumi di efficienza dello storage sensibili alla temperatura in ONTAP 9.8 e versioni successive.

Se si attiva solo la deduplica su un volume, la deduplica viene eseguita sui dati. Se si abilitano deduplica, compressione dei dati e compaction dei dati su un volume, la compressione dei dati viene eseguita per prima, seguita da deduplica e compaction dei dati.

Quando si esegue la compressione dei dati sui dati esistenti, per impostazione predefinita l'operazione di compressione dei dati salta i blocchi di dati condivisi dalla deduplica e i blocchi di dati bloccati dalle copie Snapshot. Se si sceglie di eseguire la compressione dei dati su blocchi condivisi, l'ottimizzazione viene disattivata e le informazioni sulle impronte digitali vengono acquisite e riutilizzate per la condivisione. È possibile modificare il comportamento predefinito della compressione dei dati durante la compressione dei dati esistenti.

È possibile eseguire un massimo di otto operazioni di deduplica, compressione dei dati o compattazione dei dati contemporaneamente per nodo. Le operazioni rimanenti vengono inserite nella coda.



La compressione post-processo non viene eseguita sulle piattaforme AFF. Viene generato un messaggio EMS per informare che questa operazione è stata ignorata.

## Fase

1. Utilizzare `volume efficiency start -scan-old-data` comando per eseguire la deduplica, la compressione dei dati o la compattazione dei dati manualmente sui dati esistenti.

Il seguente comando consente di eseguire queste operazioni manualmente sui dati esistenti nel volume Vola:

```
volume efficiency start -vserver vs1 -volume VolA -scan-old-data true [-compression | -dedupe | -compaction ] true
```

## Gestire le operazioni di efficienza dei volumi utilizzando le pianificazioni

### Eseguire operazioni di efficienza in base alla quantità di nuovi dati scritti

È possibile modificare la pianificazione delle operazioni di efficienza per eseguire la deduplica o la compressione dei dati quando il numero di nuovi blocchi scritti nel volume dopo l'operazione di efficienza precedente (eseguita manualmente o pianificata) supera una percentuale di soglia specificata.

#### A proposito di questa attività

Se il `schedule` l'opzione è impostata su `auto`, l'operazione di efficienza pianificata viene eseguita quando la quantità di nuovi dati supera la percentuale specificata. Il valore di soglia predefinito è 20 per cento. Questo valore di soglia è la percentuale del numero totale di blocchi già elaborati dall'operazione di efficienza.

## Fase

1. Utilizzare `volume efficiency modify` con il `auto@num` opzione per modificare il valore della percentuale di soglia.

`num` è un numero di due cifre per specificare la percentuale.

## Esempio

Il comando seguente modifica il valore della soglia percentuale al 30% per il volume Vola:

```
volume efficiency modify -vserver vs1 -volume -VolA -schedule auto@30
```

### Eseguire operazioni di efficienza utilizzando la pianificazione

È possibile modificare la pianificazione delle operazioni di deduplica o compressione dei dati su un volume utilizzando `volume efficiency modify` comando. Le opzioni di configurazione di una policy di pianificazione e di efficienza dei volumi si escludono a vicenda.

## Fase

1. Utilizzare `volume efficiency modify` comando per modificare la pianificazione delle operazioni di deduplica o compressione dei dati su un volume.

## Esempi

Il seguente comando modifica la pianificazione delle operazioni di efficienza per Vola da eseguire alle 11:00, dal lunedì al venerdì:

```
volume efficiency modify -vserver vs1 -volume VolA -schedule mon-fri@23
```

## Monitorare le operazioni di efficienza dei volumi

### Visualizza le operazioni e lo stato di efficienza

È possibile visualizzare se la deduplica o la compressione dei dati è attivata su un volume. È inoltre possibile visualizzare lo stato, lo stato, il tipo di compressione e l'avanzamento delle operazioni di efficienza su un volume utilizzando `volume efficiency show` comando.

### Visualizza lo stato di efficienza

#### Fase

1. Visualizzare lo stato di un'operazione di efficienza su un volume: `volume efficiency show`

Il seguente comando visualizza lo stato di un'operazione di efficienza sul volume Vola a cui è assegnato il tipo di compressione adattiva:

```
volume efficiency show -instance -vserver vs1 -volume VolA
```

Se l'operazione di efficienza è attivata sul volume volta e l'operazione è inattiva, nell'output di sistema viene visualizzato quanto segue:

```
cluster1::> volume efficiency show -vserver vs1 -volume VolA

Vserver Name: vs1
Volume Name: VolA
Volume Path: /vol/VolA
      State: Enabled
      Status: Idle
Progress: Idle for 00:03:20
```

## Determinare se i volumi contengono dati compressi in sequenza

È possibile visualizzare un elenco di volumi con il packing sequenziale attivato, ad esempio, quando è necessario ripristinare una release di ONTAP precedente alla 9.13.1. Per utilizzare questo comando, è necessario essere in modalità avanzata con privilegi.

#### Fase

1. Impostare il livello di privilegio: `set -privilege advanced`
2. Elencare i volumi con il packing sequenziale abilitato: "L'efficienza dei volumi mostra -compressione estesa-automatica-adattativa-true"

### Visualizza i risparmi di spazio in termini di efficienza

È possibile visualizzare la quantità di risparmio di spazio ottenuto tramite la deduplica e la compressione dei dati su un volume utilizzando `volume show` comando.

### A proposito di questa attività

I risparmi di spazio nelle copie Snapshot non sono inclusi nel calcolo dei risparmi di spazio ottenuti su un volume. L'utilizzo della deduplica non influisce sulle quote dei volumi. Le quote vengono riportate a livello logico e rimangono invariate.

### Fase

1. Utilizzare `volume show` comando per visualizzare i risparmi di spazio ottenuti su un volume utilizzando la deduplica e la compressione dei dati.

### Esempio

Il seguente comando consente di visualizzare i risparmi di spazio ottenuti utilizzando la deduplica e la compressione dei dati sul volume Vola: `volume show -vserver vs1 -volume Vola`

```
cluster1::> volume show -vserver vs1 -volume Vola

Vserver Name: vs1
Volume Name: Vola

...

    Space Saved by Storage Efficiency: 115812B
Percentage Saved by Storage Efficiency: 97%
    Space Saved by Deduplication: 13728B
Percentage Saved by Deduplication: 81%
    Space Shared by Deduplication: 1028B
    Space Saved by Compression: 102084B
Percentage Space Saved by Compression: 97%

...
```

### Visualizzare le statistiche di efficienza di un volume FlexVol

È possibile visualizzare i dettagli delle operazioni di efficienza eseguite su un volume FlexVol utilizzando `volume efficiency stat` comando.

### Fase

1. Utilizzare `volume efficiency stat` Per visualizzare le statistiche delle operazioni di efficienza su un volume FlexVol.

### Esempio

Il seguente comando consente di visualizzare le statistiche delle operazioni di efficienza sul volume Vola: `volume efficiency stat -vserver vs1 -volume Vola`



```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA
```

```
Vserver Name: vs1
```

```
Volume Name: VolA
```

```
Volume Path: /vol/VolA
```

```
Inline Compression Attempts: 0
```

## Arrestare le operazioni di efficienza dei volumi

È possibile interrompere un'operazione di deduplica o compressione post-elaborazione utilizzando `volume efficiency stop` comando. Questo comando genera automaticamente un checkpoint.

### Fase

1. Utilizzare `volume efficiency stop` per interrompere un'operazione di deduplica attiva o di compressione post-processo.

Se si specifica `-all` le operazioni di efficienza attive e in coda vengono interrotte.

### Esempi

Il seguente comando interrompe l'operazione di deduplica o compressione post-processo attualmente attiva sul volume VolA:

```
volume efficiency stop -vserver vs1 -volume VolA
```

Il seguente comando interrompe le operazioni di deduplica attiva e in coda o di compressione post-processo sul volume VolA:

```
volume efficiency stop -vserver vs1 -volume VolA -all true
```

## Informazioni sulla rimozione dei risparmi di spazio da un volume

È possibile scegliere di rimuovere i risparmi di spazio ottenuti eseguendo le operazioni di efficienza su un volume, ma deve avere spazio sufficiente per adattarsi alla loro inversione.

Consulta questi articoli della Knowledge base:

- ["Come verificare i risparmi di spazio derivanti da deduplica, compressione e compattazione in ONTAP 9"](#)
- ["Come annullare i risparmi in termini di efficienza dello storage in ONTAP"](#)

## Eseguire il rehosting di un volume da una SVM a un'altra SVM

### Panoramica di un volume da una SVM a un'altra SVM

Il re-host dei volumi consente di riassegnare volumi NAS o SAN da una macchina virtuale di storage (SVM, precedentemente nota come Vserver) a un'altra SVM senza richiedere una copia SnapMirror. Le procedure di rehost del volume dipendono dal tipo di protocollo

e dal tipo di volume. Il rehost dei volumi è un'operazione di interruzione per l'accesso ai dati e la gestione dei volumi.

### **Prima di iniziare**

Prima di poter eseguire il rehosting di un volume da una SVM a un'altra, è necessario soddisfare diverse condizioni:

- Il volume deve essere online.
- Protocolli: SAN o NAS

Per il protocollo NAS, il volume deve essere smontato.

- Se il volume si trova in una relazione SnapMirror, la relazione deve essere eliminata o interrotta prima di eseguire il rehosting del volume.

È possibile risincronizzare la relazione di SnapMirror dopo l'operazione di rehosting del volume.

### **Eseguire nuovamente l'hosting dei volumi SMB**

È possibile eseguire il rehosting dei volumi che servono i dati tramite il protocollo SMB. Dopo aver eseguito il rehosting del volume CIFS, per continuare ad accedere ai dati tramite il protocollo SMB, è necessario configurare manualmente i criteri e le regole associate.

#### **A proposito di questa attività**

- Il rehosting è un'operazione che interrompe.
- Se l'operazione di rehosting non riesce, potrebbe essere necessario riconfigurare i criteri del volume e le regole associate sul volume di origine.
- Se i domini Active Directory SVM di origine e SVM di destinazione differiscono, l'accesso agli oggetti sul volume potrebbe essere perso.
- A partire da ONTAP 9.8, è supportato il rehosting di un volume con crittografia volume NetApp (NVE). Se si utilizza un gestore di chiavi integrato, i metadati crittografati verranno modificati durante l'operazione di rehosting. I dati dell'utente non vengono modificati.

Se si utilizza ONTAP 9.8 o una versione precedente, è necessario annullare la crittografia del volume prima di eseguire l'operazione di rehosting.

- Quando la SVM di origine dispone di utenti e gruppi locali, le autorizzazioni per i file e le directory (ACL) impostati non sono più efficaci dopo l'operazione di rehosting del volume.

Lo stesso vale per gli ACL di controllo (SACL)

- Dopo l'operazione di rehosting, le seguenti policy, regole dei criteri e configurazioni del volume vengono perse dal volume di origine e devono essere riconfigurate manualmente sul volume rehosted:
  - Policy di esportazione di volumi e qtree
  - Policy antivirus
  - Policy di efficienza dei volumi
  - Policy sulla qualità del servizio (QoS)

- Policy di Snapshot
- Regole di quota
- criteri e regole di esportazione della configurazione di ns-switch e name services
- ID utente e gruppo

### Prima di iniziare

- Il volume deve essere online.
- Le operazioni di gestione dei volumi, ad esempio lo spostamento del volume o del LUN, non devono essere in esecuzione.
- L'accesso ai dati al volume che viene reospitato deve essere interrotto.
- La configurazione ns-switch e name Services della SVM di destinazione deve essere configurata per supportare l'accesso ai dati del volume di re-hosting.
- La SVM di origine e la SVM di destinazione devono avere lo stesso dominio Active Directory e realmDNS.
- L'ID utente e l'ID gruppo del volume devono essere disponibili nella SVM di destinazione o modificati nel volume di hosting.



Se sono configurati utenti e gruppi locali e se sono presenti file e directory su quel volume con autorizzazioni impostate per tali utenti o gruppi, queste autorizzazioni non sono più effettive.

### Fasi

1. Registrare le informazioni sulle condivisioni CIFS per evitare di perdere le informazioni sulle condivisioni CIFS in caso di errore dell'operazione di rehost del volume.
2. Smontare il volume dal volume padre:

```
volume unmount
```

3. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

4. Eseguire nuovamente l'hosting del volume sulla SVM di destinazione:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver  
destination_svm
```

5. Montare il volume sotto il percorso di giunzione appropriato nella SVM di destinazione:

```
volume mount
```

6. Creare condivisioni CIFS per il volume rehosted:

```
vserver cifs share create
```

7. Se i domini DNS differiscono tra SVM di origine e SVM di destinazione, creare nuovi utenti e gruppi.
8. Aggiornare il client CIFS con i nuovi LIF SVM di destinazione e il percorso di giunzione per il volume rehosted.

## Al termine

È necessario riconfigurare manualmente i criteri e le regole associate sul volume rehosted.

["Configurazione SMB"](#)

["Configurazione multiprotocollo SMB e NFS"](#)

## Eseguire nuovamente l'hosting dei volumi NFS

È possibile eseguire il rehosting dei volumi che servono i dati tramite il protocollo NFS. Dopo aver eseguito il rehosting dei volumi NFS, per continuare ad accedere ai dati tramite il protocollo NFS, è necessario associare il volume alla policy di esportazione della SVM di hosting e configurare manualmente i criteri e le regole associate.

### A proposito di questa attività

- Il rehosting è un'operazione che interrompe.
- Se l'operazione di rehosting non riesce, potrebbe essere necessario riconfigurare i criteri del volume e le regole associate sul volume di origine.
- A partire da ONTAP 9.8, è supportato il rehosting di un volume con crittografia volume NetApp (NVE). Se si utilizza un gestore di chiavi integrato, i metadati crittografati verranno modificati durante l'operazione di rehosting. I dati dell'utente non vengono modificati.

Se si utilizza ONTAP 9.8 o una versione precedente, è necessario annullare la crittografia del volume prima di eseguire l'operazione di rehosting.

- Dopo l'operazione di rehosting, le seguenti policy, regole dei criteri e configurazioni del volume vengono perse dal volume di origine e devono essere riconfigurate manualmente sul volume rehosted:
  - Policy di esportazione di volumi e qtree
  - Policy antivirus
  - Policy di efficienza dei volumi
  - Policy sulla qualità del servizio (QoS)
  - Policy di Snapshot
  - Regole di quota
  - criteri e regole di esportazione della configurazione di ns-switch e name services
  - ID utente e gruppo

### Prima di iniziare

- Il volume deve essere online.
- Le operazioni di gestione dei volumi, come gli spostamenti dei volumi o delle LUN, non devono essere in esecuzione.
- L'accesso ai dati al volume che viene reospitato deve essere interrotto.
- La configurazione ns-switch e name Services della SVM di destinazione deve essere configurata per supportare l'accesso ai dati del volume di re-hosting.
- L'ID utente e l'ID gruppo del volume devono essere disponibili nella SVM di destinazione o modificati nel volume di hosting.

## Fasi

1. Registrare le informazioni relative ai criteri di esportazione NFS per evitare di perdere informazioni sui criteri NFS in caso di errore dell'operazione di rehost del volume.

2. Smontare il volume dal volume padre:

```
volume unmount
```

3. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

4. Eseguire nuovamente l'hosting del volume sulla SVM di destinazione:

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver  
destination_svm
```

Il criterio di esportazione predefinito della SVM di destinazione viene applicato al volume rehosted.

5. Creare la policy di esportazione:

```
vserver export-policy create
```

6. Aggiornare il criterio di esportazione del volume reospitato in un criterio di esportazione definito dall'utente:

```
volume modify
```

7. Montare il volume sotto il percorso di giunzione appropriato nella SVM di destinazione:

```
volume mount
```

8. Verificare che il servizio NFS sia in esecuzione sulla SVM di destinazione.

9. Riprendere l'accesso NFS al volume reospitato.

10. Aggiornare le credenziali del client NFS e le configurazioni LIF per riflettere le LIF SVM di destinazione.

Questo perché il percorso di accesso al volume (LIF e percorso di giunzione) è stato modificato.

### **Al termine**

È necessario riconfigurare manualmente i criteri e le regole associate sul volume rehosted.

### **"Configurazione NFS"**

### **Eseguire il rehosting dei volumi SAN**

È possibile eseguire il rehosting dei volumi con LUN mappati. Dopo aver ricreato il gruppo di iniziatori (igroup) nella SVM di destinazione, il rehost del volume può rimappare automaticamente il volume sulla stessa SVM.

### **A proposito di questa attività**

- Il rehosting è un'operazione che interrompe.
- Se l'operazione di rehosting non riesce, potrebbe essere necessario riconfigurare i criteri del volume e le regole associate sul volume di origine.

- A partire da ONTAP 9.8, è supportato il rehosting di un volume con crittografia volume NetApp (NVE). Se si utilizza un gestore di chiavi integrato, i metadati crittografati verranno modificati durante l'operazione di rehosting. I dati dell'utente non vengono modificati.

Se si utilizza ONTAP 9.8 o una versione precedente, è necessario annullare la crittografia del volume prima di eseguire l'operazione di rehosting.

- Dopo l'operazione di rehosting, le seguenti policy, regole dei criteri e configurazioni del volume vengono perse dal volume di origine e devono essere riconfigurate manualmente sul volume rehosted:
  - Policy antivirus
  - Policy di efficienza dei volumi
  - Policy sulla qualità del servizio (QoS)
  - Policy di Snapshot
  - criteri e regole di esportazione della configurazione di ns-switch e name services
  - ID utente e gruppo

### Prima di iniziare

- Il volume deve essere online.
- Le operazioni di gestione dei volumi, come gli spostamenti dei volumi o delle LUN, non devono essere in esecuzione.
- Non devono essere presenti i/o attivi sui volumi o sui LUN.
- È necessario verificare che la SVM di destinazione non abbia igroup con lo stesso nome ma iniziatori diversi.

Se l'igroup ha lo stesso nome, è necessario rinominare l'igroup in una delle SVM (origine o destinazione).

- È necessario aver attivato `force-unmap-luns` opzione.
  - Il valore predefinito di `force-unmap-luns` l'opzione è `false`.
  - Quando si imposta, non viene visualizzato alcun messaggio di avviso o di conferma `force-unmap-luns` opzione a. `true`.

### Fasi

1. Registrare le informazioni di mappatura LUN sul volume di destinazione:

```
lun mapping show volume volume vserver source_svm
```

Si tratta di una procedura precauzionale per evitare la perdita di informazioni sulla mappatura LUN in caso di errore del rehost del volume.

2. Elimina igroups associati al volume di destinazione.
3. Eseguire nuovamente l'hosting del volume di destinazione nella SVM di destinazione:

```
volume rehost -vserver source_svm -volume volume_name -destination-vserver  
destination_svm
```

4. Mappare i LUN sul volume di destinazione su igroups appropriati.
  - Il rehost del volume conserva le LUN sul volume di destinazione; tuttavia, le LUN rimangono non mappate.

- Utilizzare la porta SVM di destinazione impostata durante la mappatura dei LUN.
- Se il `auto-remap-luns` l'opzione è impostata su `true`, i LUN vengono mappati automaticamente dopo il rehost.

## Eseguire il rehosting dei volumi in una relazione SnapMirror

È possibile eseguire il rehosting dei volumi in una relazione SnapMirror.

### A proposito di questa attività

- Il rehosting è un'operazione che interrompe.
- Se l'operazione di rehosting non riesce, potrebbe essere necessario riconfigurare i criteri del volume e le regole associate sul volume di origine.
- Dopo l'operazione di rehosting, le seguenti policy, regole dei criteri e configurazioni del volume vengono perse dal volume di origine e devono essere riconfigurate manualmente sul volume rehosted:
  - Policy di esportazione di volumi e qtree
  - Policy antivirus
  - Policy di efficienza dei volumi
  - Policy sulla qualità del servizio (QoS)
  - Policy di Snapshot
  - Regole di quota
  - criteri e regole di esportazione della configurazione di ns-switch e name services
  - ID utente e gruppo

### Prima di iniziare

- Il volume deve essere online.
- Le operazioni di gestione dei volumi, come gli spostamenti dei volumi o delle LUN, non devono essere in esecuzione.
- L'accesso ai dati al volume che viene reospitato deve essere interrotto.
- La configurazione ns-switch e name Services della SVM di destinazione deve essere configurata per supportare l'accesso ai dati del volume di re-hosting.
- L'ID utente e l'ID gruppo del volume devono essere disponibili nella SVM di destinazione o modificati nel volume di hosting.

### Fasi

1. Registrare il tipo di relazione SnapMirror:

```
snapmirror show
```

Si tratta di una procedura precauzionale per evitare di perdere informazioni sul tipo di relazione SnapMirror in caso di errore del rehost del volume.

2. Dal cluster di destinazione, eliminare la relazione SnapMirror:

```
snapmirror delete
```

Non interrompere la relazione di SnapMirror; in caso contrario, la funzionalità di protezione dei dati del volume di destinazione viene persa e la relazione non può essere ristabilita dopo l'operazione di rehosting.

3. Dal cluster di origine, rimuovere le informazioni sulle relazioni di SnapMirror:

```
snapmirror release relationship-info-only true
```

Impostazione di `relationship-info-only` parametro a. `true` Rimuove le informazioni di relazione di origine senza eliminare le copie Snapshot.

4. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

5. Eseguire nuovamente l'hosting del volume sulla SVM di destinazione:

```
volume rehost -vserver source_svm -volume vol_name -destination-vserver  
destination_svm
```

6. Se la relazione di peering SVM non è presente, creare la relazione peer SVM tra SVM di origine e SVM di destinazione:

```
vserver peer create
```

7. Creare la relazione di SnapMirror tra il volume di origine e il volume di destinazione:

```
snapmirror create
```

È necessario eseguire `snapmirror create` Dal SVM che ospita il volume DP. Il volume rehosted può essere l'origine o la destinazione della relazione SnapMirror.

8. Risincronizzare la relazione SnapMirror.

## Funzionalità che non supportano il re-host dei volumi

Alcune funzionalità non supportano il rehost del volume.

Le seguenti funzionalità non supportano il rehost dei volumi:

- DR. SVM
- Configurazioni MetroCluster



Anche il cloning di un volume come volume FlexClone su una SVM diversa non è supportato nelle configurazioni MetroCluster.

- Volumi SnapLock
- Volumi con crittografia dei volumi NetApp (nelle versioni di ONTAP precedenti alla 9.8)

Nelle versioni di ONTAP precedenti alla 9.8, è necessario annullare la crittografia del volume prima di eseguirne il rehosting. Le chiavi di crittografia dei volumi dipendono dalle chiavi SVM. Se un volume viene spostato in un'altra SVM e la configurazione della chiave multi-tenant è attivata sulla SVM di origine o di destinazione, le chiavi del volume e della SVM non corrispondono.

A partire da ONTAP 9.8, è possibile eseguire il rehosting di un volume con NVE.

- Volumi FlexGroup



- Clonare i volumi

## Limiti di storage

Esistono limiti per gli oggetti di storage che è necessario prendere in considerazione durante la pianificazione e la gestione dell'architettura di storage.

I limiti dipendono spesso dalla piattaforma. Fare riferimento a. ["NetApp Hardware Universe"](#) per conoscere i limiti della configurazione specifica. Vedere [\[hwu\]](#) Per istruzioni su come identificare le informazioni appropriate per la configurazione ONTAP in uso.

I limiti sono elencati nelle seguenti sezioni:

- [\[vollimits\]](#)
- [\[flexclone\]](#)

I limiti di storage per Cloud Volumes ONTAP sono documentati nella ["Note di rilascio di Cloud Volumes ONTAP"](#).

## Limiti di volume

Oggetto di storage	Limite	Storage nativo	Storage array
<b>LUN array</b>	Dimensione minima del volume root <sup>1</sup>	N/A.	In base al modello
<b>File</b>	Dimensione massima	Dipendente dalla versione <sup>2</sup>	Dipendente dalla versione <sup>2</sup>
Massimo per volume <sup>4</sup>	Dipendente dalle dimensioni del volume, fino a 2 miliardi di dollari	Dipendente dalle dimensioni del volume, fino a 2 miliardi di dollari	<b>Volumi FlexClone</b>
Profondità del clone gerarchico <sup>5</sup>	499	499	<b>Volumi FlexVol</b>
Massimo per nodo <sup>1</sup>	In base al modello	In base al modello	Massimo per nodo per SVM <sup>6</sup>
In base al modello	In base al modello	Dimensione minima	20 MB
20 MB	Dimensione massima <sup>1</sup>	In base al modello	In base al modello
<b>Volumi FlexVol per carichi di lavoro primari</b>	Massimo per nodo <sup>3</sup>	In base al modello	In base al modello
<b>Volumi root FlexVol</b>	Dimensione minima <sup>1</sup>	In base al modello	In base al modello
<b>LUN</b>	Massimo per nodo <sup>6</sup>	In base al modello	In base al modello

Oggetto di storage	Limite	Storage nativo	Storage array
Massimo per cluster <sup>6</sup>	In base al modello	In base al modello	Massimo per volume <sup>6</sup>
In base al modello	In base al modello	Dimensione massima	Dipendente dalla versione <sup>2</sup>
Dipendente dalla versione <sup>2</sup>	<b>Qtree</b>	Massimo per volume FlexVol	4,995
4,995	<b>Copie Snapshot</b>	Massimo per volume <sup>7</sup>	255/1023
255/1023	<b>Volumi</b>	Massimo per cluster per NAS	12,000
12,000	Massimo per cluster con protocolli SAN configurati	In base al modello	In base al modello

#### Note:

1. In ONTAP 9.3 e versioni precedenti, un volume può contenere fino a 255 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume può contenere fino a 1023 copie Snapshot.
2. A partire da ONTAP 9.12.1P2, il limite è di 128 TB. In ONTAP 9.11.1 e nelle versioni precedenti, il limite è di 16 TB.
3. A partire da ONTAP 9,7, il numero massimo di volumi FlexVol supportati sulle piattaforme AFF con almeno 128 GB di memoria è aumentato a 2.500 volumi FlexVol per nodo.

Per informazioni specifiche sulla piattaforma e per informazioni aggiornate sul supporto, visitare il sito Web all'indirizzo ["Hardware Universe"](#).

4. 2 miliardi =  $2 \times 10^9$ .
5. Profondità massima di una gerarchia nidificata di volumi FlexClone che è possibile creare da un singolo volume FlexVol.
6. Questo limite si applica solo agli ambienti SAN.

#### ["Configurazione SAN"](#)

7. È possibile utilizzare una distribuzione a cascata di SnapMirror per aumentare questo limite.

#### Limiti di file FlexClone e LUN FlexClone

Limite	Storage nativo	Storage array
<b>Massimo per file o LUN<sup>1</sup></b>	32,767	32,767
<b>Massimo totale dei dati condivisi per volume FlexVol</b>	640 TB	640 TB

#### Nota:

1. Se si tenta di creare più di 32,767 cloni, ONTAP crea automaticamente una nuova copia fisica del file padre o del LUN.

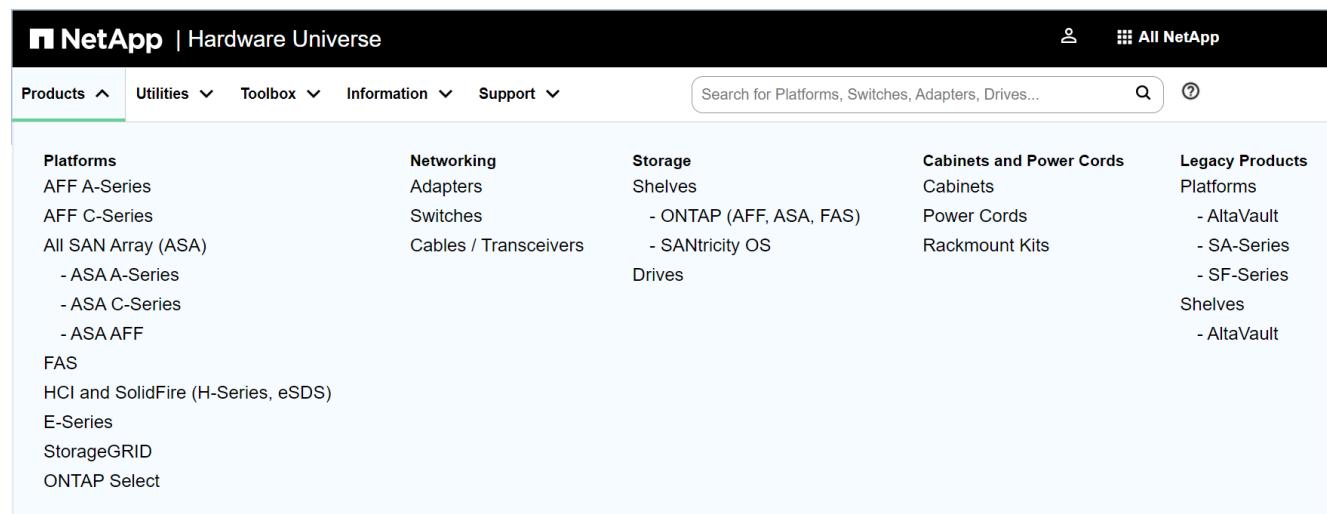
Questo limite potrebbe essere inferiore per i volumi FlexVol che utilizzano la deduplica.

## Navigare in NetApp Hardware Universe

Per individuare i limiti specifici della piattaforma e dipendenti dal modello, fare riferimento alla ["NetApp Hardware Universe"](#).

### Fasi

1. Nel menu a discesa **prodotti**, selezionare la configurazione hardware.



2. Selezionare la piattaforma.

☒ **Start with Platforms**      ☐ **Start with OS**      Help

☐ **Show EOA Platforms**

☒ **Display Platform Configurations**

Filter Platforms

☒ AFF C-Series

☒ AFF C250

☐ AFF C250 Single Chassis HA Pair

☐ AFF C250 Single Chassis HA Pair 100V

☐ AFF C250 4-Node MetroCluster IP

☐ AFF C250 8-Node MetroCluster IP

☒ AFF C400

☐ AFF C400 Single Chassis HA Pair, Ethernet Bundle

☐ AFF C400 Single Chassis HA Pair, FC Bundle

☐ AFF C400 4-Node MetroCluster IP, Ethernet Bundle

☐ AFF C400 4-Node MetroCluster IP, FC Bundle

☐ AFF C400 8-Node MetroCluster IP, Ethernet Bundle

☐ AFF C400 8-Node MetroCluster IP, FC Bundle

☒ AFF C800

☐ AFF C800 Single Chassis HA Pair

☐ AFF C800 4-Node MetroCluster IP

3. Selezionare la versione appropriata di ONTAP quindi **Mostra risultati**.

758

Start with Platforms

Start with OS

Help

☐ Show EOA Platforms
 ☒ Display Platform Configurations

Filter Platforms

AFF C-Series

☐ AFF C250
 

☐ AFF C250 Single Chassis HA Pair
 ☐ AFF C250 Single Chassis HA Pair 100V
 ☐ AFF C250 4-Node MetroCluster IP
 ☐ AFF C250 8-Node MetroCluster IP

☐ AFF C400
 

☐ AFF C400 Single Chassis HA Pair, Ethernet Bundle
 ☐ AFF C400 Single Chassis HA Pair, FC Bundle
 ☐ AFF C400 4-Node MetroCluster IP, Ethernet Bundle
 ☐ AFF C400 4-Node MetroCluster IP, FC Bundle
 ☐ AFF C400 8-Node MetroCluster IP, Ethernet Bundle
 ☐ AFF C400 8-Node MetroCluster IP, FC Bundle

☒ AFF C800
 

☒ AFF C800 Single Chassis HA Pair
 ☒ AFF C800 4-Node MetroCluster IP
 ☒ AFF C800 8-Node MetroCluster IP

Filter by OS Status :

☐ Show All
 ☒ Hide EOVS
 ☐ Hide Obsolete

Show OS :

☒ Support at least one of the platform selected
 ☐ Support all the platform selected
 ☐ Show all

DataONTAP

9.14.1

☐ Release Candidate
 

☐ 9.14.1RC1

9.13.1

☒ General Availability
 

☒ 9.13.1

☐ Patch Release
 

☐ 9.13.1P6
 ☐ 9.13.1P4
 ☐ 9.13.1P3
 ☐ 9.13.1P2
 ☐ 9.13.1P1

9.12.1

☐ Patch Release
 

☐ 9.12.1P10
 ☐ 9.12.1P9
 ☐ 9.12.1P8

Clear

Clear

Note: AFF C190 model information is in the AFF A-Series product category

Preference ▾

Show Results

## Informazioni correlate

["Trova le Note di rilascio relative alla tua versione di Cloud Volumes ONTAP"](#)

## Combinazioni di configurazione di volume e file o LUN consigliate

### Panoramica delle combinazioni di configurazione di volume e file o LUN consigliate

Esistono combinazioni specifiche di configurazioni di volume e file o LUN FlexVol che è possibile utilizzare, a seconda dei requisiti di amministrazione e dell'applicazione. La comprensione dei vantaggi e dei costi di queste combinazioni può aiutarti a determinare la combinazione di configurazione del volume e del LUN più adatta al tuo ambiente.

Si consiglia di utilizzare le seguenti combinazioni di configurazione del volume e del LUN:

- File o LUN con spazio riservato con provisioning di volumi thick
- File o LUN non riservati in termini di spazio con provisioning di volumi thin

759

- File o LUN con spazio riservato con provisioning di volumi semi-spessi

È possibile utilizzare il thin provisioning SCSI sui LUN in combinazione con una qualsiasi di queste combinazioni di configurazione.

#### **File o LUN con spazio riservato con provisioning di volumi thick**

##### **Benefici:**

- Tutte le operazioni di scrittura all'interno dei file con spazio riservato sono garantite; non si verificheranno errori a causa dello spazio insufficiente.
- Non esistono limitazioni all'efficienza dello storage e alle tecnologie di protezione dei dati sul volume.

##### **Costi e limitazioni:**

- È necessario disporre di spazio sufficiente per l'aggregato in primo piano per supportare il volume con provisioning spesso.
- Lo spazio pari al doppio delle dimensioni del LUN viene allocato dal volume al momento della creazione del LUN.

#### **File o LUN non riservati in termini di spazio con provisioning di volumi thin**

##### **Benefici:**

- Non esistono limitazioni all'efficienza dello storage e alle tecnologie di protezione dei dati sul volume.
- Lo spazio viene allocato solo quando viene utilizzato.

##### **Costi e restrizioni:**

- Le operazioni di scrittura non sono garantite; possono fallire se il volume esaurisce lo spazio libero.
- È necessario gestire lo spazio libero nell'aggregato in modo efficace per evitare che l'aggregato esaurisca lo spazio libero.

#### **File o LUN con spazio riservato con provisioning di volumi semi-spessi**

##### **Benefici:**

Meno spazio viene riservato in anticipo rispetto al provisioning di volumi spessi e viene comunque fornita una garanzia di scrittura con il massimo sforzo.

##### **Costi e restrizioni:**

- Con questa opzione, le operazioni di scrittura possono non riuscire.

È possibile ridurre questo rischio bilanciando correttamente lo spazio libero nel volume rispetto alla volatilità dei dati.

- Non è possibile fare affidamento sulla conservazione di oggetti di protezione dei dati come copie Snapshot e file FlexClone e LUN.
- Non è possibile utilizzare le funzionalità di efficienza dello storage per la condivisione di blocchi di ONTAP che non possono essere eliminate automaticamente, tra cui deduplica, compressione e offload ODX/copia.

## Determinare la combinazione di configurazione del volume e del LUN corretta per l'ambiente in uso

Rispondendo ad alcune domande di base sull'ambiente in uso, è possibile determinare la migliore configurazione del volume FlexVol e del LUN per l'ambiente in uso.

### A proposito di questa attività

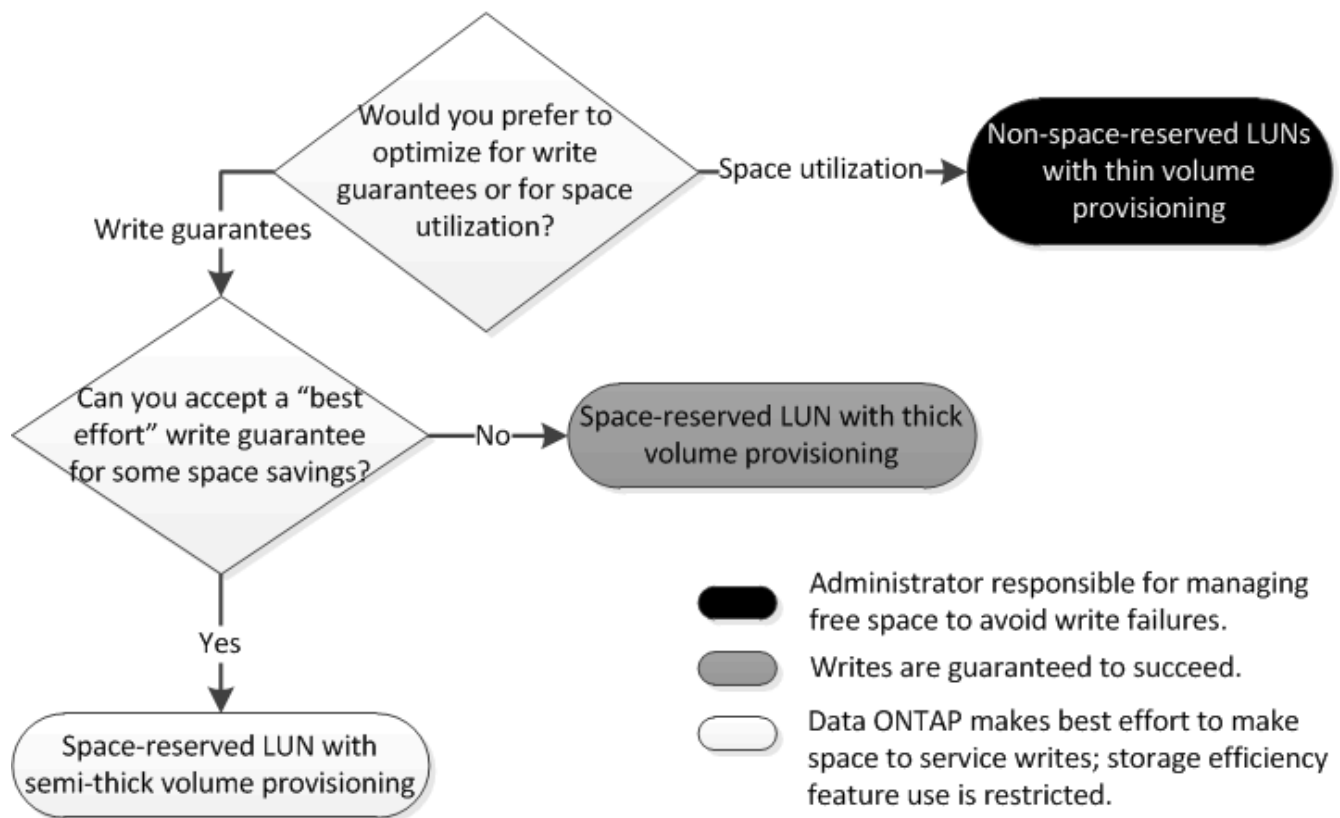
È possibile ottimizzare le configurazioni di LUN e volumi per il massimo utilizzo dello storage o per la sicurezza delle garanzie di scrittura. In base ai requisiti di utilizzo dello storage e alla capacità di monitorare e riempire rapidamente lo spazio libero, è necessario determinare il volume FlexVol e i volumi LUN appropriati per l'installazione.



Non è necessario un volume separato per ogni LUN.

### Fase

1. Utilizzare la seguente struttura decisionale per determinare la combinazione di configurazione del volume e del LUN migliore per l'ambiente in uso:



### Impostazioni di configurazione per file o LUN con spazio riservato con volumi con thick provisioning

Questa combinazione di configurazione di file e volumi FlexVol o LUN offre la possibilità di utilizzare le tecnologie di efficienza dello storage e non richiede il monitoraggio attivo dello spazio libero, in quanto viene allocato spazio sufficiente in anticipo.

Le seguenti impostazioni sono necessarie per configurare un file o LUN con spazio riservato in un volume utilizzando il thick provisioning:

<b>Impostazione del volume</b>	<b>Valore</b>
Garanzia	Volume
Riserva frazionaria	100
Riserva di Snapshot	Qualsiasi
Eliminazione automatica di Snapshot	Opzionale
Crescita automatica	Facoltativo; se attivato, lo spazio libero aggregato deve essere monitorato attivamente.

<b>Impostazione del file o del LUN</b>	<b>Valore</b>
Prenotazione di spazio	Attivato

### **Impostazioni di configurazione per file non riservati allo spazio o LUN con volumi con thin provisioning**

Questa combinazione di configurazione di file e volumi FlexVol o LUN richiede la minima quantità di storage da allocare in anticipo, ma richiede la gestione dello spazio libero attivo per evitare errori dovuti alla mancanza di spazio.

Le seguenti impostazioni sono necessarie per configurare un LUN o file non riservati allo spazio in un volume con thin provisioning:

<b>Impostazione del volume</b>	<b>Valore</b>
Garanzia	Nessuno
Riserva frazionaria	0
Riserva di Snapshot	Qualsiasi
Eliminazione automatica di Snapshot	Opzionale
Crescita automatica	Opzionale

<b>Impostazione del file o del LUN</b>	<b>Valore</b>
Prenotazione di spazio	Disattivato

### **Considerazioni aggiuntive**

Quando il volume o l'aggregato esaurisce lo spazio, le operazioni di scrittura sul file o sul LUN possono avere esito negativo.



Se non si desidera monitorare attivamente lo spazio libero per il volume e l'aggregato, attivare la crescita automatica per il volume e impostare la dimensione massima del volume in base alle dimensioni dell'aggregato. In questa configurazione, è necessario monitorare attivamente lo spazio libero aggregato, ma non è necessario monitorare lo spazio libero nel volume.

### **Impostazioni di configurazione per file o LUN con spazio riservato con provisioning di volumi semi-spessi**

Questa combinazione di configurazione di file e volumi FlexVol o LUN richiede una quantità inferiore di storage da allocare in anticipo rispetto alla combinazione con provisioning completo, ma pone restrizioni sulle tecnologie di efficienza che è possibile utilizzare per il volume. Le sovrascritture vengono eseguite con il massimo sforzo per questa combinazione di configurazione.

Le seguenti impostazioni sono necessarie per configurare un LUN con spazio riservato in un volume utilizzando il provisioning semi-spessi:

<b>Impostazione del volume</b>	<b>Valore</b>
Garanzia	Volume
Riserva frazionaria	0
Riserva di Snapshot	0
Eliminazione automatica di Snapshot	On, con un livello di impegno di Destroy, un elenco Destroy che include tutti gli oggetti, il trigger impostato sul volume e tutti i LUN FlexClone e i file FlexClone abilitati per l'eliminazione automatica.
Crescita automatica	Facoltativo; se attivato, lo spazio libero aggregato deve essere monitorato attivamente.

<b>Impostazione del file o del LUN</b>	<b>Valore</b>
Prenotazione di spazio	Attivato

### **Restrizioni tecnologiche**

Non è possibile utilizzare le seguenti tecnologie per l'efficienza dello storage dei volumi per questa combinazione di configurazione:

- Compressione
- Deduplica
- Offload delle copie di ODX e FlexClone
- LUN FlexClone e file FlexClone non contrassegnati per l'eliminazione automatica (cloni attivi)
- File secondari FlexClone
- Offload ODX/copia

## Considerazioni aggiuntive

Quando si utilizza questa combinazione di configurazione, è necessario considerare i seguenti fatti:

- Quando il volume che supporta tale LUN occupa poco spazio, i dati di protezione (LUN e file FlexClone, copie Snapshot) vengono distrutti.
- Le operazioni di scrittura possono scadere e fallire quando il volume esaurisce lo spazio libero.

La compressione è attivata per impostazione predefinita per le piattaforme AFF. È necessario disattivare esplicitamente la compressione per qualsiasi volume per il quale si desidera utilizzare il provisioning semi-thick su una piattaforma AFF.

## Precauzioni e considerazioni per la modifica della capacità di file o directory

### Considerazioni per la modifica del numero massimo di file consentiti su un volume FlexVol

I volumi FlexVol possono contenere un numero massimo di file. È possibile modificare il numero massimo di file per un volume, ma prima di procedere, è necessario comprendere come questa modifica influisca sul volume.

Se i dati richiedono un numero elevato di file o directory molto grandi, è possibile espandere la capacità di file o directory di ONTAP. Tuttavia, prima di procedere, è necessario comprendere le limitazioni e gli avvertimenti relativi a tale operazione.

Il numero di file che un volume può contenere è determinato dal numero di inode. Un *inode* è una struttura di dati che contiene informazioni sui file. I volumi hanno inode sia privati che pubblici. Gli inode pubblici vengono utilizzati per i file visibili all'utente; gli inode privati vengono utilizzati per i file utilizzati internamente da ONTAP. È possibile modificare solo il numero massimo di inode pubblici per un volume. Non è possibile modificare il numero di inode privati.

ONTAP imposta automaticamente il numero massimo di inode pubblici per un volume appena creato in base alle dimensioni del volume: 1 inode per 32 KB di dimensione del volume. Quando la dimensione di un volume viene aumentata, direttamente da un amministratore o automaticamente da ONTAP tramite la funzione di dimensionamento automatico, ONTAP aumenta anche (se necessario) il numero massimo di inode pubblici, in modo che vi sia almeno 1 inode per 32 KB di dimensione del volume. Fino a quando il volume non raggiunge circa 680 GB.

Nelle versioni di ONTAP precedenti al 9.13.1, aumentare il volume di dimensioni superiori a 680 GB non comporta automaticamente più inodes, perché ONTAP non crea automaticamente più di 22.369.621 inodes. Se sono necessari più file rispetto al numero predefinito per volumi di qualsiasi dimensione, è possibile utilizzare il comando di modifica del volume per aumentare il numero massimo di inode per il volume.

A partire da ONTAP 9.13.1, il numero massimo di inode continua a crescere, quindi c'è un inode per 32 KB di spazio di volume anche se il volume è superiore a 680 GB. Questa crescita continua fino a quando il volume raggiunge il massimo di 2.147.483.632 inode.

È inoltre possibile ridurre il numero massimo di inode pubblici. Diminuendo il numero di inodes pubblici *non* si modifica la quantità di spazio allocato in inodes, ma diminuisce la quantità massima di spazio che il file inode pubblico può consumare. Dopo che lo spazio è stato allocato per gli inode, non viene mai restituito al volume. Pertanto, l'abbassamento del numero massimo di inodi al di sotto del numero di inodi attualmente allocati non restituisce lo spazio utilizzato dagli inodi allocati.

### Ulteriori informazioni

- [Visualizzazione dell'utilizzo di file o inode](#)

## Precauzioni per l'aumento delle dimensioni massime della directory per i volumi FlexVol

È possibile aumentare le dimensioni massime predefinite della directory per un volume FlexVol specifico utilizzando `-maxdir-size` opzione di `volume modify` ma ciò potrebbe influire sulle prestazioni del sistema. Consultare l'articolo della Knowledge base ["Che cos'è maxdirsize?"](#).

Per ulteriori informazioni sulle dimensioni massime delle directory per i volumi FlexVol in base al modello, visitare il ["NetApp Hardware Universe"](#).

## Regole che regolano i volumi root dei nodi e gli aggregati root

Il volume root di un nodo contiene directory e file speciali per quel nodo. L'aggregato root contiene il volume root. Alcune regole governano il volume root e l'aggregato root di un nodo.

Il volume root di un nodo è un volume FlexVol installato in fabbrica o dal software di installazione. È riservato ai file di sistema, ai file di log e ai file principali. Il nome della directory è `/mroot`, accessibile solo attraverso la shell di sistema dal supporto tecnico. La dimensione minima del volume root di un nodo dipende dal modello di piattaforma.

- Le seguenti regole governano il volume root del nodo:
  - A meno che il supporto tecnico non lo richieda, non modificare la configurazione o il contenuto del volume root.
  - Non memorizzare i dati dell'utente nel volume root.

L'archiviazione dei dati dell'utente nel volume root aumenta il tempo di giveback dello storage tra i nodi di una coppia ha.

- È possibile spostare il volume root in un altro aggregato.

["Spostamento dei volumi root in nuovi aggregati"](#)

- L'aggregato root è dedicato solo al volume root del nodo.

ONTAP impedisce la creazione di altri volumi nell'aggregato root.

["NetApp Hardware Universe"](#)

## Spostare i volumi root in nuovi aggregati

La procedura di sostituzione root migra l'aggregato root corrente in un altro set di dischi senza interruzioni.

### A proposito di questa attività

È possibile modificare la posizione del volume root in un nuovo aggregato nei seguenti scenari:

- Quando gli aggregati root non si trovano sul disco, si preferisce

- Quando si desidera riorganizzare i dischi collegati al nodo
- Quando si esegue una sostituzione degli shelf degli shelf di dischi EOS

## Fasi

### 1. Spostare l'aggregato root:

```
system node migrate-root -node node_name -disklist disk_list -raid-type
raid_type
```

- **-nodo**

Specifica il nodo proprietario dell'aggregato root che si desidera migrare.

- **-disklist**

Specifica l'elenco dei dischi su cui verrà creato il nuovo aggregato root. Tutti i dischi devono essere spare e di proprietà dello stesso nodo. Il numero minimo di dischi richiesto dipende dal tipo di RAID.

- **-raid-type**

Specifica il tipo RAID dell'aggregato root. Il valore predefinito è `raid-dp`. Questo è l'unico tipo supportato in modalità avanzata.

### 2. Monitorare l'avanzamento del lavoro:

```
job show -id jobid -instance
```

## Risultati

Se tutti i controlli preliminari hanno esito positivo, il comando avvia un processo di sostituzione del volume root ed esce.

## Funzionalità supportate con file FlexClone e LUN FlexClone

### Funzionalità supportate con file FlexClone e LUN FlexClone

I file FlexClone e le LUN FlexClone funzionano con diverse funzionalità di ONTAP, come deduplica, copie Snapshot, quote e volumi SnapMirror.

Le seguenti funzionalità sono supportate con i file FlexClone e le LUN FlexClone:

- Deduplica
- Copie Snapshot
- Elenchi di controllo degli accessi
- Quote
- Volumi FlexClone
- NDMP
- Volume SnapMirror
- Il `volume move` comando

- Prenotazione di spazio
- Configurazione HA

### **Come funziona la deduplica con i file FlexClone e le LUN FlexClone**

È possibile utilizzare in modo efficiente lo spazio di storage fisico dei blocchi di dati creando un file FlexClone o un LUN FlexClone del file padre e del LUN padre in un volume abilitato alla deduplica.

Anche il meccanismo di condivisione dei blocchi utilizzato dai file e dalle LUN FlexClone viene utilizzato dalla deduplica. È possibile massimizzare il risparmio di spazio in un volume FlexVol attivando la deduplica sul volume e quindi clonando il volume abilitato alla deduplica.



Durante l'esecuzione di `sis undo` Su un volume abilitato alla deduplica, non è possibile creare file FlexClone e LUN FlexClone dei file padre e LUN padre che risiedono in tale volume.

### **Funzionamento delle copie Snapshot con i file FlexClone e le LUN FlexClone**

È possibile creare file FlexClone e LUN FlexClone da una copia Snapshot esistente dei file padre e LUN padre contenuti in un volume FlexVol.

Tuttavia, non è possibile eliminare manualmente una copia Snapshot da cui vengono creati i file FlexClone o i LUN FlexClone fino al completamento del processo di condivisione dei blocchi tra le entità padre e clone. La copia Snapshot rimane bloccata fino al completamento del processo di condivisione dei blocchi, che si verifica in background. Pertanto, quando si tenta di eliminare una copia Snapshot bloccata, il sistema visualizza un messaggio che richiede di riprovare l'operazione dopo un certo periodo di tempo. In tal caso, se si desidera eliminare manualmente la copia Snapshot specifica, è necessario riprovare l'operazione di eliminazione in modo che la copia Snapshot venga eliminata al termine della condivisione del blocco.

### **Funzionamento degli elenchi di controllo degli accessi con i file FlexClone e le LUN FlexClone**

I file FlexClone e le LUN FlexClone ereditano gli elenchi di controllo degli accessi dei file padre e delle LUN.

Se i file padre contengono flussi Windows NT, i file FlexClone ereditano anche le informazioni sul flusso. Tuttavia, i file padre contenenti più di sei flussi non possono essere clonati.

### **Come funzionano le quote con i file FlexClone e le LUN FlexClone**

I limiti di quota vengono applicati alla dimensione logica totale dei file FlexClone o delle LUN FlexClone. Le operazioni di cloning non falliscono la condivisione dei blocchi anche se causa il superamento delle quote.

Quando si crea un file FlexClone o un LUN FlexClone, le quote non riconoscono alcun risparmio di spazio. Ad esempio, se si crea un file FlexClone di un file padre di 10 GB, si utilizzano solo 10 GB di spazio fisico, ma l'utilizzo delle quote viene registrato come 20 GB (10 GB per il file padre e 10 GB per il file FlexClone).

Se la creazione di un file FlexClone o di un LUN determina il superamento della quota di gruppo o utente, l'operazione di clonazione riesce a condizione che il volume FlexVol disponga di spazio sufficiente per contenere i metadati per il clone. Tuttavia, la quota per quell'utente o gruppo viene sottoscritta in eccesso.

## Come funzionano i volumi FlexClone con i file FlexClone e le LUN FlexClone

È possibile creare un volume FlexClone di un volume FlexVol che contiene un file FlexClone e un LUN FlexClone e il relativo file padre o LUN.

I file FlexClone o le LUN FlexClone e i relativi file padre o LUN presenti nel volume FlexClone continuano a condividere i blocchi allo stesso modo del volume FlexVol padre. Infatti, tutte le entità FlexClone e le loro società madri condividono gli stessi blocchi di dati fisici sottostanti, riducendo al minimo l'utilizzo dello spazio su disco fisico.

Se il volume FlexClone viene diviso dal volume principale, i file FlexClone o le LUN FlexClone e i relativi file padre o LUN smettono di condividere i blocchi nel clone del volume FlexClone. In seguito, esistono come file indipendenti o LUN. Ciò significa che il clone del volume utilizza più spazio rispetto a prima dell'operazione di suddivisione.

## Funzionamento di NDMP con i file FlexClone e le LUN FlexClone

NDMP funziona a livello logico con file FlexClone e LUN FlexClone. Il backup di tutti i file o LUN FlexClone viene eseguito come file o LUN separati.

Quando si utilizzano i servizi NDMP per eseguire il backup di un qtree o di un volume FlexVol che contiene file FlexClone o LUN FlexClone, la condivisione dei blocchi tra entità padre e clone non viene preservata e le entità clonate vengono sottoposte a backup su nastro come file o LUN separati. Il risparmio di spazio viene perso. Pertanto, il nastro su cui si esegue il backup dovrebbe avere spazio sufficiente per memorizzare la quantità espansa di dati. Quando si esegue il ripristino, tutti i file FlexClone e le LUN FlexClone vengono ripristinati come file fisici e LUN separati. È possibile attivare la deduplica sul volume per ripristinare i vantaggi della condivisione di blocchi.



Quando si creano file FlexClone e LUN FlexClone da una copia Snapshot esistente di un volume FlexVol, non è possibile eseguire il backup del volume su nastro fino al completamento del processo di condivisione dei blocchi, che avviene in background. Se si utilizza NDMP sul volume durante il processo di condivisione dei blocchi, il sistema visualizza un messaggio che richiede di riprovare l'operazione dopo un certo periodo di tempo. In una situazione del genere, è necessario continuare a provare l'operazione di backup su nastro in modo che abbia esito positivo al termine della condivisione dei blocchi.

## Come funziona il volume SnapMirror con i file FlexClone e le LUN FlexClone

Volume SnapMirror utilizzato con i file FlexClone e le LUN FlexClone consente di risparmiare spazio, poiché le entità clonate vengono replicate una sola volta.

Se un volume FlexVol è un'origine SnapMirror e contiene file FlexClone o LUN FlexClone, il volume SnapMirror trasferisce solo il blocco fisico condiviso e una piccola quantità di metadati alla destinazione SnapMirror del volume. La destinazione memorizza solo una copia del blocco fisico e questo blocco viene condiviso tra le entità padre e clonate. Pertanto, il volume di destinazione è una copia esatta del volume di origine e tutti i file clone o LUN sul volume di destinazione condividono lo stesso blocco fisico.

## Come lo spostamento del volume influisce sui file FlexClone e sulle LUN FlexClone

Durante la fase di cutover di un'operazione di spostamento del volume, non è possibile creare file FlexClone o LUN FlexClone di un volume FlexVol.

## Come funziona la prenotazione di spazio con i file FlexClone e le LUN FlexClone

Per impostazione predefinita, i file FlexClone e le LUN FlexClone ereditano l'attributo di riserva dello spazio dal file padre e dal LUN padre. Tuttavia, è possibile creare file FlexClone e LUN FlexClone con la riserva di spazio disattivata da un file padre e LUN padre con la riserva di spazio attivata se il volume FlexVol non dispone di spazio.

Se il volume FlexVol non contiene spazio sufficiente per creare un file FlexClone o un LUN FlexClone con la stessa riserva di spazio di quella dell'origine, l'operazione di cloning non riesce.

## Funzionamento di una configurazione ha con file FlexClone e LUN FlexClone

Le operazioni del file FlexClone e del LUN FlexClone sono supportate in una configurazione ha.

In una coppia ha, non è possibile creare file FlexClone o LUN FlexClone sul partner mentre è in corso l'operazione di takeover o giveback. Tutte le operazioni di condivisione dei blocchi in sospeso sul partner vengono riavviate al termine dell'operazione di acquisizione o di giveback.

## Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup

Un volume FlexGroup è un container NAS scalabile che offre performance elevate insieme alla distribuzione automatica del carico. I volumi FlexGroup offrono una capacità elevata (in petabyte), che supera notevolmente i limiti dei volumi FlexVol, senza aggiungere alcun overhead di gestione.

Gli argomenti di questa sezione illustrano come gestire i volumi FlexGroup con Gestione sistema in ONTAP 9.7 e versioni successive. Se si utilizza Gestione di sistema classico (disponibile solo in ONTAP 9.7 e versioni precedenti), consultare questo argomento:

- ["Creare volumi FlexGroup"](#)

A partire da ONTAP 9.9.1, sono supportate le relazioni di fanout di SnapMirror di due o più volumi FlexGroup, con un massimo di otto segmenti fanout. System Manager non supporta le relazioni dei volumi FlexGroup a cascata di SnapMirror.

ONTAP seleziona automaticamente i Tier locali richiesti per la creazione del volume FlexGroup.

A partire da ONTAP 9.8, quando si esegue il provisioning dello storage, la qualità del servizio viene attivata per impostazione predefinita. È possibile disattivare la QoS o scegliere una policy QoS personalizzata durante il processo di provisioning o in un secondo momento.

### Fasi

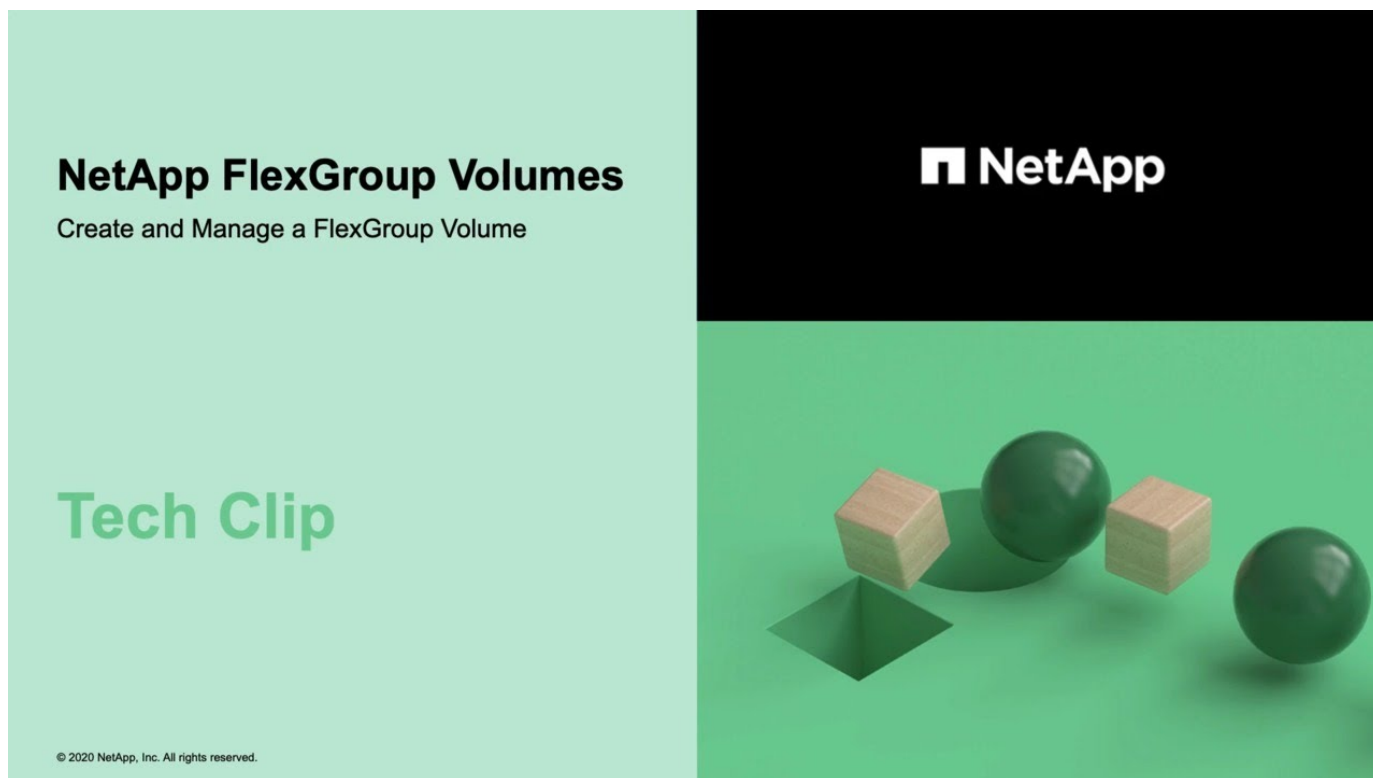
1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Fare clic su **Aggiungi**.
3. Fare clic su **altre opzioni**, quindi selezionare **Distribuisci i dati del volume nel cluster**.



Se si esegue ONTAP 9,8 o versioni successive e si desidera disattivare QoS o scegliere un criterio QoS personalizzato, fare clic su **altre opzioni**, quindi in **archiviazione e ottimizzazione**, selezionare **livello servizio prestazioni**.

## Video

### Creare e gestire un volume FlexGroup



### Volumi FlexGroup: Più risultati con meno risorse

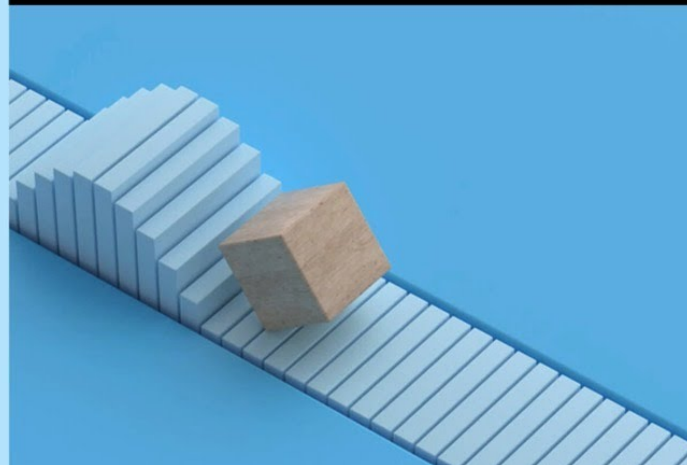


# NetApp FlexGroup Volumes

Do More with Less

## Use Case

© 2020 NetApp, Inc. All rights reserved.



## Gestione dei volumi FlexGroup con l'interfaccia CLI

### Panoramica sulla gestione dei volumi FlexGroup con l'interfaccia CLI

È possibile configurare, gestire e proteggere i volumi FlexGroup per garantire scalabilità e performance. Un volume FlexGroup è un volume scale-out che offre performance elevate insieme alla distribuzione automatica del carico.

È possibile configurare i volumi FlexGroup se si verificano le seguenti condizioni:

- Si utilizza ONTAP 9.1 o versione successiva.
- Si desidera utilizzare NFSv4.x, NFSv3, SMB 2.0 o SMB 2.1.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI) di ONTAP, non Gestione di sistema o uno strumento di scripting automatico.

I dettagli sulla sintassi dei comandi sono disponibili nella guida dell'interfaccia utente e nelle pagine man di ONTAP.

Un importante sottoinsieme di funzionalità FlexGroup è disponibile in Gestione sistema.

- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Si dispone di privilegi di amministratore del cluster, non di amministratore SVM.



A partire da ONTAP 9,5, i gruppi flessibili sostituiscono gli Infinite Volume, che non sono supportati in ONTAP 9,5 o versioni successive.

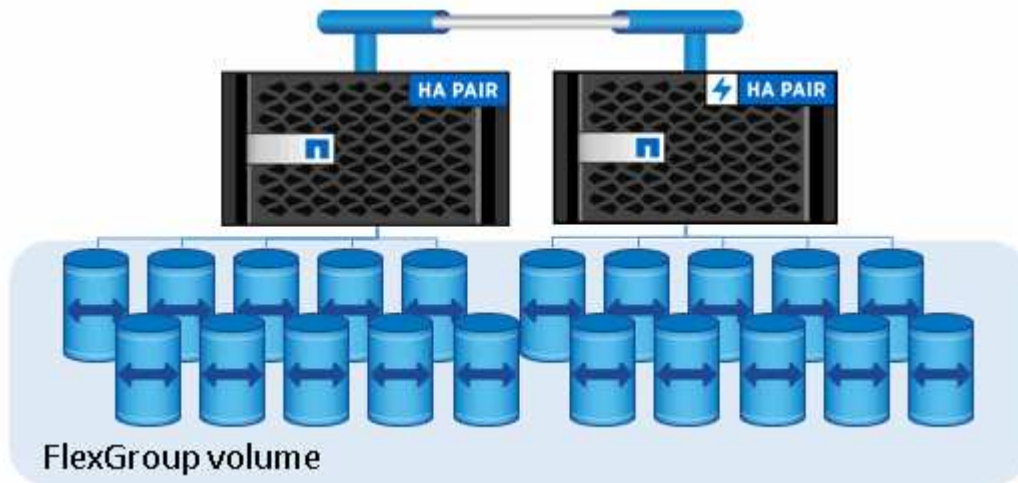
### Informazioni correlate

Le informazioni concettuali sui volumi FlexVol sono applicabili ai volumi FlexGroup. Informazioni sui volumi FlexVol e sulla tecnologia ONTAP sono disponibili nella libreria di riferimento ONTAP e nei report tecnici (TR).

## Che cos'è un volume FlexGroup

Un volume FlexGroup è un container NAS scale-out che offre performance elevate, distribuzione automatica del carico e scalabilità. Un volume FlexGroup contiene diversi componenti che condividono automaticamente e in modo trasparente il traffico.

*Costituenti* sono i volumi FlexVol sottostanti che costituiscono un volume FlexGroup.



I volumi FlexGroup offrono i seguenti vantaggi:

- Elevata scalabilità

La dimensione massima per un volume FlexGroup in ONTAP 9.1 e versioni successive è di 20 PB, con 400 miliardi di file in un cluster a 10 nodi.

- Performance elevate

I volumi FlexGroup possono utilizzare le risorse del cluster per gestire carichi di lavoro con throughput elevato e bassa latenza.

- Gestione semplificata

Un volume FlexGroup è un singolo contenitore di namespace che può essere gestito in modo simile ai volumi FlexVol.

## Configurazioni supportate e non supportate per i volumi FlexGroup

È necessario conoscere le funzionalità di ONTAP supportate e non supportate da FlexGroup Volumes in ONTAP 9.

### Funzioni supportate a partire da ONTAP 9.14.1

- Etichettatura delle copie Snapshot: Supporto per la creazione, la modifica e l'eliminazione di tag di copia Snapshot (etichette e commenti di SnapMirror) per le copie Snapshot su volumi FlexGroup utilizzando il `volume snapshot` comando.

## Funzionalità supportate a partire da ONTAP 9.13.1

- Protezione ransomware autonoma (ARP) per volumi FlexGroup, incluse le seguenti funzionalità supportate:
  - FlexGroup espande le operazioni: Un nuovo costituente eredita attributi di protezione ransomware autonoma.
  - Conversioni da FlexVol a FlexGroup: È possibile convertire FlexVol con protezione ransomware autonoma attiva.
  - Ribilanciamento dei FlexGroup: La protezione autonoma dai ransomware è supportata durante operazioni di ribilanciamento senza interruzioni e con interruzioni.
- Pianificazione di una singola operazione di ribilanciamento FlexGroup.
- Relazioni di fanout di SnapMirror con DR SVM su volumi FlexGroup. Supporta fan-out fino a otto siti.

## Funzionalità supportate a partire da ONTAP 9.12.1

- Ribilanciamento FlexGroup
- SnapLock per SnapVault
- FabricPool, FlexGroup e SVM DR funzionano in collaborazione. (Nelle release precedenti a ONTAP 9.12.1, due di queste funzionalità funzionavano insieme, ma non tutte e tre insieme).
- Dimensioni massime dei componenti del volume FlexGroup di 300 TB sulle piattaforme AFF e FAS con ONTAP 9.12.1 P2 e versioni successive.

## Funzionalità supportate a partire da ONTAP 9.11.1

- Volumi SnapLock

SnapLock non supporta le seguenti funzionalità con FlexGroup Volumes:

- Conservazione a fini giudiziari
- Conservazione basata sugli eventi
- SnapLock per SnapVault

SnapLock viene configurato a livello di FlexGroup. Non è possibile configurare SnapLock a livello di componente.

### [Che cos'è SnapLock](#)

- Eliminazione asincrona della directory del client

[Gestire i diritti dei client per eliminare rapidamente le directory](#)

## Funzionalità supportate a partire da ONTAP 9.10.1

- Conversione di volumi FlexVol in volumi FlexGroup in un'origine SVM-DR

[Convertire un volume FlexVol in un volume FlexGroup in una relazione SVM-DR](#)

- Supporto FlexClone DR SVM per volumi FlexGroup

[Scopri di più sulla creazione di volumi FlexClone.](#)

## Funzionalità supportate a partire da ONTAP 9.9.1

- Disaster recovery SVM

La clonazione di un volume FlexGroup che fa parte di una relazione SVM-DR non è supportata.

- Relazioni di fanout di SnapMirror di 2 o più (Da A a B, Da A a C), con un massimo di 8 segmenti di fanout.

[Considerazioni per la creazione di relazioni a cascata e fan-out di SnapMirror per FlexGroups](#)

- Relazioni a cascata di SnapMirror fino a due livelli (Da A a B a C)

[Considerazioni per la creazione di relazioni a cascata e fan-out di SnapMirror per FlexGroups](#)

## Funzionalità supportate a partire da ONTAP 9.8

- Ripristino di un singolo file da un vault di FlexGroup SnapMirror o da una destinazione UDP
  - Il ripristino può essere eseguito da un volume FlexGroup di qualsiasi geometria a un volume FlexGroup di qualsiasi geometria
  - È supportato un solo file per operazione di ripristino
- Conversione dei volumi passati da sistemi 7-mode a volumi FlexGroup

Per ulteriori informazioni, consultare l'articolo della Knowledge base ["Come convertire un FlexVol in transizione in FlexGroup"](#).

- NFSv4.2
- Eliminazione asincrona di file e directory
- File System Analytics (FSA)
- FlexGroup come datastore VMware vSphere
- Supporto aggiuntivo per backup e ripristino su nastro con NDMP, incluse le seguenti funzionalità:
  - NDMP Restartable Backup Extension (RBE) e Snapshot Management Extension (SSME)
  - Le variabili di ambiente ESCLUDONO e MULTI\_SUBTREE\_NAMES supportano i backup FlexGroup
  - Introduzione della variabile di ambiente IGNORE\_CTIME\_MTIME per i backup FlexGroup
  - Il ripristino di singoli file in un FlexGroup utilizzando il messaggio NDMP\_SNAP\_RECOVER, che fa parte dell'estensione 0x2050, le sessioni di dump e ripristino vengono interrotte durante un aggiornamento o un revert.

## Funzionalità supportate a partire da ONTAP 9.7

- Volume FlexClone
- NFSv4 e NFSv4.1
- PNFS
- Backup e ripristino su nastro utilizzando NDMP

Per il supporto NDMP sui volumi FlexGroup, è necessario conoscere i seguenti punti:

- Il messaggio NDMP\_SNAP\_RECOVER nella classe di estensione 0x2050 può essere utilizzato solo per il ripristino di un intero volume FlexGroup.

I singoli file in un volume FlexGroup non possono essere ripristinati.

- NDMP retardable backup Extension (RBE) non è supportato per i volumi FlexGroup.
- Le variabili di ambiente ESCLUDI e MULTI\_SUBTREE\_NAMES non sono supportate per i volumi FlexGroup.
- Il `ndmcopy` Il comando è supportato per il trasferimento dei dati tra volumi FlexVol e FlexGroup.

Se si ripristina Data ONTAP 9.7 a una versione precedente, le informazioni di trasferimento incrementale dei trasferimenti precedenti non vengono conservate e, di conseguenza, è necessario eseguire una copia di riferimento dopo il ripristino.

- API vStorage VMware per l'integrazione degli array (VAAI)
- Conversione di un volume FlexVol in un volume FlexGroup
- Volumi FlexGroup come volumi di origine FlexCache

### **Funzionalità supportate a partire da ONTAP 9.6**

- Condivisioni SMB sempre disponibili
- Configurazioni MetroCluster
- Ridenominazione di un volume FlexGroup (`volume rename` comando)
- Riduzione o riduzione delle dimensioni di un volume FlexGroup (`volume size` comando)
- Dimensionamento elastico
- Crittografia aggregata NetApp (NAE)
- Cloud Volumes ONTAP

### **Funzionalità supportate a partire da ONTAP 9.5**

- Offload delle copie ODX
- Access Guard a livello di storage
- Miglioramenti alle notifiche di modifica per le condivisioni SMB

Le notifiche di modifica vengono inviate per le modifiche apportate alla directory principale in cui si trova `changenotify` la proprietà viene impostata e per le modifiche a tutte le sottodirectory della directory principale.

- FabricPool
- Applicazione delle quote
- Statistiche qtree
- QoS adattiva per i file nei volumi FlexGroup
- FlexCache (solo cache; FlexGroup come origine supportato in ONTAP 9.7)

### **Funzionalità supportate a partire da ONTAP 9.4**

- FPolicy
- Controllo dei file
- Throughput floor (QoS min) e QoS adattiva per volumi FlexGroup

- Limite di throughput (QoS max) e piano di throughput (QoS min) per i file nei volumi FlexGroup

Si utilizza `volume file modify` Comando per gestire il gruppo di policy QoS associato a un file.

- Limiti di SnapMirror rilassati
- SMB 3.x multicanale

### **Funzionalità supportate a partire da ONTAP 9.3**

- Configurazione antivirus
- Notifiche di modifica per le condivisioni SMB

Le notifiche vengono inviate solo per le modifiche apportate alla directory principale in cui si trova `changenotify` proprietà impostata. Le notifiche di modifica non vengono inviate per le modifiche apportate alle sottodirectory nella directory principale.

- Qtree
- Limite di throughput (QoS max)
- Espandere il volume FlexGroup di origine e il volume FlexGroup di destinazione in una relazione SnapMirror
- Backup e ripristino di SnapVault
- Relazioni unificate per la data Protection
- Opzione di crescita automatica e opzione di riduzione automatica
- Conteggio inode conteggiato per l'acquisizione

### **Funzione supportata a partire da ONTAP 9.2**

- Crittografia dei volumi
- Deduplica aggregata inline (deduplica tra volumi)
- Crittografia dei volumi NetApp (NVE)

### **Funzionalità supportate a partire da ONTAP 9.1**

FlexGroup Volumes è stato introdotto in ONTAP 9.1, con il supporto di diverse funzionalità di ONTAP.

- Tecnologia SnapMirror
- Copie Snapshot
- Active IQ
- Compressione adattiva inline
- Deduplica inline
- Compaction dei dati inline
- AFF
- Creazione di report sulle quote
- Tecnologia Snapshot di NetApp
- Software SnapRestore (livello FlexGroup)

- Aggregati ibridi
- Spostamento del volume del componente o del membro
- Deduplica post-elaborazione
- Tecnologia NetApp RAID-TEC
- Punto di coerenza per aggregato
- Condivisione di FlexGroup con il volume FlexVol nella stessa SVM

### Configurazioni non supportate in ONTAP 9

Protocolli non supportati	Funzionalità di protezione dei dati non supportate	Altre funzioni ONTAP non supportate
<ul style="list-style-type: none"> <li>• PNFS (ONTAP da 9.0 a 9.6)</li> <li>• SMB 1.0</li> <li>• Failover trasparente SMB (da ONTAP 9.0 a 9.5)</li> <li>• SAN</li> </ul>	<ul style="list-style-type: none"> <li>• SnapLock Volumes (ONTAP 9.10.1 e versioni precedenti)</li> <li>• SMTape</li> <li>• SnapMirror sincrono</li> <li>• DR SVM con volumi FlexGroup contenenti FabricPools</li> </ul>	<ul style="list-style-type: none"> <li>• Servizio di copia shadow del volume remoto (VSS)</li> <li>• Mobilità dei dati SVM</li> </ul>

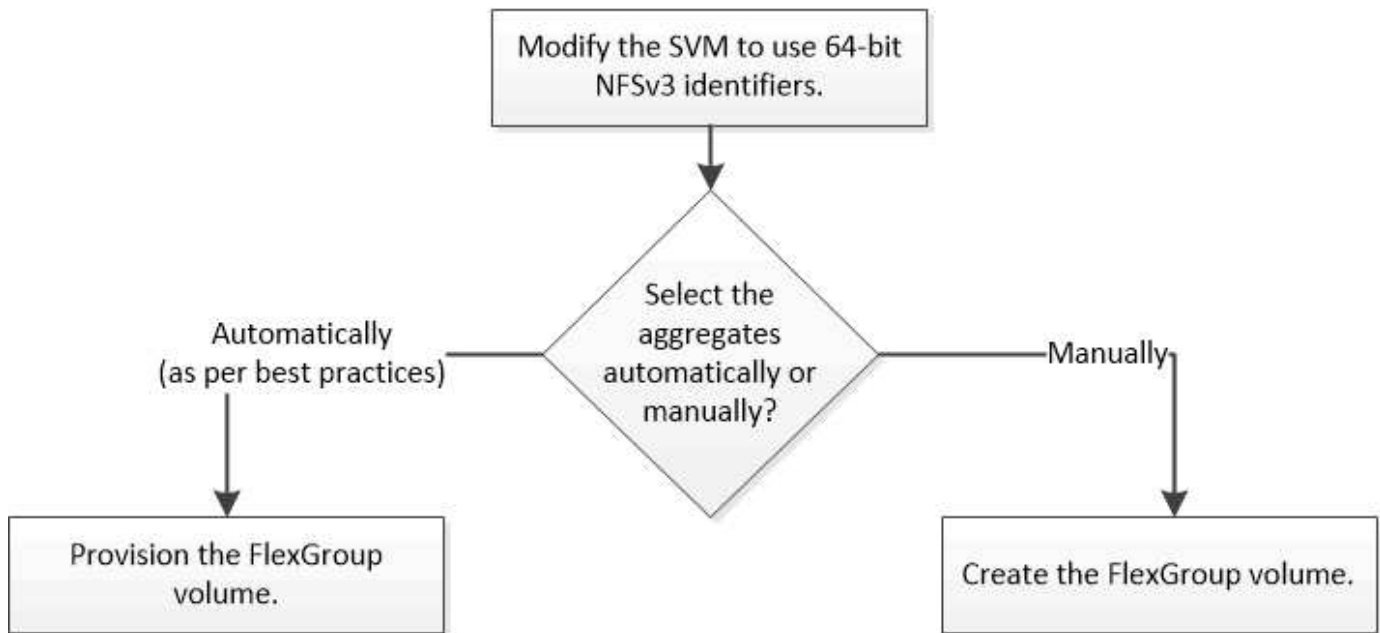
### Informazioni correlate

["Centro documentazione di ONTAP 9"](#)

## Configurazione del volume FlexGroup

### Workflow di setup del volume FlexGroup

È possibile eseguire il provisioning di un volume FlexGroup in cui ONTAP seleziona automaticamente gli aggregati in base alle Best practice per ottenere performance ottimali oppure creare un volume FlexGroup selezionando manualmente gli aggregati e configurandolo per l'accesso ai dati.



### Di cosa hai bisogno

È necessario aver creato la SVM con NFS e SMB aggiunti all'elenco dei protocolli consentiti per la SVM.

### A proposito di questa attività

È possibile eseguire il provisioning automatico di un volume FlexGroup solo su cluster con quattro nodi o meno. Nei cluster con più di quattro nodi, è necessario creare manualmente un volume FlexGroup.

### Abilitare gli identificatori NFSv3 a 64 bit su una SVM

Per supportare il numero elevato di file dei volumi FlexGroup ed evitare collisioni di ID file, è necessario attivare gli identificatori di file a 64 bit sulla SVM in cui deve essere creato il volume FlexGroup.

### Fasi

1. Accedere al livello di privilegio avanzato: `set -privilege advanced`
2. Modificare la SVM in modo che utilizzi FSID e ID file NFSv3 a 64 bit: `vserver nfs modify -vserver svm_name -v3-64bit-identifiers enabled`



```
cluster1::*> vserver nfs modify -vserver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
        FSIDs and File IDs from 32 to 64 on Vserver "vs0". This could
        result in older client software no longer working with the
volumes
        owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
        "vs0", it is highly recommended that you remount all NFSv3
clients
        connected to it after the command completes.
Do you want to continue? {y|n}: y
```

## Al termine

Tutti i client devono essere rimontati. Ciò è necessario perché gli ID del file system cambiano e i client potrebbero ricevere messaggi di gestione dei file obsoleti quando tentano le operazioni NFS.

## Provisioning automatico di un volume FlexGroup

È possibile eseguire il provisioning automatico di un volume FlexGroup. ONTAP crea e configura un volume FlexGroup selezionando automaticamente gli aggregati. Gli aggregati vengono selezionati in base alle Best practice per ottenere performance ottimali.

## Di cosa hai bisogno

Ogni nodo del cluster deve avere almeno un aggregato.



Per creare un volume FlexGroup per FabricPool in ONTAP 9.5, ciascun nodo deve disporre di almeno un aggregato FabricPool.


## A proposito di questa attività

ONTAP seleziona due aggregati con la maggiore quantità di spazio utilizzabile su ciascun nodo per creare il volume FlexGroup. Se non sono disponibili due aggregati, ONTAP seleziona un aggregato per nodo per creare il volume FlexGroup.

## Fasi

1. Provisioning del volume FlexGroup:

Se si utilizza...	Utilizzare questo comando...

ONTAP 9.2 o versione successiva	<pre>volume create -vserver svm_name -volume fg_vol_name -auto-provision-as flexgroup -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name] [-support- tiering true]</pre> <p>A partire da ONTAP 9.5, è possibile creare volumi FlexGroup per FabricPool. Per eseguire il provisioning automatico di un volume FlexGroup su FabricPool, è necessario impostare <code>-support-tiering</code> parametro a. <code>true</code>. La garanzia del volume deve essere sempre impostata su <code>none</code> Per FabricPool. È inoltre possibile specificare il criterio di tiering e il periodo minimo di raffreddamento del tiering per il volume FlexGroup.</p> <p>"Gestione di dischi e aggregati"</p> <p>A partire da ONTAP 9.3, è possibile specificare un limite massimo di throughput (QoS max) per i volumi FlexGroup, che limita le risorse di performance che il volume FlexGroup può consumare. A partire da ONTAP 9.4, è possibile specificare i livelli di throughput (QoS min) e la QoS adattiva per i volumi FlexGroup.</p> <p>"Gestione delle performance"</p> <p>A partire da ONTAP 9.2, è possibile impostare <code>-encrypt</code> parametro a. <code>true</code> Se si desidera attivare la crittografia sul volume FlexGroup. Per creare un volume crittografato, è necessario aver installato la licenza per la crittografia del volume e il gestore delle chiavi.</p> <div data-bbox="873 1402 928 1461">  </div> <p>Al momento della creazione, è necessario attivare la crittografia sui volumi FlexGroup. Non è possibile attivare la crittografia sui volumi FlexGroup esistenti.</p> <p>"Crittografia dei dati inattivi"</p>
ONTAP 9.1	<pre>volume flexgroup deploy -vserver svm_name -size fg_size</pre>

Il `size` Parametro specifica le dimensioni del volume FlexGroup in KB, MB, GB, TB o PB.

Nell'esempio seguente viene illustrato come eseguire il provisioning di un volume FlexGroup di 400 TB in ONTAP 9.2:

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

Nell'esempio seguente viene illustrato come creare un gruppo di criteri QoS per il limite di throughput e come applicarlo a un volume FlexGroup:

```
cluster1::> qos policy-group create -policy group pg-vs1 -vserver vs1
-max-throughput 5000iops
```

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

L'esempio seguente mostra come eseguire il provisioning di un volume FlexGroup di 400 TB su aggregati in FabricPool in ONTAP 9.5:

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

Il volume FlexGroup viene creato con otto componenti su ciascun nodo del cluster. I componenti sono distribuiti in modo uguale tra i due aggregati più grandi su ciascun nodo.

Per impostazione predefinita, il volume FlexGroup viene creato con `volume` Impostazione della garanzia di spazio eccetto per i sistemi AFF. Per i sistemi AFF, per impostazione predefinita il volume FlexGroup viene creato con `none` garanzia di spazio.

2. Montare il volume FlexGroup con un percorso di giunzione: `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
```

### Al termine

È necessario montare il volume FlexGroup dal client.

Se si utilizza ONTAP 9.6 o versioni precedenti e la macchina virtuale di storage (SVM) ha configurato NFSv3 e NFSv4, il montaggio del volume FlexGroup dal client potrebbe non riuscire. In questi casi, è necessario specificare esplicitamente la versione di NFS quando si monta il volume FlexGroup dal client.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
# ls /mnt/fg2
file1  file2
```

### Creare un volume FlexGroup

È possibile creare un volume FlexGroup selezionando manualmente gli aggregati in cui deve essere creato il volume FlexGroup e specificando il numero di componenti su ciascun aggregato.

#### A proposito di questa attività

È necessario conoscere lo spazio richiesto negli aggregati per la creazione di un volume FlexGroup.

Quando si crea un volume FlexGroup per ottenere i migliori risultati delle performance con un volume FlexGroup, è necessario prendere in considerazione le seguenti linee guida:

- Un volume FlexGroup deve comprendere solo aggregati che si trovano su sistemi hardware identici.

L'utilizzo di sistemi hardware identici aiuta a fornire performance prevedibili nel volume FlexGroup.

- Un volume FlexGroup deve includere aggregati con lo stesso tipo di disco e configurazioni di gruppo RAID.

Per ottenere performance costanti, è necessario assicurarsi che tutti gli aggregati siano costituiti da tutti gli SSD, tutti gli HDD o tutti gli aggregati ibridi. Inoltre, gli aggregati devono avere lo stesso numero di dischi e gruppi RAID nel volume FlexGroup.

- Un volume FlexGroup può estendersi su parti di un cluster.

Non è necessario configurare un volume FlexGroup per l'intero cluster, ma in questo modo è possibile sfruttare al meglio le risorse hardware disponibili.

- Quando si crea un volume FlexGroup, è preferibile che gli aggregati su cui viene implementato il volume FlexGroup abbiano le seguenti caratteristiche:
  - La stessa quantità di spazio libero dovrebbe essere disponibile in più aggregati, soprattutto quando si utilizza il thin provisioning.
  - Circa il 3% dello spazio libero deve essere riservato ai metadati aggregati dopo la creazione del

volume FlexGroup.

- Per i sistemi FAS, è consigliabile disporre di due aggregati per nodo e per i sistemi AFF, è necessario disporre di un aggregato per nodo per il volume FlexGroup.
- Per ogni volume FlexGroup, è necessario creare almeno otto componenti distribuiti su due o più aggregati nei sistemi FAS e su uno o più aggregati nei sistemi AFF.

### Prima di iniziare

- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilita analisi del file system](#).

### Fasi

1. Creare il volume FlexGroup: `volume create -vserver svm_name -volume flexgroup_name -aggr-list aggr1,aggr2,... -aggr-list-multiplier constituents_per_aggr -size fg_size [-encrypt true] [-qos-policy-group qos_policy_group_name]`

- Il `-aggr-list` Parametro specifica l'elenco di aggregati da utilizzare per i componenti del volume FlexGroup.

Ogni voce dell'elenco crea un costituente nell'aggregato specificato. È possibile specificare un aggregato più volte per creare più costituenti sull'aggregato.

Per ottenere performance costanti nel volume FlexGroup, tutti gli aggregati devono utilizzare lo stesso tipo di disco e le stesse configurazioni del gruppo RAID.

- Il `-aggr-list-multiplier` il parametro specifica il numero di iterazioni degli aggregati elencati con `-aggr-list` Quando si crea un volume FlexGroup.

Il valore predefinito di `-aggr-list-multiplier` il parametro è 4.

- Il `size` Parametro specifica le dimensioni del volume FlexGroup in KB, MB, GB, TB o PB.
- A partire da ONTAP 9.5, è possibile creare volumi FlexGroup per FabricPool, che utilizzano solo tutti gli aggregati SSD.

Per creare un volume FlexGroup per FabricPool, tutti gli aggregati specificati con `-aggr-list` Il parametro deve essere FabricPool. La garanzia del volume deve essere sempre impostata su `none` Per FabricPool. È inoltre possibile specificare il criterio di tiering e il periodo minimo di raffreddamento del tiering per il volume FlexGroup.

### Gestione di dischi e aggregati

- A partire da ONTAP 9.4, è possibile specificare i livelli di throughput (QoS min) e la QoS adattiva per i volumi FlexGroup.

### "Gestione delle performance"

- A partire da ONTAP 9.3, è possibile specificare un limite massimo di throughput (QoS max) per i volumi FlexGroup, che limita le risorse di performance che il volume FlexGroup può consumare.

- A partire da ONTAP 9.2, è possibile impostare `-encrypt` parametro a. `true` Se si desidera attivare la crittografia sul volume FlexGroup.

Per creare un volume crittografato, è necessario aver installato la licenza per la crittografia del volume e il gestore delle chiavi.



Al momento della creazione, è necessario attivare la crittografia sui volumi FlexGroup. Non è possibile attivare la crittografia sui volumi FlexGroup esistenti.

### "Crittografia dei dati inattivi"

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list  
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB
```

```
Warning: A FlexGroup "fg2" will be created with the following number of  
constituents of size 62.50TB: 8.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 43] Job succeeded: Successful
```

Nell'esempio precedente, per creare il volume FlexGroup per FabricPool, tutti gli aggregati (aggr1, aggr2 e aggr3) devono essere aggregati in FabricPool. Montare il volume FlexGroup con un percorso di giunzione:

```
volume mount -vserver vserver_name -volume vol_name -junction-path junction_path
```

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

### Al termine

È necessario montare il volume FlexGroup dal client.

Se si utilizza ONTAP 9.6 o versioni precedenti e la macchina virtuale di storage (SVM) ha configurato NFSv3 e NFSv4, il montaggio del volume FlexGroup dal client potrebbe non riuscire. In questi casi, è necessario specificare esplicitamente la versione di NFS quando si monta il volume FlexGroup dal client.

```
# mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2  
# ls /mnt/fg2  
file1  file2
```

### Informazioni correlate

["Report tecnico di NetApp 4571: Guida alle Best practice e all'implementazione di NetApp FlexGroup"](#)

## Gestire i volumi FlexGroup

### Monitorare l'utilizzo dello spazio di un volume FlexGroup

È possibile visualizzare un volume FlexGroup e i relativi componenti e monitorare lo

spazio utilizzato dal volume FlexGroup.

### A proposito di questa attività

A partire da ONTAP 9.6, è supportato il dimensionamento elastico. ONTAP aumenta automaticamente un componente di un volume FlexGroup se lo spazio è esaurito, riducendo di una quantità equivalente qualsiasi altro componente del volume FlexGroup che dispone di spazio libero. Il dimensionamento elastico evita gli errori di spazio insufficiente generati a causa dello spazio insufficiente di uno o più volumi costituenti FlexGroup.



A partire da ONTAP 9.9.1, è disponibile anche il reporting e l'imposizione dello spazio logico per i volumi FlexGroup. Per ulteriori informazioni, vedere ["Creazione di report e applicazione dello spazio logico per i volumi"](#).

### Fase

1. Visualizzare lo spazio utilizzato dal volume FlexGroup e dai suoi componenti: `volume show -vserver vs1 -volume-style-extended flexgroup vs1 -volume-style-extended [flexgroup | flexgroup-constituent]`

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver   Volume      Aggregate   State      Type      Size
Available Used%
-----
vs1        fg1          -           online     RW        500GB
207.5GB    56%
```

```
ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-constituent
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				

vs1	fg1__0001	aggr3	online	RW	31.25GB
12.97GB	56%				
vs1	fg1__0002	aggr1	online	RW	31.25GB
12.98GB	56%				
vs1	fg1__0003	aggr1	online	RW	31.25GB
13.00GB	56%				
vs1	fg1__0004	aggr3	online	RW	31.25GB
12.88GB	56%				
vs1	fg1__0005	aggr1	online	RW	31.25GB
13.00GB	56%				
vs1	fg1__0006	aggr3	online	RW	31.25GB
12.97GB	56%				
vs1	fg1__0007	aggr1	online	RW	31.25GB
13.01GB	56%				
vs1	fg1__0008	aggr1	online	RW	31.25GB
13.01GB	56%				
vs1	fg1__0009	aggr3	online	RW	31.25GB
12.88GB	56%				
vs1	fg1__0010	aggr1	online	RW	31.25GB
13.01GB	56%				
vs1	fg1__0011	aggr3	online	RW	31.25GB
12.97GB	56%				
vs1	fg1__0012	aggr1	online	RW	31.25GB
13.01GB	56%				
vs1	fg1__0013	aggr3	online	RW	31.25GB
12.95GB	56%				
vs1	fg1__0014	aggr3	online	RW	31.25GB
12.97GB	56%				
vs1	fg1__0015	aggr3	online	RW	31.25GB
12.88GB	56%				
vs1	fg1__0016	aggr1	online	RW	31.25GB
13.01GB	56%				

16 entries were displayed.

È possibile utilizzare lo spazio disponibile e lo spazio percentuale utilizzati per monitorare l'utilizzo dello spazio del volume FlexGroup.



## Aumentare le dimensioni di un volume FlexGroup

È possibile aumentare le dimensioni di un volume FlexGroup aggiungendo maggiore capacità ai componenti esistenti del volume FlexGroup oppure espandendo il volume FlexGroup con nuovi componenti.

### Di cosa hai bisogno

Negli aggregati deve essere disponibile uno spazio sufficiente.

### A proposito di questa attività

Se si desidera aggiungere più spazio, è possibile aumentare le dimensioni collettive del volume FlexGroup. L'aumento delle dimensioni di un volume FlexGroup ridimensiona i componenti esistenti del volume FlexGroup.

Se si desidera migliorare le prestazioni, è possibile espandere il volume FlexGroup. È possibile espandere un volume FlexGroup e aggiungere nuovi componenti nelle seguenti situazioni:

- Sono stati aggiunti nuovi nodi al cluster.
- Sono stati creati nuovi aggregati sui nodi esistenti.
- I componenti esistenti del volume FlexGroup hanno raggiunto la dimensione massima FlexVol per l'hardware, pertanto il volume FlexGroup non può essere ridimensionato.

Nelle release precedenti a ONTAP 9.3, non è necessario espandere i volumi FlexGroup dopo aver stabilito una relazione SnapMirror. Se si espande il volume FlexGroup di origine dopo l'interruzione della relazione SnapMirror nelle release precedenti a ONTAP 9.3, è necessario eseguire nuovamente un trasferimento di riferimento al volume FlexGroup di destinazione. A partire da ONTAP 9.3, è possibile espandere i volumi FlexGroup in relazione a SnapMirror.

### Fase

1. Aumentare le dimensioni del volume FlexGroup aumentando la capacità o le prestazioni del volume FlexGroup, secondo necessità:

Se si desidera aumentare...	Quindi...
Capacità del volume FlexGroup	<p>Ridimensionare i componenti del volume FlexGroup:</p> <pre>volume modify -vserver vserver_name -volume fg_name -size new_size</pre>

Performance al volume FlexGroup	<p>Espandere il volume FlexGroup aggiungendo nuovi componenti:</p> <pre>volume expand -vserver vserver_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]</pre> <p>Il valore predefinito di <code>-aggr-list-multiplier</code> il parametro è 1.</p> <p>Per espandere un volume FlexGroup per FabricPool in ONTAP 9.5, i nuovi aggregati utilizzati devono essere FabricPool.</p>
---------------------------------	---

Se possibile, aumentare la capacità di un volume FlexGroup. Se è necessario espandere un volume FlexGroup, aggiungere i componenti negli stessi multipli dei componenti del volume FlexGroup esistente per garantire prestazioni costanti. Ad esempio, se il volume FlexGroup esistente ha 16 componenti con otto componenti per nodo, è possibile espandere il volume FlexGroup esistente di 8 o 16 componenti.

## Esempi

### Esempio di aumento della capacità dei componenti esistenti

L'esempio seguente mostra come aggiungere 20 TB di spazio a un volume FlexGroup Volx:

```
cluster1::> volume modify -vserver svm1 -volume volX -size +20TB
```

Se il volume FlexGroup ha 16 componenti, lo spazio di ciascun componente viene aumentato di 1.25 TB.

### Esempio di miglioramento delle performance con l'aggiunta di nuovi componenti

Nell'esempio seguente viene illustrato come aggiungere altri due componenti al volume FlexGroup Volx:

```
cluster1::> volume expand -vserver vs1 -volume volX -aggr-list aggr1,aggr2
```

Le dimensioni dei nuovi componenti sono identiche a quelle dei componenti esistenti.

## Ridurre le dimensioni di un volume FlexGroup

A partire da ONTAP 9.6, è possibile ridimensionare un volume FlexGroup a un valore inferiore alle dimensioni correnti per liberare spazio inutilizzato dal volume. Quando si riducono le dimensioni di un volume FlexGroup, ONTAP ridimensiona automaticamente tutti i componenti FlexGroup.

### Fase

1. Controllare le dimensioni correnti del volume FlexGroup: 'Volume size -vserver *vserver\_name* -volume *fg\_name*'

2. Ridurre le dimensioni del volume FlexGroup: `volume size -vserver vservice_name -volume fg_name new_size`

Quando si specifica la nuova dimensione, è possibile specificare un valore inferiore alla dimensione corrente o un valore negativo utilizzando il segno meno (-) per ridurre la dimensione corrente del volume FlexGroup.



Se la riduzione automatica è attivata per il volume (`volume autosize`), la dimensione automatica minima viene impostata sulla nuova dimensione del volume.

Nell'esempio seguente vengono visualizzate le dimensioni correnti del volume FlexGroup denominato Volx e il volume viene ridimensionato a 10 TB:

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX 10TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

Nell'esempio seguente vengono visualizzate le dimensioni correnti del volume FlexGroup denominato Volx e le dimensioni del volume vengono ridotte di 5 TB:

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX -5TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

## Configurare i volumi FlexGroup per aumentare e ridurre automaticamente le dimensioni

A partire da ONTAP 9.3, è possibile configurare i volumi FlexGroup in modo che aumentino e diminuiscano automaticamente in base allo spazio attualmente richiesto.

### Di cosa hai bisogno

Il volume FlexGroup deve essere online.

### A proposito di questa attività

È possibile dimensionare automaticamente i volumi FlexGroup in due modalità:

- Aumentare automaticamente le dimensioni del volume (`grow` modalità)

La crescita automatica aiuta a evitare che un volume FlexGroup esaurisca lo spazio, se l'aggregato è in grado di fornire più spazio. È possibile configurare le dimensioni massime del volume. L'aumento viene

attivato automaticamente in base alla quantità di dati scritti nel volume in relazione alla quantità corrente di spazio utilizzato e alle soglie impostate.

Per impostazione predefinita, la dimensione massima a cui un volume può crescere è pari al 120% della dimensione a cui è attivata la funzione di crescita automatica. Se è necessario garantire che il volume possa crescere fino a raggiungere un valore superiore, è necessario impostare di conseguenza la dimensione massima del volume.

- Ridurre automaticamente le dimensioni del volume (`grow_shrink` modalità)

La riduzione automatica impedisce a un volume di essere più grande del necessario, liberando spazio nell'aggregato per l'utilizzo da parte di altri volumi.

La riduzione automatica può essere utilizzata solo in combinazione con la crescita automatica per soddisfare le esigenze di spazio in continua evoluzione e non è disponibile da sola. Quando la funzione di riduzione automatica è attivata, ONTAP gestisce automaticamente il comportamento di riduzione di un volume per evitare un loop infinito di operazioni di crescita automatica e di riduzione automatica.

Man mano che un volume cresce, il numero massimo di file che può contenere potrebbe aumentare automaticamente. Quando un volume viene ridotto, il numero massimo di file che può contenere rimane invariato e un volume non può essere ridotto automaticamente al di sotto delle dimensioni corrispondenti al numero massimo di file corrente. Per questo motivo, potrebbe non essere possibile ridurre automaticamente un volume fino alle dimensioni originali.

## Fase

1. Configurare il volume in modo che aumenti e riduca automaticamente le sue dimensioni: `volume autosize -vserver vs_server_name -volume vol_name -mode [grow | grow_shrink]`

È inoltre possibile specificare le dimensioni massime, le dimensioni minime e le soglie per aumentare o ridurre il volume.

Il seguente comando consente di modificare automaticamente le dimensioni di un volume chiamato `fg1`. Il volume è configurato per crescere fino a un massimo di 5 TB quando è pieno al 70%.

```
cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
-grow-threshold-percent 70
vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
```

## Eliminare rapidamente le directory sul cluster

A partire da ONTAP 9.8, è possibile utilizzare la funzionalità di *eliminazione rapida delle directory* a bassa latenza per eliminare le directory dalle condivisioni client Linux e Windows in modo asincrono (ovvero in background). Gli amministratori di cluster e SVM possono eseguire operazioni di eliminazione asincrone su volumi FlexVol e FlexGroup.

Se si utilizza una versione di ONTAP precedente a ONTAP 9.11.1, è necessario essere un amministratore del cluster o un amministratore SVM che utilizzi la modalità avanzata dei privilegi.

A partire da ONTAP 9.11.1, un amministratore dello storage può concedere diritti su un volume per consentire ai client NFS e SMB di eseguire operazioni di eliminazione asincrone. Per ulteriori informazioni, vedere ["Gestire i diritti dei client per eliminare rapidamente le directory"](#).

A partire da ONTAP 9.8, è possibile utilizzare la funzionalità di eliminazione rapida delle directory utilizzando l'interfaccia utente di ONTAP. A partire da ONTAP 9.9.1, è possibile utilizzare questa funzionalità con Gestore di sistema. Per ulteriori informazioni su questo processo, vedere ["Intraprendere azioni correttive basate sugli analytics"](#).

## System Manager

1. Fare clic su **Storage > Volumes**, quindi su **Explorer**.

Quando si passa il mouse su un file o una cartella, viene visualizzata l'opzione da eliminare. È possibile eliminare un solo oggetto alla volta.



Quando le directory e i file vengono cancellati, i nuovi valori di capacità dello storage non vengono visualizzati immediatamente.

## CLI

### Utilizzare la CLI per eseguire una rapida eliminazione della directory

1. Accedere alla modalità avanzata dei privilegi:

```
-privilege advance
```

2. Eliminare le directory su un volume FlexVol o FlexGroup:

```
volume file async-delete start -vserver vserver_name -volume volume_name  
-path file_path -throttle throttle
```

Il valore minimo dell'acceleratore è 10, il valore massimo è 100,000 e il valore predefinito è 5000.

Nell'esempio seguente viene eliminata la directory denominata d2, che si trova nella directory denominata d1.

```
cluster::*>volume file async-delete start -vserver vs1 -volume voll  
-path d1/d2
```

3. Verificare che la directory sia stata eliminata:

```
event log show
```

L'esempio seguente mostra l'output del registro eventi quando la directory viene eliminata correttamente.

```
cluster-cli::*> event log show  
Time                               Node                               Severity    Event  
-----  
MM/DD/YYYY 00:11:11  cluster-vsim      INFORMATIONAL  
asyncDelete.message.success: Async delete job on path d1/d2 of  
volume (MSID: 2162149232) was completed.
```

### Annulla un processo di eliminazione directory

1. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

2. Verificare che l'eliminazione della directory sia in corso:

```
volume file async-delete show
```

Se vengono visualizzati SVM, volume, ID lavoro e percorso della directory, è possibile annullare il lavoro.

3. Per annullare l'eliminazione della directory:

```
volume file async-delete cancel -vserver SVM_name -volume volume_name  
-jobid job_id
```

### Gestire i diritti dei client per eliminare rapidamente le directory

A partire da ONTAP 9.11.1, gli amministratori dello storage possono concedere diritti su un volume per consentire ai client NFS e SMB di eseguire autonomamente operazioni di *eliminazione rapida delle directory* a bassa latenza. Quando l'eliminazione asincrona è attivata sul cluster, gli utenti del client Linux possono utilizzare `mv`. Gli utenti di Command e Windows client possono utilizzare `rename` comando per eliminare rapidamente una directory sul volume specificato spostandola in una directory nascosta che per impostazione predefinita è denominata `.ontaptrashbin`.

#### Abilitare l'eliminazione asincrona della directory del client

##### Fasi

1. Dalla CLI del cluster, accedere alla modalità avanzata dei privilegi: `-privilege advance`
2. Abilitare l'eliminazione asincrona del client e, se lo si desidera, fornire un nome alternativo per la directory del raccoglitore:

```
volume file async-delete client enable volume volname vserver vserverName  
trashbinname name
```

Esempio di utilizzo del nome predefinito del cestino:

```
cluster1::*> volume file async-delete client enable -volume v1 -vserver  
vs0
```

```
Info: Async directory delete from the client has been enabled on volume  
"v1" in  
      Vserver "vs0".
```

Esempio di specificazione di un nome di cestino alternativo:

```
cluster1::*> volume file async-delete client enable -volume test
-trashbin .ntaptrash -vserver vs1

Success: Async directory delete from the client is enabled on volume
"v1" in
      Vserver "vs0".
```

### 3. Verificare che l'eliminazione asincrona del client sia attivata:

```
volume file async-delete client show
```

Esempio:

```
cluster1::*> volume file async-delete client show

Vserver Volume      async-delete client TrashBinName
-----
vs1         vol1         Enabled         .ntaptrash
vs2         vol2         Disabled        -

2 entries were displayed.
```

## Disattivare l'eliminazione asincrona della directory del client

### Fasi

#### 1. Dalla CLI del cluster, disattivare l'eliminazione asincrona della directory del client:

```
volume file async-delete client disable volume volname vserver vserverName
```

Esempio:

```
cluster1::*> volume file async-delete client disable -volume vol1
-vserver vs1

      Success: Asynchronous directory delete client disabled
successfully on volume.
```

#### 2. Verificare che l'eliminazione asincrona del client sia disattivata:

```
volume file async-delete client show
```

Esempio:



```
cluster1::*> volume file async-delete client show
```

Vserver	Volume	async-delete client	TrashBinName
vs1	vol1	Disabled	-
vs2	vol2	Disabled	-

```
2 entries were displayed.
```

## Creare qtree con volumi FlexGroup

A partire da ONTAP 9.3, è possibile creare qtree con volumi FlexGroup. I qtree consentono di suddividere i volumi FlexGroup in segmenti più piccoli che è possibile gestire singolarmente.

### A proposito di questa attività

- Se si desidera ripristinare ONTAP 9.2 o versioni precedenti e se sono stati creati uno o più qtree nel volume FlexGroup o modificati gli attributi (stile di protezione e oplock SMB) del qtree predefinito, È necessario eliminare tutti i qtree non predefiniti e disattivare la funzionalità qtree su ciascun volume FlexGroup prima di tornare a ONTAP 9.2 o versione precedente.

["Disattivare la funzionalità qtree nei volumi FlexGroup prima di eseguire il ripristino"](#)

- Se il volume FlexGroup di origine ha qtree in una relazione SnapMirror, il cluster di destinazione deve eseguire ONTAP 9.3 o versione successiva (una versione del software ONTAP che supporta qtree).
- A partire da ONTAP 9.5, le statistiche qtree sono supportate per i volumi FlexGroup.

### Fasi

1. Creare un qtree nel volume FlexGroup: `volume qtree create -vserver vs1 -volume volume_name -qtree qtree name`

È possibile specificare lo stile di protezione, gli oplock SMB, le autorizzazioni UNIX e i criteri di esportazione per qtree.

```
cluster1::> volume qtree create -vserver vs0 -volume fg1 -qtree qtree1  
-security-style mixed
```

### Informazioni correlate

["Gestione dello storage logico"](#)

## Utilizzare le quote per i volumi FlexGroup

In ONTAP 9.4 e versioni precedenti, è possibile applicare le regole delle quote ai volumi FlexGroup solo a scopo di reporting, ma non per l'applicazione dei limiti di quota. A partire da ONTAP 9.5, è possibile applicare limiti alle regole di quota applicate ai volumi FlexGroup.

## A proposito di questa attività

- A partire da ONTAP 9.5, è possibile specificare le quote limite hard, soft e threshold per i volumi FlexGroup.

È possibile specificare questi limiti per limitare la quantità di spazio, il numero di file che un utente, un gruppo o un qtree specifico può creare o entrambi. I limiti di quota generano messaggi di avviso nei seguenti scenari:

- Quando l'utilizzo supera un limite minimo configurato, ONTAP emette un messaggio di avviso, ma è ancora consentito ulteriore traffico.

Se in seguito l'utilizzo scende di nuovo al di sotto del limite di tolleranza configurato, viene visualizzato un messaggio di cancellazione completa.

- Quando l'utilizzo supera un limite di soglia configurato, ONTAP emette un secondo messaggio di avviso.

Non viene emesso alcun messaggio amministrativo completo quando l'utilizzo in seguito scende al di sotto di un limite di soglia configurato.

- Se l'utilizzo raggiunge un limite massimo configurato, ONTAP impedisce un ulteriore consumo di risorse rifiutando il traffico.
- In ONTAP 9.5, le regole di quota non possono essere create o attivate sul volume FlexGroup di destinazione di una relazione SnapMirror.
- Durante l'inizializzazione della quota, le quote non vengono applicate e non vengono notificate le violazioni delle quote in seguito all'inizializzazione della quota.


Per controllare se le quote sono state violate durante l'inizializzazione delle quote, è possibile utilizzare `volume quota report` comando.

## Destinazioni e tipi di quota

Le quote hanno un tipo: Possono essere utente, gruppo o albero. Le destinazioni di quota specificano l'utente, il gruppo o il qtree per cui vengono applicati i limiti di quota.

La tabella seguente elenca i tipi di target di quota, i tipi di quote a cui ciascun target di quota è associato e il modo in cui ciascun target di quota è rappresentato:

Destinazione della quota	Tipo di quota	Come viene rappresentato il target	Note
utente	quota utente	Nome utente UNIX UID UNIX  Nome utente Windows in formato precedente a Windows 2000  SID di Windows	Le quote utente possono essere applicate a un volume o qtree specifico.

gruppo	quota di gruppo	Nome del gruppo UNIX GID	<p>Le quote di gruppo possono essere applicate a un volume o qtree specifico.</p> <div>  <p>ONTAP non applica quote di gruppo basate sugli ID Windows.</p> </div>
qtree	quota ad albero	nome del qtree	Le quote ad albero vengono applicate a un particolare volume e non influiscono sui qtree di altri volumi.
""	quota di preventivi utente quota ad albero	Virgolette doppie ("" )	Una destinazione di quota di "" indica una <i>quota predefinita</i> . Per le quote predefinite, il tipo di quota è determinato dal valore del campo tipo.

#### Comportamento dei volumi FlexGroup quando vengono superati i limiti di quota

A partire da ONTAP 9.5, i limiti di quota sono supportati sui volumi FlexGroup. Esistono alcune differenze nel modo in cui i limiti di quota vengono applicati a un volume FlexGroup rispetto a un volume FlexVol.

Quando si superano i limiti di quota, i volumi FlexGroup potrebbero mostrare i seguenti comportamenti:

- L'utilizzo di spazio e file in un volume FlexGroup potrebbe superare fino al 5% il limite massimo configurato prima che venga applicato il limite di quota rifiutando ulteriore traffico.

Per ottenere le migliori prestazioni, ONTAP potrebbe consentire al consumo di spazio di superare il limite massimo configurato di un piccolo margine prima dell'inizio dell'applicazione delle quote. Questo consumo di spazio aggiuntivo non supera il 5% dei limiti rigidi configurati, 1 GB o 65536 file, a seconda del valore più basso.

- Una volta raggiunto il limite di quota, se un utente o un amministratore elimina alcuni file o directory in modo tale che l'utilizzo della quota sia ora inferiore al limite, la successiva operazione di file che consuma quote potrebbe riprendere con un ritardo (potrebbe richiedere fino a 5 secondi per la ripresa).
- Quando lo spazio totale e l'utilizzo di file di un volume FlexGroup superano i limiti di quota configurati, potrebbe verificarsi un leggero ritardo nella registrazione di un messaggio del registro eventi.
- Se alcuni componenti del volume FlexGroup si esaurono, ma non vengono raggiunti i limiti di quota, potrebbero verificarsi errori "no space".
- Le operazioni, come la ridenominazione di un file o di una directory o lo spostamento di file tra qtree, sulle destinazioni di quota per le quali sono configurati limiti rigidi di quota, potrebbero richiedere più tempo rispetto a operazioni simili sui volumi FlexVol.

## Esempi di applicazione delle quote per i volumi FlexGroup

È possibile utilizzare gli esempi per comprendere come configurare le quote con limiti in ONTAP 9.5 e versioni successive.

### Esempio 1: Applicazione di una regola di quota con limiti di disco

1. È necessario creare una regola di tipo del criterio di quota `user` con un limite di dischi `soft` e un limite di dischi rigidi raggiungibili.

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. È possibile visualizzare la regola dei criteri di quota:

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG
```

Vserver: vs0			Policy: default		Volume: FG		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
Threshold							
-----	-----	-----	-----	-----	-----	-----	-----
-----							
user	""	""	off	1TB	800GB	-	-
-							

3. Per attivare la nuova regola di quota, inizializza le quote sul volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. È possibile visualizzare le informazioni sull'utilizzo del disco e del file del volume FlexGroup utilizzando il report delle quote.

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0
```

Volume Specifier	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
FG		user	root	50GB	-	1	-	
FG		user	*	800GB	1TB	0	-	*

2 entries were displayed.

Una volta raggiunto il limite del disco rigido, la destinazione della regola del criterio di quota (in questo caso l'utente) non può scrivere più dati nei file.

## Esempio 2: Applicazione di una regola di quota per più utenti

1. È necessario creare una regola di tipo del criterio di quota `user`, in cui più utenti sono specificati nella destinazione della quota (utenti UNIX, utenti SMB o una combinazione di entrambi) e in cui la regola ha un limite di dischi rigidi e un limite di dischi rigidi raggiungibili.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit 800GB
```

2. È possibile visualizzare la regola dei criteri di quota:

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG
```

Vserver: vs0			Policy: default			Volume: FG	
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	"rdavis,ABCCORP\RobertDavis"	""	off	1TB	800GB	-	-

3. Per attivare la nuova regola di quota, inizializza le quote sul volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. È possibile verificare che lo stato della quota sia attivo:

```
cluster1::> volume quota show -vserver vs0 -volume FG
Vserver Name: vs0
Volume Name: FG
Quota State: on
Scan Status: -
Logging Messages: on
Logging Interval: 1h
Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
```

5. È possibile visualizzare le informazioni sull'utilizzo del disco e del file del volume FlexGroup utilizzando il report delle quote.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0
```

Volume	Tree	Type	ID	-----Disk-----	-----Files-----	Quota	
Specifier				Used	Limit	Used	Limit
-----	-----	-----	-----	-----	-----	-----	-----
FG		user	rdavis,ABCCORP\RobertDavis	0B	1TB	0	-
rdavis,ABCCORP\RobertDavis							

Il limite di quota viene condiviso tra tutti gli utenti elencati nella destinazione della quota.

Una volta raggiunto il limite del disco rigido, gli utenti elencati nella destinazione della quota non possono scrivere più dati nei file.

### Esempio 3: Applicazione della quota con mappatura utente attivata

1. È necessario creare una regola di tipo del criterio di quota `user`, Specificare un utente UNIX o Windows come destinazione della quota con `user-mapping` impostare su ``on`` e creare la regola con un limite di dischi rigidi e un limite di dischi rigidi raggiungibili.

La mappatura tra utenti UNIX e Windows deve essere configurata in precedenza utilizzando `vserver name-mapping create` comando.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit 800GB -user-mapping on
```

2. È possibile visualizzare la regola dei criteri di quota:

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG
```

Vserver: vs0			Policy: default		Volume: FG		
Type	Target	Qtree	User Mapping	Disk Limit	Soft Disk Limit	Files Limit	Soft Files Limit
user	rdavis	""	on	1TB	800GB	-	-

3. Per attivare la nuova regola di quota, inizializza le quote sul volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. È possibile verificare che lo stato della quota sia attivo:

```
cluster1::> volume quota show -vserver vs0 -volume FG
Vserver Name: vs0
Volume Name: FG
Quota State: on
Scan Status: -
Logging Messages: on
Logging Interval: 1h
Sub Quota Status: none
Last Quota Error Message: -
Collection of Quota Errors: -
```

5. È possibile visualizzare le informazioni sull'utilizzo del disco e del file del volume FlexGroup utilizzando il report delle quote.

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0
```

Volume	Tree	Type	ID	----Disk----		----Files-----		Quota
				Used	Limit	Used	Limit	
Specifier								
-----								
-----								
FG		user	rdavis,ABCCORP\RobertDavis	0B	1TB	0		-
rdavis								

Il limite di quota viene condiviso tra l'utente elencato nella destinazione di quota e il corrispondente utente Windows o UNIX.

Una volta raggiunto il limite del disco rigido, sia l'utente elencato nella destinazione della quota che l'utente Windows o UNIX corrispondente non possono scrivere più dati nei file.

#### Esempio 4: Verifica della dimensione del qtree quando la quota è attivata

1. È necessario creare una regola di tipo del criterio di quota `tree` e dove la regola ha sia un limite di dischi fissi che un limite di dischi fissi.

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. È possibile visualizzare la regola dei criteri di quota:

```
cluster1::> quota policy rule show -vserver vs0
```

Vserver: vs0			Policy: default			Volume: FG	
Type	Target	Qtree	User	Disk	Soft	Files	Soft
Threshold			Mapping	Limit	Disk	Limit	Files
					Limit		Limit
-----							
-----							
tree	tree_4118314302	""	-	48GB	-	20	-

3. Per attivare la nuova regola di quota, inizializza le quote sul volume:

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```



- a. È possibile visualizzare le informazioni sull'utilizzo del disco e del file del volume FlexGroup utilizzando il report delle quote.

```
cluster1:> quota report -vserver vs0
Vserver: vs0
----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit Specifier
-----
FG tree_4118314302 tree 1 30.35GB 48GB 14 20 tree_4118314302
```

Il limite di quota viene condiviso tra l'utente elencato nella destinazione di quota e il corrispondente utente Windows o UNIX.

4. Da un client NFS, utilizzare `df` per visualizzare l'utilizzo totale dello spazio, lo spazio disponibile e lo spazio utilizzato.

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
Filesystem 1M-blocks Used Available Use% Mounted on
10.53.2.189/FG-3 49152 31078 18074 63% /t/10.53.2.189/FG-3
```

Con limite massimo, l'utilizzo dello spazio viene calcolato da un client NFS come segue:

- Utilizzo totale dello spazio = limite massimo per l'albero
  - Spazio libero = limite massimo meno utilizzo dello spazio qtree senza limite massimo, l'utilizzo dello spazio viene calcolato da un client NFS come segue:
  - Utilizzo dello spazio = utilizzo della quota
  - Spazio totale = somma dell'utilizzo della quota e dello spazio fisico libero nel volume
5. Dalla condivisione SMB, utilizzare Esplora risorse per visualizzare l'utilizzo totale dello spazio, lo spazio disponibile e lo spazio utilizzato.

Da una condivisione SMB, è necessario tenere presenti le seguenti considerazioni per il calcolo dell'utilizzo dello spazio:

- Per il calcolo dello spazio totale disponibile viene preso in considerazione il limite massimo di quota utente per l'utente e il gruppo.
- Il valore minimo tra lo spazio libero della regola di quota albero, la regola di quota utente e la regola di quota gruppo viene considerato come spazio libero per la condivisione SMB.
- L'utilizzo dello spazio totale è variabile per SMB e dipende dal limite massimo che corrisponde allo spazio libero minimo tra struttura, utente e gruppo.

## Applicare regole e limiti al volume FlexGroups

### Fasi

1. Creare regole di quota per gli obiettivi:  
`volume quota policy rule create -vserver vs0 -policy-name quota_policy_of_the_rule -volume flexgroup_vol -type {tree|user|group} -target target_for_rule -qtree qtree_name [-disk-limit hard_disk_limit_size] [-file-limit hard_limit_number_of_files] [-threshold`

```
threshold_disk_limit_size] [-soft-disk-limit soft_disk_limit_size] [-soft-file-limit soft_limit_number_of_files]
```

- In ONTAP 9.2 e ONTAP 9.1, il tipo di destinazione della quota può essere solo `user` oppure `group`. Per volumi FlexGroup.

Il tipo di quota ad albero non è supportato per i volumi FlexGroup in ONTAP 9.2 e ONTAP 9.1.

- In ONTAP 9.3 e versioni successive, il tipo di destinazione della quota può essere `user`, `group`, o `tree`. Per volumi FlexGroup.
- Un percorso non è supportato come destinazione quando si creano regole di quota per i volumi FlexGroup.
- A partire da ONTAP 9.5, è possibile specificare il limite del disco rigido, il limite del disco virtuale, il limite del file soft e le quote del limite di soglia per i volumi FlexGroup.

In ONTAP 9.4 e versioni precedenti, non è possibile specificare il limite del disco, il limite del file, la soglia per il limite del disco, il limite del disco virtuale o il limite del file soft quando si creano regole di quota per i volumi FlexGroup.

Nell'esempio seguente viene illustrata la creazione di una regola di quota predefinita per il tipo di destinazione dell'utente:

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name  
quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

Nell'esempio seguente viene illustrata la creazione di una regola di quota `tree` per il `qtree` denominato `qtree1`:

```
cluster1::> volume quota policy rule create -policy-name default -vserver  
vs0 -volume fg1 -type tree -target "qtree1"
```

1. Attivare le quote per il volume FlexGroup specificato: `volume quota on -vserver svm_name -volume flexgroup_vol -foreground true`

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. Monitorare lo stato di inizializzazione della quota: `volume quota show -vserver svm_name`

I volumi FlexGroup potrebbero visualizzare `mixed` stato, che indica che tutti i volumi costituenti non sono ancora nello stesso stato.

```
cluster1::> volume quota show -vserver vs0
```

Vserver	Volume	State	Scan Status
vs0	fg1	initializing	95%
vs0	vol1	off	-

2 entries were displayed.

1. Visualizzare il report delle quote per il volume FlexGroup con le quote attive: `volume quota report -vserver svm_name -volume flexgroup_vol`

Non è possibile specificare un percorso con `volume quota report` Comando per volumi FlexGroup.

L'esempio seguente mostra la quota utente per il volume FlexGroup fg1:

```
cluster1::> volume quota report -vserver vs0 -volume fg1
Vserver: vs0
```

Quota				----Disk----		----Files----		
Volume	Tree	Type	ID	Used	Limit	Used	Limit	
Specifier								
fg1		user	*	0B	-	0	-	*
fg1		user	root	1GB	-	1	-	*

2 entries were displayed.

Nell'esempio seguente viene illustrata la quota ad albero per il volume FlexGroup fg1:

```
cluster1::> volume quota report -vserver vs0 -volume fg1
Vserver: vs0
```

Quota				----Disk----		----Files----		Quota
Volume	Tree	Type	ID	Used	Limit	Used	Limit	
Specifier								
fg1	qtree1	tree	1	68KB	-	18	-	
qtree1								
fg1		tree	*	0B	-	0	-	*

2 entries were displayed.

## Risultati

Le regole e i limiti di quota vengono applicati al volume FlexGroups.

L'utilizzo potrebbe superare fino al 5% il limite massimo configurato prima che ONTAP imprima la quota rifiutando ulteriore traffico.

## Informazioni correlate

["Comandi di ONTAP 9"](#)

## Abilitare l'efficienza dello storage su un volume FlexGroup

È possibile eseguire la deduplica e la compressione dei dati insieme o indipendentemente su un volume FlexGroup per ottenere risparmi di spazio ottimali.

### Di cosa hai bisogno

Il volume FlexGroup deve essere online.

### Fasi

1. Abilitare l'efficienza dello storage sul volume FlexGroup: `volume efficiency on -vserver svm_name -volume volume_name`

Le operazioni di efficienza dello storage sono attivate su tutti i componenti del volume FlexGroup.

Se un volume FlexGroup viene espanso dopo l'attivazione dell'efficienza dello storage sul volume, l'efficienza dello storage viene automaticamente attivata sui nuovi componenti.

2. Attivare l'efficienza dello storage richiesta sul volume FlexGroup utilizzando `volume efficiency modify` comando.

È possibile abilitare la deduplica inline, la deduplica post-processo, la compressione inline e la compressione post-processo sui volumi FlexGroup. È inoltre possibile impostare il tipo di compressione (secondaria o adattiva) e specificare una pianificazione o un criterio di efficienza per il volume FlexGroup.

3. Se non si utilizzano pianificazioni o policy di efficienza per l'esecuzione delle operazioni di efficienza dello storage, avviare l'operazione di efficienza: `volume efficiency start -vserver svm_name -volume volume_name`

Se la deduplica e la compressione dei dati sono attivate su un volume, la compressione dei dati viene eseguita inizialmente, seguita dalla deduplica. Questo comando non riesce se un'operazione di efficienza è già attiva sul volume FlexGroup.

4. Verificare le operazioni di efficienza attivate sul volume FlexGroup: `volume efficiency show -vserver svm_name -volume volume_name`

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
      Vserver Name: vs1
      Volume Name: fg1
      Volume Path: /vol/fg1
      State: Enabled
      Status: Idle
      Progress: Idle for 17:07:25
      Type: Regular
      Schedule: sun-sat@0

...

      Compression: true
      Inline Compression: true
      Incompressible Data Detection: false
      Constituent Volume: false
      Compression Quick Check File Size: 524288000
      Inline Dedupe: true
      Data Compaction: false
```

## Proteggere i volumi FlexGroup utilizzando le copie Snapshot

È possibile creare policy Snapshot che gestiscono automaticamente la creazione di copie Snapshot oppure creare manualmente copie Snapshot per volumi FlexGroup. Una copia Snapshot valida viene creata per un volume FlexGroup solo dopo che ONTAP è in grado di creare una copia Snapshot per ciascun componente del volume FlexGroup.

### A proposito di questa attività

- Se si dispone di più volumi FlexGroup associati a un criterio Snapshot, è necessario assicurarsi che le pianificazioni dei volumi FlexGroup non si sovrappongano.
- A partire da ONTAP 9.8, il numero massimo di copie Snapshot supportate su un volume FlexGroup è 1023.





A partire da ONTAP 9.8, la `volume snapshot show` Command for FlexGroup Volumes (comando per volumi Snapshot) riporta le dimensioni delle copie Snapshot utilizzando blocchi logici, invece di calcolare i blocchi di proprietà più giovani. Questo nuovo metodo di calcolo delle dimensioni potrebbe rendere la dimensione della copia Snapshot più grande rispetto ai calcoli delle versioni precedenti di ONTAP.

### Fasi

1. Creare una policy Snapshot o creare manualmente una copia Snapshot:

Se si desidera creare un...	Immettere questo comando...
-----------------------------	-----------------------------

Policy di Snapshot	<p>volume snapshot policy create</p> <div>  <p>Le pianificazioni associate alla policy Snapshot di un volume FlexGroup devono avere un intervallo superiore a 30 minuti.</p> </div> <p>Quando si crea un volume FlexGroup, il default il criterio Snapshot viene applicato al volume FlexGroup.</p>
Copia Snapshot manuale	<p>volume snapshot create</p> <div>  <p>Dopo aver creato una copia Snapshot per un volume FlexGroup, non è possibile modificare gli attributi della copia Snapshot. Se si desidera modificare gli attributi, è necessario eliminare e ricreare la copia Snapshot.</p> </div>

Quando viene creata una copia Snapshot, l'accesso del client al volume FlexGroup viene brevemente messo in modalità di disattivazione.

1. Verificare che venga creata una copia Snapshot valida per il volume FlexGroup: `volume snapshot show -volume volume_name -fields state`

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot                state
-----
fg_vs    fg      hourly.2016-08-23_0505 valid
```

2. Visualizzare le copie Snapshot per i componenti del volume FlexGroup: `volume snapshot show -is -constituent true`

```
cluster1::> volume snapshot show -is-constituent true
```

---Blocks---				
Vserver	Volume	Snapshot	Size	Total%
Used%				
-----	-----	-----	-----	-----
fg_vs	fg__0001	hourly.2016-08-23_0505	72MB	0%
27%				
	fg__0002	hourly.2016-08-23_0505	72MB	0%
27%				
	fg__0003	hourly.2016-08-23_0505	72MB	0%
27%				
...				
	fg__0016	hourly.2016-08-23_0505	72MB	0%
27%				

## Spostare i componenti di un volume FlexGroup

È possibile spostare i componenti di un volume FlexGroup da un aggregato all'altro per bilanciare il carico quando alcuni componenti sperimentano un maggior traffico. Lo spostamento dei componenti consente inoltre di liberare spazio su un aggregato per il ridimensionamento dei componenti esistenti.

### Di cosa hai bisogno

Per spostare un componente di un volume FlexGroup che si trova in una relazione SnapMirror, è necessario aver inizializzato la relazione SnapMirror.

### A proposito di questa attività

Non è possibile eseguire un'operazione di spostamento del volume durante l'espansione dei componenti del volume FlexGroup.

### Fasi

1. Identificare il componente del volume FlexGroup che si desidera spostare:

```
volume show -vserver svm_name -is-constituent true
```

```
cluster1::> volume show -vserver vs2 -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
vs2	fg1	-	online	RW	400TB
15.12TB	62%				
vs2	fg1__0001	aggr1	online	RW	25TB
8.12MB	59%				
vs2	fg1__0002	aggr2	online	RW	25TB
2.50TB	90%				
...					

## 2. Identificare un aggregato in cui è possibile spostare il costituente del volume FlexGroup:

```
volume move target-aggr show -vserver svm_name -volume vol_constituent_name
```

Lo spazio disponibile nell'aggregato selezionato deve essere maggiore della dimensione del componente del volume FlexGroup che si sta spostando.

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
```

Aggregate Name	Available Size	Storage Type
aggr2	467.9TB	hdd
node12a_aggr3	100.34TB	hdd
node12a_aggr2	100.36TB	hdd
node12a_aggr1	100.36TB	hdd
node12a_aggr4	100.36TB	hdd
5 entries were displayed.		

## 3. Verificare che il componente del volume FlexGroup possa essere spostato nell'aggregato desiderato:

```
volume move start -vserver svm_name -volume vol_constituent_name -destination  
-aggregate aggr_name -perform-validation-only true
```

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination  
-aggregate node12a_aggr3 -perform-validation-only true  
Validation succeeded.
```

## 4. Spostare il componente del volume FlexGroup:

```
volume move start -vserver svm_name -volume vol_constituent_name -destination  
-aggregate aggr_name [-allow-mixed-aggr-types {true|false}]
```

L'operazione di spostamento del volume viene eseguita come processo in background.



A partire da ONTAP 9.5, è possibile spostare i componenti del volume FlexGroup da un pool di fabric a un pool non fabric o viceversa impostando `-allow-mixed-aggr-types` parametro a `true`. Per impostazione predefinita, il `-allow-mixed-aggr-types` l'opzione è impostata su `false`.



Non è possibile utilizzare `volume move` Comando per l'attivazione della crittografia sui volumi FlexGroup.

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```



Se l'operazione di spostamento del volume non riesce a causa di un'operazione SnapMirror attiva, interrompere l'operazione SnapMirror utilizzando `snapmirror abort -h` comando. In alcuni casi, anche l'operazione di interruzione di SnapMirror potrebbe non riuscire. In tali situazioni, interrompere l'operazione di spostamento del volume e riprovare in seguito.

#### 5. Verificare lo stato dell'operazione di spostamento del volume:

```
volume move show -volume vol_constituent_name
```

Nell'esempio seguente viene illustrato lo stato di un volume costituente FlexGroup che ha completato la fase di replica e si trova nella fase di cutover dell'operazione di spostamento del volume:

```
cluster1::> volume move show -volume fg1_002
```

Vserver	Volume	State	Move Phase	Percent-Complete	Time-To-Complete
vs2	fg1_002	healthy	cutover	-	-

### Utilizza gli aggregati in FabricPool per i volumi FlexGroup esistenti

A partire da ONTAP 9.5, FabricPool è supportato per FlexGroup Volumes. Se si desidera utilizzare gli aggregati in FabricPool per i volumi FlexGroup esistenti, è possibile convertire gli aggregati in cui risiede il volume FlexGroup in aggregati in FabricPool o migrare i componenti del volume FlexGroup in aggregati in FabricPool.

#### Di cosa hai bisogno

- Il volume FlexGroup deve avere la garanzia di spazio impostata su `none`.
- Se si desidera convertire gli aggregati in cui risiede il volume FlexGroup in aggregati in FabricPool, gli aggregati devono utilizzare tutti i dischi SSD.

#### A proposito di questa attività

Se un volume FlexGroup esistente risiede in aggregati non SSD, è necessario migrare i componenti del volume FlexGroup in aggregati in FabricPool.

#### Scelte

- Per convertire gli aggregati in cui risiede il volume FlexGroup in aggregati in FabricPool, attenersi alla seguente procedura:

- a. Impostare il criterio di tiering sul volume FlexGroup esistente: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. Identificare gli aggregati su cui risiede il volume FlexGroup: `volume show -volume flexgroup_name -fields aggr-list`

```
cluster-2::> volume show -volume fg1 -fields aggr-list
vserver volume aggr-list
-----
vs1      fg1      aggr1,aggr3
```

- c. Allegare un archivio di oggetti a ciascun aggregato elencato nell'elenco aggregato: `storage aggregate object-store attach -aggregate aggregate name -name object-store-name -allow-flexgroup true`

È necessario associare tutti gli aggregati a un archivio di oggetti.

```
cluster-2::> storage aggregate object-store attach -aggregate aggr1
-object-store-name Amazon01B1
```

- Per migrare i componenti del volume FlexGroup negli aggregati in FabricPool, attenersi alla seguente procedura:

- a. Impostare il criterio di tiering sul volume FlexGroup esistente: `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

```
cluster-2::> volume modify -volume fg1 -tiering-policy auto
```

- b. Spostare ciascun componente del volume FlexGroup in un aggregato in FabricPool nello stesso cluster: `volume move start -volume constituent-volume -destination-aggregate FabricPool_aggregate -allow-mixed-aggr-types true`

È necessario spostare tutti i componenti del volume FlexGroup negli aggregati in FabricPool (nel caso in cui i componenti del volume FlexGroup si trovino su tipi di aggregati misti) e assicurarsi che tutti i componenti siano bilanciati tra i nodi del cluster.

```
cluster-2::> volume move start -volume fg1_001 -destination-aggregate
FP_aggr1 -allow-mixed-aggr-types true
```

## Informazioni correlate

"Gestione di dischi e aggregati"

### Ribilanciare i volumi FlexGroup

A partire da ONTAP 9.12.1, è possibile ribilanciare i volumi FlexGroup spostando senza interruzioni i file da un costituente in un FlexGroup a un altro costituente.

Il ribilanciamento di FlexGroup aiuta a ridistribuire la capacità quando si sviluppano squilibri nel tempo grazie all'aggiunta di nuovi file e alla crescita dei file. Dopo aver avviato manualmente l'operazione di ribilanciamento, ONTAP seleziona i file e li sposta automaticamente e senza interruzioni.



È importante tenere presente che il ribilanciamento di FlexGroup riduce le prestazioni del sistema quando un numero elevato di file viene spostato come parte di un singolo evento di ribilanciamento o su più eventi di ribilanciamento a causa della creazione di inodes multi-parte. Ogni file spostato come parte di un evento di ribilanciamento ha 2 inodes multi-parte associati a quel file. Maggiore è il numero di file con inode multiparte come percentuale del numero totale di file in un FlexGroup, maggiore sarà l'impatto sulle prestazioni. Alcuni casi di utilizzo, come una conversione da FlexVol a FlexGroup, possono portare a una quantità significativa di creazione di inode multi-parte.

Il ribilanciamento è disponibile solo quando tutti i nodi del cluster eseguono ONTAP 9.12.1 o release successive. È necessario abilitare la funzionalità dati granulare su qualsiasi volume FlexGroup che esegue l'operazione di ribilanciamento. Una volta abilitata questa funzionalità, non è possibile ripristinare ONTAP 9.11.1 e versioni precedenti a meno che non si elimini questo volume o si ripristini da una copia Snapshot creata prima dell'attivazione dell'impostazione.

A partire da ONTAP 9.14.1, ONTAP introduce un algoritmo per spostare senza interruzioni e in modo proattivo i file in volumi che hanno abilitato dati granulari senza interazione dell'utente. L'algoritmo funziona in scenari molto specifici e mirati per ridurre i colli di bottiglia delle prestazioni. Gli scenari in cui questo algoritmo potrebbe agire includono un carico di scrittura molto elevato su un particolare set di file su un nodo nel cluster o un file in continua crescita in una directory principale molto attiva.

### Considerazioni sul ribilanciamento di FlexGroup

È necessario conoscere il funzionamento del ribilanciamento di FlexGroup e il modo in cui interagisce con altre funzionalità di ONTAP.

- Conversione da FlexVol a FlexGroup

Si consiglia di *non* utilizzare il ribilanciamento automatico di FlexGroup dopo una conversione da FlexVol a FlexGroup. È invece possibile utilizzare la funzione di spostamento dei file retroattivo e disgregativo disponibile in ONTAP 9.10.1 e versioni successive, immettendo il `volume rebalance file-move` comando. Per la sintassi dei comandi, vedere `volume rebalance file-move start` pagina man.

Il ribilanciamento con la funzionalità di ribilanciamento automatico di FlexGroup può degradare le prestazioni quando si sposta un elevato numero di file, come quando si esegue una conversione da FlexVol a FlexGroup, e fino al 50-85% dei dati sul volume FlexVol viene spostato in un nuovo componente.

- Dimensione minima e massima del file

La selezione del file per il ribilanciamento automatico si basa sui blocchi salvati. La dimensione minima del file considerata per il ribilanciamento è di 100 MB per impostazione predefinita (può essere configurata a partire da 20 MB utilizzando il parametro `min-file-size` mostrato di seguito) e la dimensione massima del file

è di 100 GB.

- File nelle copie Snapshot

È possibile configurare il ribilanciamento di FlexGroup per considerare solo i file da spostare che non sono attualmente presenti in alcuna copia Snapshot. Quando si avvia il ribilanciamento, viene visualizzata una notifica se viene pianificata un'operazione di copia Snapshot in qualsiasi momento durante un'operazione di ribilanciamento.

Le copie Snapshot sono limitate se un file viene spostato e viene sottoposto a framing nella destinazione. Un'operazione di ripristino della copia Snapshot non è consentita mentre è in corso il ribilanciamento del file.

- Operazioni di SnapMirror

Il ribilanciamento di FlexGroup deve avvenire tra le operazioni pianificate di SnapMirror. Un'operazione SnapMirror potrebbe non riuscire se un file viene spostato prima dell'inizio di un'operazione SnapMirror, se tale spostamento non viene completato entro il periodo di 24 minuti. Qualsiasi nuovo trasferimento di file che inizia dopo l'avvio di un trasferimento SnapMirror non avrà esito negativo.

- Efficienza dello storage per la compressione basata su file

Con l'efficienza dello storage di compressione basato su file, il file viene decompresso prima di essere spostato a destinazione, in modo da perdere i risparmi di compressione. I risparmi di compressione vengono riottenuti dopo l'esecuzione di uno scanner in background avviato manualmente sul volume FlexGroup dopo il ribilanciamento. Tuttavia, se un file è associato a una copia Snapshot su qualsiasi volume, il file viene ignorato per la compressione.

- Deduplica

Lo spostamento dei file deduplicati può causare un maggiore utilizzo generale del volume FlexGroup. Durante il ribilanciamento dei file, vengono spostati solo i blocchi univoci nella destinazione, liberando tale capacità nell'origine. I blocchi condivisi rimangono sull'origine e vengono copiati nella destinazione. Anche se questo raggiunge l'obiettivo di ridurre la capacità utilizzata su un componente di origine quasi completo, può anche portare a un maggiore utilizzo generale sul volume FlexGroup a causa delle copie dei blocchi condivisi sulle nuove destinazioni. Ciò è possibile anche quando i file che fanno parte di una copia Snapshot vengono spostati. Il risparmio di spazio non viene riconosciuto completamente fino a quando il programma di copia Snapshot non viene riciclato e non sono più presenti copie dei file nelle copie Snapshot.

- Volumi FlexClone

Se durante la creazione di un volume FlexClone è in corso il ribilanciamento dei file, il ribilanciamento non verrà eseguito sul volume FlexClone. Il ribilanciamento sul volume FlexClone deve essere eseguito dopo la sua creazione.

- Spostamento del file

Quando un file viene spostato durante un'operazione di ribilanciamento FlexGroup, la dimensione del file viene riportata come parte della contabilità delle quote sia sui componenti di origine che di destinazione. Una volta completato lo spostamento, la contabilità delle quote torna alla normalità e la dimensione del file viene riportata solo sulla nuova destinazione.

- Protezione ransomware autonoma

A partire da ONTAP 9.13.1, la protezione autonoma da ransomware è supportata durante operazioni di

ribilanciamento senza interruzioni e con interruzioni.

- Volumi degli archivi di oggetti

Il ribilanciamento della capacità dei volumi non è supportato sui volumi degli archivi di oggetti, come i bucket S3.

### **Abilitare il ribilanciamento FlexGroup**

A partire da ONTAP 9.12.1, puoi abilitare il ribilanciamento automatico del volume FlexGroup senza interruzioni per ridistribuire i file tra costituenti di FlexGroup.

A partire da ONTAP 9.13.1, è possibile pianificare una singola operazione di ribilanciamento FlexGroup per iniziare in futuro a una data e a un'ora.

### **Prima di iniziare**


È necessario aver attivato `granular-data` Sul volume FlexGroup prima di attivare il ribilanciamento FlexGroup. È possibile abilitarla utilizzando uno dei seguenti metodi:

- Quando si crea un volume FlexGroup utilizzando `volume create` comando
- Modificando un volume FlexGroup esistente per attivare l'impostazione utilizzando `volume modify` comando
- Impostazione automatica quando si avvia il ribilanciamento FlexGroup utilizzando `volume rebalance` comando

### **Fasi**

È possibile gestire il ribilanciamento FlexGroup utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

## System Manager

1. Accedere a **Storage > Volumes** (archiviazione > volumi) e individuare il volume FlexGroup da ribilanciare.
2. Selezionare  per visualizzare i dettagli del volume.
3. Selezionare **Ribilanciamento**.
4. Nella finestra **Rebalance Volume**, modificare le impostazioni predefinite in base alle necessità.
5. Per pianificare l'operazione di ribilanciamento, selezionare **Ribilanciamento successivo** e inserire la data e l'ora.

## CLI

1. Avviare il ribilanciamento automatico: `volume rebalance start -vserver SVM_name -volume volume_name`

In alternativa, è possibile specificare le seguenti opzioni:

`[-max-runtime] <time interval>` durata massima

`[-max-threshold <percent>]` soglia massima di sbilanciamento per costituente

`[-min-threshold <percent>]` soglia minima di sbilanciamento per costituente

`[-max-file-Moves <integer>]` numero massimo di spostamenti simultanei del file per costituente

`[-min-file-size {<integer>[KB|MB|GB|TB|PB]}]` dimensione minima del file

`[-start-time <mm/dd/yyyy-00:00:00>]` Ribilancia la data e l'ora di inizio del ribilanciamento

`[-exclude-snapshot {true|false}]` Escludi i file bloccati nelle copie Snapshot


Esempio:

```
volume rebalance start -vserver vs0 -volume fg1
```

## Modificare le configurazioni di ribilanciamento FlexGroup

È possibile modificare una configurazione di ribilanciamento FlexGroup per aggiornare la soglia di squilibrio, il numero di file simultanei sposta la dimensione minima del file, il runtime massimo e per includere o escludere le copie Snapshot. Le opzioni per modificare la pianificazione del ribilanciamento FlexGroup sono disponibili a partire da ONTAP 9.13.1.

### System Manager

1. Accedere a **Storage > Volumes** (archiviazione > volumi) e individuare il volume FlexGroup da ribilanciare.
2. Selezionare  per visualizzare i dettagli del volume.
3. Selezionare **Ribilanciamento**.
4. Nella finestra **Rebalance Volume**, modificare le impostazioni predefinite in base alle necessità.

### CLI

1. Modificare il ribilanciamento automatico: `volume rebalance modify -vserver SVM_name -volume volume_name`

È possibile specificare una o più delle seguenti opzioni:

`[-max-runtime] <time interval>` durata massima

`[-max-threshold <percent>]` soglia massima di sbilanciamento per costituente

`[-min-threshold <percent>]` soglia minima di sbilanciamento per costituente

`[-max-file-Moves <integer>]` numero massimo di spostamenti simultanei del file per costituente

`[-min-file-size {<integer>[KB|MB|GB|TB|PB]}]` dimensione minima del file


`[-start-time <mm/dd/yyyy-00:00:00>]` Ribilancia la data e l'ora di inizio del ribilanciamento

`[-exclude-snapshot {true|false}]` Escludi i file bloccati nelle copie Snapshot

### Arrestare il ribilanciamento FlexGroup

Una volta attivato o pianificato il ribilanciamento FlexGroup, è possibile interromperlo in qualsiasi momento.

### System Manager

1. Accedere a **Storage > Volumes** e individuare il volume FlexGroup.
2. Selezionare  per visualizzare i dettagli del volume.
3. Selezionare **Stop Rebalance** (Interrompi ribilanciamento).


### CLI

1. Arrestare il ribilanciamento FlexGroup: `volume rebalance stop -vserver SVM_name -volume volume_name`

### Visualizzare lo stato di ribilanciamento FlexGroup

È possibile visualizzare lo stato di un'operazione di ribilanciamento FlexGroup, la configurazione di ribilanciamento FlexGroup, il tempo dell'operazione di ribilanciamento e i dettagli dell'istanza di ribilanciamento.

## System Manager

1. Accedere a **Storage > Volumes** e individuare il volume FlexGroup.
2. Selezionare  Per visualizzare i dettagli di FlexGroup.
3. **FlexGroup Balance Status** viene visualizzato nella parte inferiore del riquadro dei dettagli.
4. Per visualizzare le informazioni sull'ultima operazione di ribilanciamento, selezionare **Last Volume Rebalance Status** (ultimo stato di ribilanciamento del volume).

## CLI

1. Visualizzare lo stato di un'operazione di ribilanciamento FlexGroup: `volume rebalance show`

Esempio di stato di ribilanciamento:

```
> volume rebalance show
Vserver: vs0
```

Imbalance					Target
Volume	State	Total	Used	Used	
Size	%				
-----					
-----					
fg1	idle	4GB	115.3MB	-	
8KB	0%				

Esempio di dettagli di configurazione del ribilanciamento:

```
> volume rebalance show -config
Vserver: vs0
```

		Max	Threshold		Max
Min	Exclude				
Volume	Runtime	Min	Max	File	Moves
File Size	Snapshot				
-----					
-----					
fg1	6h0m0s	5%	20%	25	
4KB	true				

Esempio di dettagli sul tempo di ribilanciamento:



```
> volume rebalance show -time
Vserver: vs0
Volume                Start Time                Runtime
Max Runtime
-----
fgl                    Wed Jul 20 16:06:11 2022    0h1m16s
6h0m0s
```

Esempio di dettagli dell'istanza di ribilanciamento:

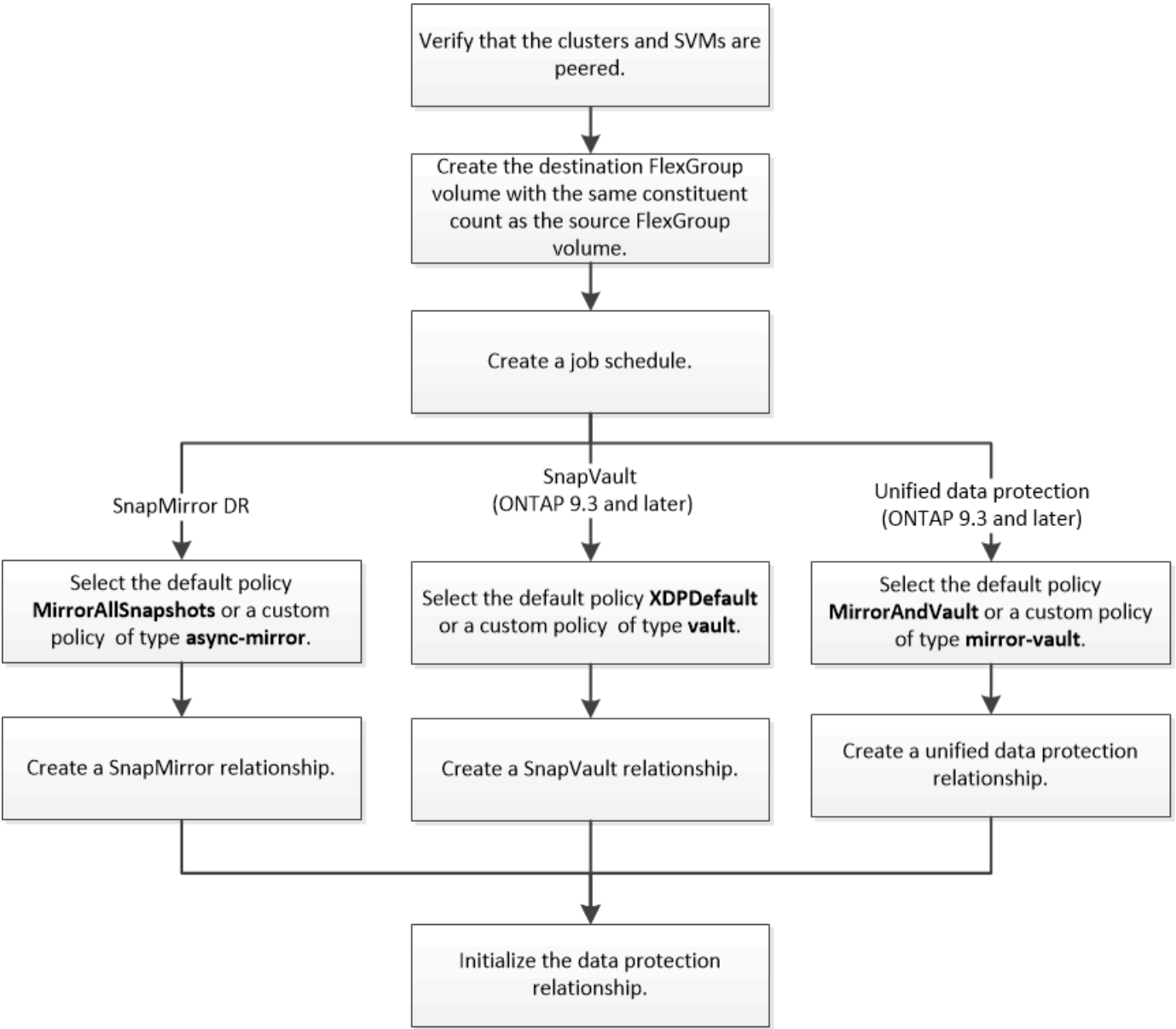
```
> volume rebalance show -instance
Vserver Name: vs0
Volume Name: fgl
Is Constituent: false
Rebalance State: idle
Rebalance Notice Messages: -
Total Size: 4GB
AFS Used Size: 115.3MB
Constituent Target Used Size: -
Imbalance Size: 8KB
Imbalance Percentage: 0%
Moved Data Size: -
Maximum Constituent Imbalance Percentage: 1%
Rebalance Start Time: Wed Jul 20 16:06:11 2022
Rebalance Stop Time: -
Rebalance Runtime: 0h1m32s
Rebalance Maximum Runtime: 6h0m0s
Maximum Imbalance Threshold per Constituent: 20%
Minimum Imbalance Threshold per Constituent: 5%
Maximum Concurrent File Moves per Constituent: 25
Minimum File Size: 4KB
Exclude Files Stuck in Snapshot Copies: true
```

## Protezione dei dati per i volumi FlexGroup

### Workflow di data Protection per FlexGroup Volumes

È possibile creare relazioni di disaster recovery (DR) di SnapMirror per i volumi FlexGroup. A partire da ONTAP 9.3, è anche possibile eseguire il backup e il ripristino dei volumi FlexGroup utilizzando la tecnologia SnapVault e creare una relazione di protezione dei dati unificata che utilizza la stessa destinazione per il backup e il DR.

Il flusso di lavoro per la protezione dei dati consiste nella verifica delle relazioni tra cluster e peer SVM, nella creazione di un volume di destinazione, nella creazione di una pianificazione dei processi, nella specifica di una policy, nella creazione di una relazione di protezione dei dati e nell’inizializzazione della relazione.



**A proposito di questa attività**

Il tipo di relazione SnapMirror è sempre XDP. Per volumi FlexGroup, il tipo di protezione dei dati fornita da una relazione SnapMirror è determinato dal criterio di replica utilizzato. È possibile utilizzare il criterio predefinito o un criterio personalizzato del tipo richiesto per la relazione di replica che si desidera creare. La tabella seguente mostra i tipi di criteri predefiniti e i tipi di criteri personalizzati supportati per diversi tipi di relazioni di protezione dei dati.

Tipo di relazione	Policy predefinita	Tipo di policy personalizzata
Dr. SnapMirror	MirrorAllSnapshot	mirror asincrono
Backup SnapVault	XDPDefault	vault

Protezione unificata dei dati	MirrorAndVault	vault mirror
-------------------------------	----------------	--------------

Il criterio MirrorLatest non è supportato con i volumi FlexGroup.

### Creare una relazione SnapMirror per i volumi FlexGroup

È possibile creare una relazione SnapMirror tra il volume FlexGroup di origine e il volume FlexGroup di destinazione su una SVM peered per la replica dei dati per il disaster recovery. È possibile utilizzare le copie mirror del volume FlexGroup per ripristinare i dati in caso di disastro.

#### Di cosa hai bisogno

È necessario aver creato la relazione di peering del cluster e la relazione di peering SVM.

#### "Peering di cluster e SVM"

#### A proposito di questa attività

- È possibile creare relazioni di SnapMirror tra cluster e relazioni di SnapMirror tra cluster per volumi FlexGroup.
- A partire da ONTAP 9.3, è possibile espandere i volumi FlexGroup in relazione a SnapMirror.

Se si utilizza una versione di ONTAP precedente a ONTAP 9.3, non è necessario espandere i volumi FlexGroup dopo aver stabilito una relazione SnapMirror; tuttavia, è possibile aumentare la capacità dei volumi FlexGroup dopo aver stabilito una relazione SnapMirror. Se si espande il volume FlexGroup di origine dopo l'interruzione della relazione SnapMirror nelle release precedenti a ONTAP 9.3, è necessario eseguire un trasferimento di riferimento al volume FlexGroup di destinazione.

#### Fasi

1. Creare un tipo di volume FlexGroup di destinazione `DP` Con lo stesso numero di componenti del volume FlexGroup di origine:
  - a. Dal cluster di origine, determinare il numero di componenti nel volume FlexGroup di origine: `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show -volume srcFG* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----	-----	-----	-----	-----	-----
vss	srcFG	-	online	RW	400TB
172.86GB	56%				
vss	srcFG__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vss	srcFG__0002	aggr1	online	RW	25TB
10.86TB	56%				
vss	srcFG__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vss	srcFG__0004	aggr1	online	RW	25TB
10.73TB	57%				
vss	srcFG__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vss	srcFG__0006	aggr1	online	RW	25TB
10.64TB	57%				
vss	srcFG__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

- b. Dal cluster di destinazione, creare un tipo di volume FlexGroup di destinazione DP Con lo stesso numero di componenti del volume FlexGroup di origine.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG
```

Warning: The FlexGroup volume "dstFG" will be created with the following number of constituents of size 25TB: 16.

Do you want to continue? {y|n}: y

[Job 766] Job succeeded: Successful

- c. Dal cluster di destinazione, verificare il numero di componenti nel volume FlexGroup di destinazione:
- ```
volume show -volume volume_name* -is-constituent true
```

```
cluster2::> volume show -volume dstFG* -is-constituent true
```

| Vserver   | Volume      | Aggregate  | State  | Type | Size  |
|-----------|-------------|------------|--------|------|-------|
| Available | Used%       |            |        |      |       |
| -----     | -----       | -----      | -----  | ---- | ----- |
| -----     | -----       |            |        |      |       |
| vsd       | dstFG       | -          | online | DP   | 400TB |
| 172.86GB  | 56%         |            |        |      |       |
| vsd       | dstFG__0001 | Aggr_cmode | online | DP   | 25GB  |
| 10.86TB   | 56%         |            |        |      |       |
| vsd       | dstFG__0002 | aggr1      | online | DP   | 25TB  |
| 10.86TB   | 56%         |            |        |      |       |
| vsd       | dstFG__0003 | Aggr_cmode | online | DP   | 25TB  |
| 10.72TB   | 57%         |            |        |      |       |
| vsd       | dstFG__0004 | aggr1      | online | DP   | 25TB  |
| 10.73TB   | 57%         |            |        |      |       |
| vsd       | dstFG__0005 | Aggr_cmode | online | DP   | 25TB  |
| 10.67TB   | 57%         |            |        |      |       |
| vsd       | dstFG__0006 | aggr1      | online | DP   | 25TB  |
| 10.64TB   | 57%         |            |        |      |       |
| vsd       | dstFG__0007 | Aggr_cmode | online | DP   | 25TB  |
| 10.63TB   | 57%         |            |        |      |       |
| ...       |             |            |        |      |       |

2. Creare una pianificazione del processo: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Per `-month`, `-dayofweek`, e. `-hour` opzioni, è possibile specificare all per eseguire il processo ogni mese, ogni giorno della settimana e ogni ora, rispettivamente.

Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` il sabato alle 3:00:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Creare una policy personalizzata di tipo `async-mirror` Per la relazione di SnapMirror: `snapmirror policy create -vserver SVM -policy snapmirror_policy -type async-mirror`

Se non si crea un criterio personalizzato, è necessario specificare `MirrorAllSnapshots Policy` per le relazioni SnapMirror.

4. Dal cluster di destinazione, creare una relazione SnapMirror tra il volume FlexGroup di origine e il volume FlexGroup di destinazione: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -policy snapmirror_policy -schedule sched_name`

Le relazioni di SnapMirror per i volumi FlexGroup devono essere di tipo XDP.

Se si specifica un valore di accelerazione per la relazione SnapMirror per il volume FlexGroup, ciascun componente utilizza lo stesso valore di accelerazione. Il valore della valvola a farfalla non è diviso tra i componenti.



Non è possibile utilizzare le etichette SnapMirror delle copie Snapshot per i volumi FlexGroup.

In ONTAP 9.4 e versioni precedenti, se il criterio non è specificato con `snapmirror create` il comando `MirrorAllSnapshots` il criterio viene utilizzato per impostazione predefinita. In ONTAP 9.5, se il criterio non è specificato con `snapmirror create` il comando `MirrorAndVault` il criterio viene utilizzato per impostazione predefinita.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly  
Operation succeeded: snapmirror create for the relationship with  
destination "vsd:dstFG".
```

5. Dal cluster di destinazione, inizializzare la relazione SnapMirror eseguendo un trasferimento di riferimento:  
`snapmirror initialize -destination-path dest_svm:dest_flexgroup`

Una volta completato il trasferimento di riferimento, il volume FlexGroup di destinazione viene aggiornato periodicamente in base alla pianificazione della relazione SnapMirror.

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG  
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```



Se è stata creata una relazione SnapMirror tra i volumi FlexGroup con il cluster di origine che esegue ONTAP 9.3 e il cluster di destinazione che esegue ONTAP 9.2 o versioni precedenti e se si creano qtree nel volume FlexGroup di origine, gli aggiornamenti di SnapMirror non vengono eseguiti. Per risolvere questo problema, è necessario eliminare tutti i qtree non predefiniti nel volume FlexGroup, disattivare la funzionalità qtree sul volume FlexGroup, quindi eliminare tutte le copie Snapshot attivate con la funzionalità qtree. Se la funzionalità qtree è attivata sui volumi FlexGroup, è necessario eseguire questi passaggi anche prima di passare da ONTAP 9.3 a una versione precedente di ONTAP. ["Disattivare la funzionalità qtree nei volumi FlexGroup prima di eseguire il ripristino"](#)

## Al termine

È necessario impostare la SVM di destinazione per l'accesso ai dati impostando le configurazioni richieste, ad esempio i LIF e i criteri di esportazione.

## Creare una relazione SnapVault per i volumi FlexGroup

È possibile configurare una relazione SnapVault e assegnare un criterio SnapVault alla relazione per creare un backup SnapVault.

## Di cosa hai bisogno

È necessario conoscere le considerazioni per la creazione di una relazione SnapVault per i volumi FlexGroup.

## Fasi

1. Creare un tipo di volume FlexGroup di destinazione DP Con lo stesso numero di componenti del volume FlexGroup di origine:

- a. Dal cluster di origine, determinare il numero di componenti nel volume FlexGroup di origine: `volume`

`show -volume volume_name* -is-constituent true`

```
cluster1::> volume show -volume src* -is-constituent true
Vserver    Volume          Aggregate      State      Type      Size
Available Used%
-----
vss        src              -              online     RW        400TB
172.86GB   56%
vss        src__0001        Aggr_cmode     online     RW        25GB
10.86TB    56%
vss        src__0002        aggr1         online     RW        25TB
10.86TB    56%
vss        src__0003        Aggr_cmode     online     RW        25TB
10.72TB    57%
vss        src__0004        aggr1         online     RW        25TB
10.73TB    57%
vss        src__0005        Aggr_cmode     online     RW        25TB
10.67TB    57%
vss        src__0006        aggr1         online     RW        25TB
10.64TB    57%
vss        src__0007        Aggr_cmode     online     RW        25TB
10.63TB    57%
...
```

- b. Dal cluster di destinazione, creare un tipo di volume FlexGroup di destinazione DP Con lo stesso numero di componenti del volume FlexGroup di origine.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dst
```

Warning: The FlexGroup volume "dst" will be created with the following number of constituents of size 25TB: 16.

Do you want to continue? {y|n}: y

[Job 766] Job succeeded: Successful

- c. Dal cluster di destinazione, verificare il numero di componenti nel volume FlexGroup di destinazione:

`volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show -volume dst* -is-constituent true
```

| Vserver   | Volume    | Aggregate  | State  | Type | Size  |
|-----------|-----------|------------|--------|------|-------|
| Available | Used%     |            |        |      |       |
| vsd       | dst       | -          | online | RW   | 400TB |
| 172.86GB  | 56%       |            |        |      |       |
| vsd       | dst__0001 | Aggr_cmode | online | RW   | 25GB  |
| 10.86TB   | 56%       |            |        |      |       |
| vsd       | dst__0002 | aggr1      | online | RW   | 25TB  |
| 10.86TB   | 56%       |            |        |      |       |
| vsd       | dst__0003 | Aggr_cmode | online | RW   | 25TB  |
| 10.72TB   | 57%       |            |        |      |       |
| vsd       | dst__0004 | aggr1      | online | RW   | 25TB  |
| 10.73TB   | 57%       |            |        |      |       |
| vsd       | dst__0005 | Aggr_cmode | online | RW   | 25TB  |
| 10.67TB   | 57%       |            |        |      |       |
| vsd       | dst__0006 | aggr1      | online | RW   | 25TB  |
| 10.64TB   | 57%       |            |        |      |       |
| vsd       | dst__0007 | Aggr_cmode | online | RW   | 25TB  |
| 10.63TB   | 57%       |            |        |      |       |
| ...       |           |            |        |      |       |

2. Creare una pianificazione del processo: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare all per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` il sabato alle 3:00:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Creare un criterio SnapVault, quindi definire una regola per il criterio SnapVault:
  - a. Creare una policy personalizzata di tipo `vault` Per la relazione SnapVault: `snapmirror policy create -vserver svm_name -policy policy_name -type vault`
  - b. Definire una regola per il criterio SnapVault che determina quali copie Snapshot vengono trasferite durante le operazioni di inizializzazione e aggiornamento: `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

Se non si crea un criterio personalizzato, è necessario specificare `XDPDefault` Policy per le relazioni SnapVault.



4. Creare una relazione SnapVault: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy XDPDefault`

In ONTAP 9.4 e versioni precedenti, se il criterio non è specificato con `snapmirror create` il comando `MirrorAllSnapshots` il criterio viene utilizzato per impostazione predefinita. In ONTAP 9.5, se il criterio non è specificato con `snapmirror create` il comando `MirrorAndVault` il criterio viene utilizzato per impostazione predefinita.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
```

5. Dal cluster di destinazione, inizializzare la relazione SnapVault eseguendo un trasferimento di riferimento: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dst  
Operation is queued: snapmirror initialize of destination "vsd:dst".
```

## Creare una relazione di protezione dei dati unificata per i volumi FlexGroup

A partire da ONTAP 9.3, è possibile creare e configurare le relazioni di protezione dei dati unificata di SnapMirror per configurare il disaster recovery e l'archiviazione sullo stesso volume di destinazione.

### Di cosa hai bisogno

Devi essere consapevole delle considerazioni per la creazione di relazioni di protezione dei dati unificate per i volumi FlexGroup.

["Considerazioni per la creazione di una relazione di backup SnapVault e di una relazione di protezione dati unificata per i volumi FlexGroup"](#)

### Fasi

1. Creare un tipo di volume FlexGroup di destinazione DP Con lo stesso numero di componenti del volume FlexGroup di origine:
  - a. Dal cluster di origine, determinare il numero di componenti nel volume FlexGroup di origine: `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show -volume srcFG* -is-constituent true
```

| Vserver   | Volume      | Aggregate  | State  | Type  | Size  |
|-----------|-------------|------------|--------|-------|-------|
| Available | Used%       |            |        |       |       |
| -----     | -----       | -----      | -----  | ----- | ----- |
| vss       | srcFG       | -          | online | RW    | 400TB |
| 172.86GB  | 56%         |            |        |       |       |
| vss       | srcFG__0001 | Aggr_cmode | online | RW    | 25GB  |
| 10.86TB   | 56%         |            |        |       |       |
| vss       | srcFG__0002 | aggr1      | online | RW    | 25TB  |
| 10.86TB   | 56%         |            |        |       |       |
| vss       | srcFG__0003 | Aggr_cmode | online | RW    | 25TB  |
| 10.72TB   | 57%         |            |        |       |       |
| vss       | srcFG__0004 | aggr1      | online | RW    | 25TB  |
| 10.73TB   | 57%         |            |        |       |       |
| vss       | srcFG__0005 | Aggr_cmode | online | RW    | 25TB  |
| 10.67TB   | 57%         |            |        |       |       |
| vss       | srcFG__0006 | aggr1      | online | RW    | 25TB  |
| 10.64TB   | 57%         |            |        |       |       |
| vss       | srcFG__0007 | Aggr_cmode | online | RW    | 25TB  |
| 10.63TB   | 57%         |            |        |       |       |
| ...       |             |            |        |       |       |

- b. Dal cluster di destinazione, creare un tipo di volume FlexGroup di destinazione DP Con lo stesso numero di componenti del volume FlexGroup di origine.

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG
```

Warning: The FlexGroup volume "dstFG" will be created with the following number of constituents of size 25TB: 16.

Do you want to continue? {y|n}: y

[Job 766] Job succeeded: Successful

- c. Dal cluster di destinazione, verificare il numero di componenti nel volume FlexGroup di destinazione:
- ```
volume show -volume volume_name* -is-constituent true
```

```
cluster2::> volume show -volume dstFG* -is-constituent true
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
-----	-----	-----	-----	-----	-----
vsd	dstFG	-	online	RW	400TB
172.86GB	56%				
vsd	dstFG__0001	Aggr_cmode	online	RW	25GB
10.86TB	56%				
vsd	dstFG__0002	aggr1	online	RW	25TB
10.86TB	56%				
vsd	dstFG__0003	Aggr_cmode	online	RW	25TB
10.72TB	57%				
vsd	dstFG__0004	aggr1	online	RW	25TB
10.73TB	57%				
vsd	dstFG__0005	Aggr_cmode	online	RW	25TB
10.67TB	57%				
vsd	dstFG__0006	aggr1	online	RW	25TB
10.64TB	57%				
vsd	dstFG__0007	Aggr_cmode	online	RW	25TB
10.63TB	57%				
...					

2. Creare una pianificazione del processo: `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

Per `-month`, `-dayofweek`, e. `-hour` opzioni, è possibile specificare all per eseguire il processo ogni mese, ogni giorno della settimana e ogni ora, rispettivamente.

Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` il sabato alle 3:00:

```
cluster1::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

3. Creare una policy personalizzata di tipo `mirror-vault`, quindi definire una regola per il criterio di mirroring e vault:
  - a. Creare una policy personalizzata di tipo `mirror-vault` per la relazione unificata sulla protezione dei dati: `snapmirror policy create -vserver svm_name -policy policy_name -type mirror-vault`
  - b. Definire una regola per la policy di mirroring e vault che determina quali copie Snapshot vengono trasferite durante le operazioni di inizializzazione e aggiornamento: `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

Se non si specifica un criterio personalizzato, il MirrorAndVault la policy viene utilizzata per relazioni di protezione dei dati unificate.

4. Creare una relazione unificata per la protezione dei dati: `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name -policy MirrorAndVault`

In ONTAP 9.4 e versioni precedenti, se il criterio non è specificato con `snapmirror create` il comando `MirrorAllSnapshots` il criterio viene utilizzato per impostazione predefinita. In ONTAP 9.5, se il criterio non è specificato con `snapmirror create` il comando `MirrorAndVault` il criterio viene utilizzato per impostazione predefinita.

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path  
vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
```

5. Dal cluster di destinazione, inizializzare la relazione di protezione dati unificata eseguendo un trasferimento di riferimento: `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG  
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

## Creare una relazione di disaster recovery SVM per i volumi FlexGroup

A partire da ONTAP 9.9.1, è possibile creare relazioni di disaster recovery SVM (DR SVM) utilizzando i volumi FlexGroup. Una relazione DR SVM offre ridondanza e capacità di ripristinare FlexGroups in caso di disastro sincronizzando e replicando la configurazione SVM e i relativi dati. Per il DR SVM è richiesta una licenza SnapMirror.

### Prima di iniziare

Non è possibile creare una relazione DR SVM FlexGroup con quanto segue.

- Esiste una configurazione FlexClone FlexGroup
- Il volume FlexGroup fa parte di una relazione a cascata
- Il volume FlexGroup fa parte di una relazione fanout e il cluster esegue una versione di ONTAP precedente a ONTAP 9.12.1. (A partire da ONTAP 9.13.1, le relazioni fanout sono supportate).

### A proposito di questa attività

- Tutti i nodi di entrambi i cluster devono eseguire la stessa versione di ONTAP del nodo su cui è stato aggiunto il supporto DR SVM (ONTAP 9.9.1 o versione successiva).
- La relazione di DR SVM tra il sito primario e quello secondario deve essere in buone condizioni e avere spazio sufficiente sulle SVM primarie e secondarie per supportare i volumi FlexGroup.
- A partire da ONTAP 9.12.1, FabricPool, FlexGroup e SVM DR possono funzionare insieme. Nelle release precedenti a ONTAP 9.12.1, due di queste funzionalità funzionavano insieme, ma non tutte e tre insieme.
- Quando si crea una relazione DR SVM FlexGroup in cui il volume FlexGroup fa parte di una relazione fanout, è necessario essere consapevoli dei seguenti requisiti:

- Il cluster di origine e di destinazione deve eseguire ONTAP 9.13.1 o versione successiva.
- Il DR di SVM con volumi FlexGroup supporta le relazioni di fanout di SnapMirror a otto siti.

Per informazioni sulla creazione di una relazione DR SVM, vedere ["Gestire la replica di SnapMirror SVM"](#).

## Fasi

1. Creare una relazione di DR SVM o utilizzare una relazione esistente.

["Replica di un'intera configurazione SVM"](#)

2. Creare un volume FlexGroup sul sito primario con il numero richiesto di componenti.

["Creazione di un volume FlexGroup"](#).

Prima di procedere, attendere la creazione di FlexGroup e di tutti i componenti.

3. Per replicare il volume FlexGroup, aggiornare la SVM nel sito secondario: `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`

È inoltre possibile verificare se esiste già un aggiornamento pianificato di SnapMirror immettendo `snapmirror show -fields schedule`

4. Dal sito secondario, verificare che la relazione SnapMirror sia corretta: `snapmirror show`

```
cluster2::> snapmirror show
```

Progress	Source	Destination	Mirror	Relationship	Total	
Last	Path	Type	Path	State	Status	Progress
Updated						Healthy
-----	-----	-----	-----	-----	-----	-----
-----	vs1:	XDP	vs1_dst:	Snapmirrored		
				Idle	-	true
						-

5. Dal sito secondario, verificare l'esistenza del nuovo volume FlexGroup e dei relativi componenti: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

Progress	Source	Destination	Mirror	Relationship	Total		
Last	Path	Type	Path	State	Status	Progress	Healthy
Updated							
-----	-----	-----	-----	-----	-----	-----	-----
-----							
vs1:	XDP	vs1_dst:	Snapmirrored				
			Idle		-	true	-
vs1:fg_src	XDP	vs1_dst:fg_src	Snapmirrored				
			Idle		-	true	-
vs1:fg_src__0001							
	XDP	vs1_dst:fg_src__0001	Snapmirrored				
			Idle		-	true	-
vs1:fg_src__0002							
	XDP	vs1_dst:fg_src__0002	Snapmirrored				
			Idle		-	true	-
vs1:fg_src__0003							
	XDP	vs1_dst:fg_src__0003	Snapmirrored				
			Idle		-	true	-
vs1:fg_src__0004							
	XDP	vs1_dst:fg_src__0004	Snapmirrored				
			Idle		-	true	-

6 entries were displayed.

### Transizione di una relazione SnapMirror FlexGroup esistente al DR SVM

È possibile creare una relazione di DR SVM di FlexGroup effettuando la transizione di una relazione SnapMirror di un volume FlexGroup esistente.

#### Di cosa hai bisogno

- La relazione di SnapMirror del volume FlexGroup è in buono stato.
- I volumi FlexGroup di origine e di destinazione hanno lo stesso nome.

#### Fasi

1. Dalla destinazione di SnapMirror, risincronizzare la relazione SnapMirror a livello di FlexGroup:  
`snapmirror resync`

2. Creare la relazione SnapMirror DR SVM di FlexGroup. Utilizzare lo stesso criterio SnapMirror configurato nelle relazioni SnapMirror del volume FlexGroup: `snapmirror create -destination-path dest_svm: -source-path src_svm: -identity-preserve true -policy MirrorAllSnapshots`



È necessario utilizzare `-identity-preserve true` opzione di `snapmirror create` quando si crea la relazione di replica.

3. Verificare che la relazione sia interrotta: `snapmirror show -destination-path dest_svm: -source-path src_svm:`

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:
```

Progress

Source		Destination	Mirror	Relationship	Total	
Last						
Path	Type	Path	State	Status	Progress	Healthy
Updated						
-----	----	-----	-----	-----	-----	-----
-----						
fg_vs:	XDP	fg_vs1_renamed:		Broken-off		
				Idle	-	true -

4. Arrestare la SVM di destinazione: `vserver stop -vserver vs_name`

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

5. Risincronizzare la relazione SnapMirror di SVM: `snapmirror resync -destination-path dest_svm: -source-path src_svm:`

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

6. Verificare che la relazione SnapMirror del livello di DR SVM raggiunga uno stato di inattività corretto: `snapmirror show -expand`
7. Verificare che la relazione di FlexGroup SnapMirror sia in buono stato: `snapmirror show`

## Convertire un volume FlexVol in un volume FlexGroup in una relazione SVM-DR

A partire da ONTAP 9.10.1, è possibile convertire un volume FlexVol in un volume FlexGroup su un'origine SVM-DR.

### Di cosa hai bisogno

- Il volume FlexVol in fase di conversione deve essere online.
- Le operazioni e le configurazioni sul volume FlexVol devono essere compatibili con il processo di conversione.

Se il volume FlexVol presenta incompatibilità e la conversione del volume viene annullata, viene generato un messaggio di errore. È possibile intraprendere azioni correttive e riprovare la conversione. Per ulteriori informazioni, vedere [Considerazioni per la conversione di volumi FlexVol in volumi FlexGroup](#)

### Fasi

1. Accedere utilizzando la modalità Advanced Privilege: `set -privilege advanced`
2. Dalla destinazione, aggiornare la relazione SVM-DR:

```
snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:
```

3. Assicurarsi che la relazione SVM-DR sia in uno stato SnapMirrored e non sia interrotta:

```
snapmirror show
```

4. Dalla SVM di destinazione, verificare che il volume FlexVol sia pronto per la conversione:

```
volume conversion start -vserver svm_name -volume vol_name -check-only true
```

Se questo comando genera errori diversi da "questo è un volume SVM-DR di destinazione", è possibile eseguire l'azione correttiva appropriata, eseguire nuovamente il comando e continuare la conversione.

5. Dalla destinazione, disattivare i trasferimenti sulla relazione SVM-DR:

```
snapmirror quiesce -destination-path dest_svm:
```

6. Avviare la conversione:

```
volume conversion start -vserver svm_name -volume vol_name
```

7. Verificare che la conversione sia riuscita:

```
volume show vol_name -fields -volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state

vserver    volume      state      volume-style-extended
-----
vs0        my_volume  online    flexgroup
```



8. Dal cluster di destinazione, riprendere i trasferimenti per la relazione:

```
snapmirror resume -destination-path dest_svm:
```

9. Dal cluster di destinazione, eseguire un aggiornamento per propagare la conversione alla destinazione:

```
snapmirror update -destination-path dest_svm:
```

10. Assicurarsi che la relazione SVM-DR sia in uno stato SnapMirrored e che non sia interrotta:

```
snapmirror show
```

11. Assicurarsi che la conversione sia avvenuta sulla destinazione:

```
volume show vol_name -fields -volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state
```

vserver	volume	state	volume-style-extended
-----	-----	-----	-----
vs0_dst	my_volume	online	flexgroup

### Considerazioni per la creazione di relazioni a cascata e fan-out di SnapMirror per FlexGroups

Durante la creazione delle relazioni di fanout e cascata di SnapMirror per i volumi FlexGroup, è necessario tenere presenti considerazioni e limitazioni relative al supporto.

#### Considerazioni per la creazione di relazioni a cascata

- Ciascuna relazione può essere una relazione tra cluster o tra cluster.
- Tutti i tipi di policy asincrone, inclusi async-mirror, mirror-vault e vault, sono supportati per entrambe le relazioni.
- Sono supportati solo i criteri di mirroring asincrono "MirrorAllSnapshot" e non "MirrorLatest".
- Sono supportati aggiornamenti simultanei delle relazioni XDP a cascata.
- Supporta la rimozione Da A a B e da B a C e la risincronizzazione Da A a C o la risincronizzazione da C a A.
- I volumi FlexGroup a e B supportano anche il fanout quando tutti i nodi eseguono ONTAP 9.9.1 o versione successiva.
- Sono supportate le operazioni di ripristino da volumi FlexGroup B o C.
- I trasferimenti sulle relazioni FlexGroup non sono supportati mentre la destinazione è l'origine di una relazione di ripristino.
- La destinazione di un ripristino FlexGroup non può essere la destinazione di altre relazioni FlexGroup.
- Le operazioni di ripristino dei file FlexGroup hanno le stesse restrizioni delle normali operazioni di ripristino di FlexGroup.
- Tutti i nodi del cluster in cui risiedono i volumi FlexGroup B e C devono eseguire ONTAP 9.9.1 o versione successiva.

- Sono supportate tutte le funzionalità di espansione e espansione automatica.
- In una configurazione a cascata, ad esempio Da A a B a C, se Da A a B e da B a C hanno diversi numeri di relazioni SnapMirror costitutive, un'operazione di interruzione dall'origine non è supportata per la relazione SnapMirror da B a C.
- System Manager non supporta le relazioni a cascata in ONTAP 9.9.1.
- Quando si converte un insieme Di relazioni FlexVol Da A a B in C in una relazione FlexGroup, è necessario convertire prima il nodo B in C Hop.
- Tutte le configurazioni a cascata di FlexGroup per le relazioni con i tipi di policy supportati da REST sono supportate anche dalle API REST nelle configurazioni FlexGroup a cascata.
- Come per le relazioni FlexVol, il collegamento a cascata FlexGroup non è supportato da `snapmirror protect` comando.

#### **Considerazioni per la creazione di relazioni fanout**

- Sono supportate due o più relazioni FlexGroup fanout, ad esempio Da A a B, Da A a C, con un massimo di 8 segmenti fanout.
- Ogni relazione può essere intercluster o intracluster.
- Sono supportati aggiornamenti simultanei per le due relazioni.
- Sono supportate tutte le funzionalità di espansione e espansione automatica.
- Se i rami fanout della relazione hanno diversi numeri di relazioni SnapMirror costitutive, un'operazione di interruzione dall'origine non è supportata per le relazioni A-B e A-C.
- Tutti i nodi del cluster in cui risiedono i FlexGroup di origine e di destinazione devono eseguire ONTAP 9.9.1 o versione successiva.
- Tutti i tipi di policy asincrone attualmente supportati per FlexGroup SnapMirror sono supportati nelle relazioni fanout.
- È possibile eseguire operazioni di ripristino da FlexGroups B a C.
- Tutte le configurazioni fanout con i tipi di policy supportati da REST sono supportate anche per le API REST nelle configurazioni fanout FlexGroup.

#### **Considerazioni per la creazione di una relazione di backup SnapVault e di una relazione di protezione dati unificata per i volumi FlexGroup**

È necessario conoscere le considerazioni per la creazione di una relazione di backup SnapVault e di una relazione unificata di protezione dei dati per i volumi FlexGroup.

- È possibile risincronizzare una relazione di backup SnapVault e una relazione di protezione dei dati unificata utilizzando `-preserve` Opzione che consente di conservare le copie Snapshot sul volume di destinazione più recenti rispetto all'ultima copia Snapshot comune.
- La conservazione a lungo termine non è supportata con i volumi FlexGroup.

La conservazione a lungo termine consente di creare copie Snapshot direttamente sul volume di destinazione senza dover memorizzare le copie Snapshot sul volume di origine.

- Il `snapshot` comando `expiry-time` L'opzione non è supportata per i volumi FlexGroup.
- L'efficienza dello storage non può essere configurata sul volume FlexGroup di destinazione di una relazione di backup SnapVault e di una relazione unificata di protezione dei dati.

- Non è possibile rinominare le copie Snapshot di una relazione di backup SnapVault e di una relazione di protezione dati unificata per i volumi FlexGroup.
- Un volume FlexGroup può essere il volume di origine di una sola relazione di backup o di ripristino.

Un volume FlexGroup non può essere l'origine di due relazioni SnapVault, due relazioni di ripristino o una relazione di backup SnapVault e una relazione di ripristino.

- Se si elimina una copia Snapshot sul volume FlexGroup di origine e si crea nuovamente una copia Snapshot con lo stesso nome, il trasferimento di aggiornamento successivo al volume FlexGroup di destinazione non riesce se il volume di destinazione ha una copia Snapshot con lo stesso nome.

Questo perché le copie Snapshot non possono essere rinominate per i volumi FlexGroup.

## Monitorare i trasferimenti di dati SnapMirror per i volumi FlexGroup

È necessario monitorare periodicamente lo stato delle relazioni di SnapMirror del volume FlexGroup per verificare che il volume FlexGroup di destinazione venga aggiornato periodicamente in base alla pianificazione specificata.

### A proposito di questa attività

È necessario eseguire questa attività dal cluster di destinazione.

### Fasi

1. Visualizzare lo stato della relazione di SnapMirror di tutte le relazioni di volume FlexGroup: `snapmirror show -relationship-group-type flexgroup`

```
cluster2::> snapmirror show -relationship-group-type flexgroup
```

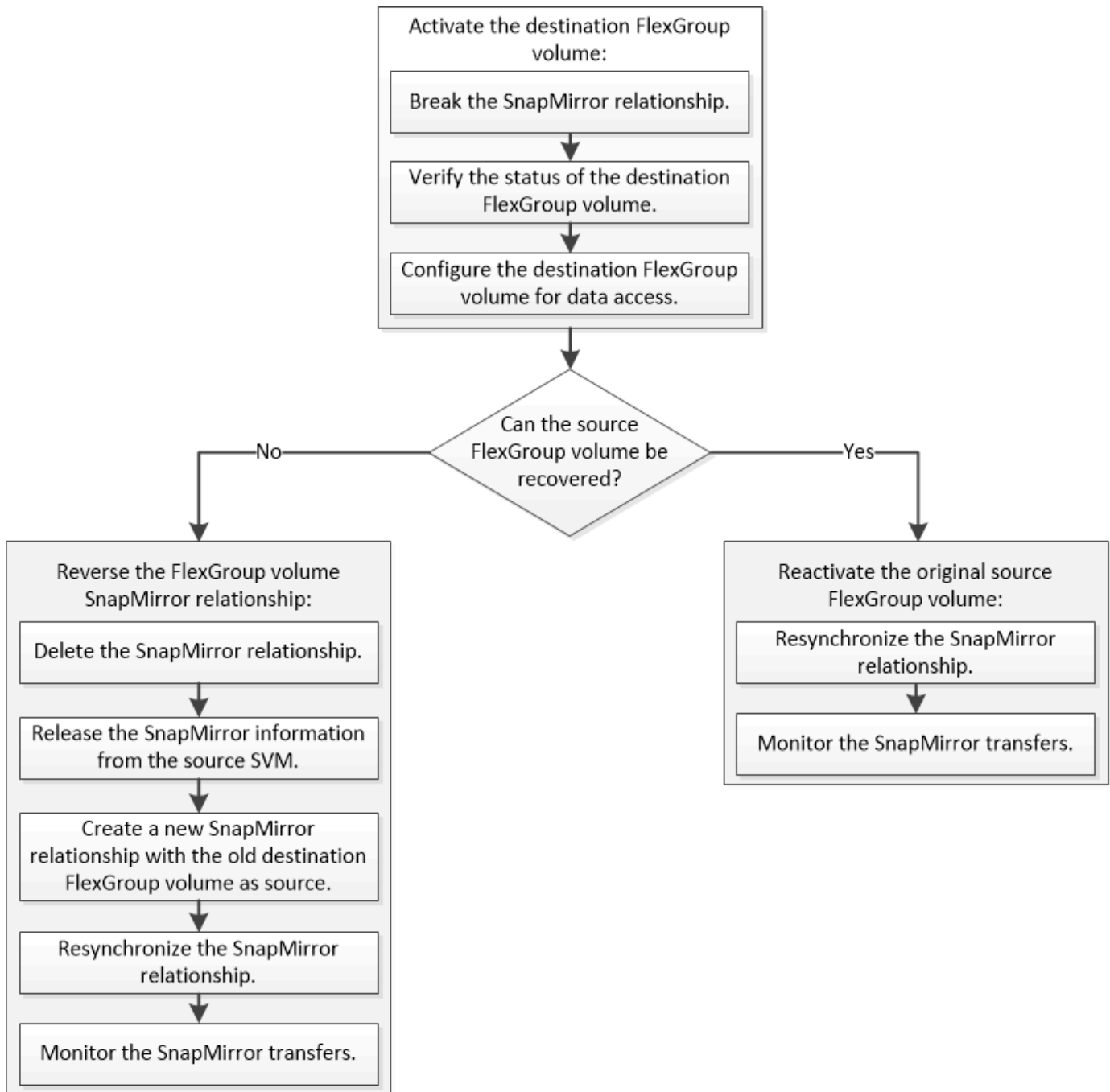
Progress	Source	Destination	Mirror	Relationship	Total	
Last	Path	Type	Path	State	Status	Progress
Updated						Healthy
-----	-----	-----	-----	-----	-----	-----
-----						
vss:s	XDP	vss:d	Snapmirrored	Idle	-	true -
vss:s2	XDP	vss:d2	Uninitialized	Idle	-	true -

2 entries were displayed.

## Gestire le operazioni di protezione dei dati per i volumi FlexGroup

### Disaster recovery per volumi FlexGroup

Quando si verifica un disastro sul volume FlexGroup di origine, è necessario attivare il volume FlexGroup di destinazione e reindirizzare l'accesso al client. A seconda che sia possibile ripristinare il volume FlexGroup di origine, è necessario riattivare il volume FlexGroup di origine o invertire la relazione di SnapMirror.



#### A proposito di questa attività

L'accesso del client al volume FlexGroup di destinazione viene bloccato per un breve periodo di tempo quando alcune operazioni di SnapMirror, ad esempio interruzione e risincronizzazione di SnapMirror, sono in esecuzione. Se l'operazione SnapMirror non riesce, è possibile che alcuni componenti rimangano in questo stato e che l'accesso al volume FlexGroup venga negato. In questi casi, è necessario ripetere l'operazione SnapMirror.

### Attivare il volume FlexGroup di destinazione

Quando il volume FlexGroup di origine non è in grado di fornire dati a causa di eventi come corruzione dei dati, eliminazione accidentale o stato offline, è necessario attivare il volume FlexGroup di destinazione per fornire l'accesso ai dati fino a quando non si ripristinino i dati sul volume FlexGroup di origine. L'attivazione comporta l'interruzione dei futuri trasferimenti di dati di SnapMirror e l'interruzione della relazione di SnapMirror.

#### A proposito di questa attività

È necessario eseguire questa attività dal cluster di destinazione.

#### Fasi

1. Disattivare i trasferimenti futuri per la relazione SnapMirror del volume FlexGroup: `snapmirror quiesce dest_svm:dest_flexgroup`

```
cluster2::> snapmirror quiesce -destination-path vsd:dst
```

2. Interrompere la relazione SnapMirror del volume FlexGroup: `snapmirror break dest_svm:dest_flexgroup`

```
cluster2::> snapmirror break -destination-path vsd:dst
```

3. Visualizzare lo stato della relazione SnapMirror: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

Progress	Source	Destination	Mirror	Relationship	Total		
Last	Path	Type	Path	State	Status	Progress	Healthy
Updated							
-----	-----	-----	-----	-----	-----	-----	-----
-----	vss:s	XDP	vsd:dst	Broken-off			
				Idle	-	true	-
	vss:s__0001	XDP	vsd:dst__0001	Broken-off			
				Idle	-	true	-
	vss:s__0002	XDP	vsd:dst__0002	Broken-off			
				Idle	-	true	-
	vss:s__0003	XDP	vsd:dst__0003	Broken-off			
				Idle	-	true	-
	vss:s__0004	XDP	vsd:dst__0004	Broken-off			
				Idle	-	true	-
	vss:s__0005	XDP	vsd:dst__0005	Broken-off			
				Idle	-	true	-
	vss:s__0006	XDP	vsd:dst__0006	Broken-off			
				Idle	-	true	-
	vss:s__0007	XDP	vsd:dst__0007	Broken-off			
				Idle	-	true	-
	vss:s__0008	XDP	vsd:dst__0008	Broken-off			
				Idle	-	true	-
...							

Lo stato della relazione SnapMirror di ciascun componente è Broken-off.

4. Verificare che il volume FlexGroup di destinazione sia in lettura/scrittura: `volume show -vserver svm_name`

```
cluster2::> volume show -vserver vsd
```

Vserver	Volume	Aggregate	State	Type	Size
Available	Used%				
vsd	dst	-	online	**RW**	2GB
1.54GB	22%				
vsd	d2	-	online	DP	2GB
1.55GB	22%				
vsd	root_vs0	aggr1	online	RW	100MB
94.02MB	5%				

3 entries were displayed.

5. Reindirizzare i client al volume FlexGroup di destinazione.

#### Riattivare il volume FlexGroup di origine originale dopo un disastro

Quando il volume FlexGroup di origine diventa disponibile, è possibile risincronizzare i volumi FlexGroup di origine e di destinazione originali. Tutti i nuovi dati presenti nel volume FlexGroup di destinazione andranno persi.

#### A proposito di questa attività

Tutte le regole di quota attive sul volume di destinazione vengono disattivate e le regole di quota vengono eliminate prima di eseguire la risincronizzazione.

È possibile utilizzare `volume quota policy rule create` e `volume quota modify` comandi per creare e riattivare le regole di quota al termine dell'operazione di risincronizzazione.

#### Fasi

1. Dal cluster di destinazione, risincronizzare la relazione SnapMirror del volume FlexGroup: `snapmirror resync -destination-path dst_svm:dest_flexgroup`
2. Visualizzare lo stato della relazione SnapMirror: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path           Type Path           State Status           Progress Healthy
Updated
-----
-----
vss:s           XDP vsd:dst           Snapmirrored
                  Idle           -           true -
vss:s__0001 XDP vsd:dst__0001 Snapmirrored
                  Idle           -           true -
vss:s__0002 XDP vsd:dst__0002 Snapmirrored
                  Idle           -           true -
vss:s__0003 XDP vsd:dst__0003 Snapmirrored
                  Idle           -           true -
vss:s__0004 XDP vsd:dst__0004 Snapmirrored
                  Idle           -           true -
vss:s__0005 XDP vsd:dst__0005 Snapmirrored
                  Idle           -           true -
vss:s__0006 XDP vsd:dst__0006 Snapmirrored
                  Idle           -           true -
vss:s__0007 XDP vsd:dst__0007 Snapmirrored
                  Idle           -           true -
vss:s__0008 XDP vsd:dst__0008 Snapmirrored
                  Idle           -           true -
...
```

Lo stato della relazione SnapMirror di ciascun componente è Snapmirrored.

#### Invertire una relazione di SnapMirror tra i volumi FlexGroup durante il disaster recovery

Quando un disastro disattiva il volume FlexGroup di origine di una relazione SnapMirror, è possibile utilizzare il volume FlexGroup di destinazione per fornire i dati durante la riparazione o la sostituzione del volume FlexGroup di origine. Una volta online il volume FlexGroup di origine, è possibile impostare il volume FlexGroup di origine come destinazione di sola lettura e invertire la relazione di SnapMirror.

#### A proposito di questa attività

Tutte le regole di quota attive sul volume di destinazione vengono disattivate e le regole di quota vengono eliminate prima di eseguire la risincronizzazione.

È possibile utilizzare `volume quota policy rule create` e `volume quota modify` comandi per creare e riattivare le regole di quota al termine dell'operazione di risincronizzazione.



## Fasi

1. Sul volume FlexGroup di destinazione originale, rimuovere la relazione del mirror di protezione dei dati tra il volume FlexGroup di origine e il volume FlexGroup di destinazione: `snapmirror delete -destination-path svm_name:volume_name`

```
cluster2::> snapmirror delete -destination-path vsd:dst
```

2. Sul volume FlexGroup di origine, rimuovere le informazioni sulle relazioni dal volume FlexGroup di origine: `snapmirror release -destination-path svm_name:volume_name -relationship-info -only`

Dopo aver eliminato una relazione SnapMirror, è necessario rimuovere le informazioni sulla relazione dal volume FlexGroup di origine prima di tentare un'operazione di risincronizzazione.

```
cluster1::> snapmirror release -destination-path vsd:dst -relationship  
-info-only true
```

3. Sul nuovo volume FlexGroup di destinazione, creare la relazione mirror: `snapmirror create -source -path src_svm_name:volume_name -destination-path dst_svm_name:volume_name -type XDP -policy MirrorAllSnapshots`

```
cluster1::> snapmirror create -source-path vsd:dst -destination-path  
vss:src -type XDP -policy MirrorAllSnapshots
```

4. Sul nuovo volume FlexGroup di destinazione, risincronizzare il FlexGroup di origine: `snapmirror resync -source-path svm_name:volume_name`

```
cluster1::> snapmirror resync -source-path vsd:dst
```

5. Monitorare i trasferimenti SnapMirror: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path            Type Path            State Status Progress Healthy
Updated
-----
-----
vsd:dst          XDP  vss:src          Snapmirrored
                  Idle          -          true  -
vss:dst__0001 XDP  vss:src__0001 Snapmirrored
                  Idle          -          true  -
vss:dst__0002 XDP  vss:src__0002 Snapmirrored
                  Idle          -          true  -
vss:dst__0003 XDP  vss:src__0003 Snapmirrored
                  Idle          -          true  -
vss:dst__0004 XDP  vss:src__0004 Snapmirrored
                  Idle          -          true  -
vss:dst__0005 XDP  vss:src__0005 Snapmirrored
                  Idle          -          true  -
vss:dst__0006 XDP  vss:src__0006 Snapmirrored
                  Idle          -          true  -
vss:dst__0007 XDP  vss:src__0007 Snapmirrored
                  Idle          -          true  -
vss:dst__0008 XDP  vss:src__0008 Snapmirrored
                  Idle          -          true  -
...
```

Lo stato della relazione SnapMirror di ciascun componente viene visualizzato come Snapmirrored ciò indica che la risincronizzazione è stata eseguita correttamente.

## Espandere i volumi FlexGroup in una relazione SnapMirror

### Espandere i volumi FlexGroup in una relazione SnapMirror

A partire da ONTAP 9.3, è possibile espandere il volume FlexGroup di origine e il volume FlexGroup di destinazione che si trovano in una relazione SnapMirror aggiungendo nuovi componenti ai volumi. È possibile espandere i volumi di destinazione manualmente o automaticamente.

#### A proposito di questa attività

- Dopo l'espansione, il numero di componenti nel volume FlexGroup di origine e nel volume FlexGroup di destinazione di una relazione SnapMirror deve corrispondere.

Se il numero di componenti nei volumi non corrisponde, i trasferimenti SnapMirror non vengono effettuati.

- Non eseguire alcuna operazione SnapMirror quando il processo di espansione è in corso.
- Se si verifica un disastro prima del completamento del processo di espansione, è necessario interrompere la relazione SnapMirror e attendere che l'operazione abbia esito positivo.



Quando il processo di espansione è in corso solo in caso di disastro, si consiglia di interrompere la relazione di SnapMirror. In caso di disastro, il completamento dell'operazione di interruzione può richiedere del tempo. Prima di eseguire un'operazione di risincronizzazione, attendere il completamento dell'operazione di interruzione. Se l'operazione di interruzione non riesce, riprovare l'operazione di interruzione. Se l'operazione di interruzione non riesce, alcuni dei nuovi componenti potrebbero rimanere nel volume FlexGroup di destinazione dopo l'operazione di interruzione. Si consiglia di eliminare questi elementi costitutivi manualmente prima di procedere ulteriormente.

#### Espandere il volume FlexGroup di origine di una relazione SnapMirror

A partire da ONTAP 9.3, è possibile espandere il volume FlexGroup di origine di una relazione SnapMirror aggiungendo nuovi componenti al volume di origine. È possibile espandere il volume di origine nello stesso modo in cui si espande un normale volume FlexGroup (volume di lettura/scrittura).

#### Fasi

1. Espandere il volume FlexGroup di origine: `volume expand -vserver vs_server_name -volume fg_src -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_src
```

```
Warning: The following number of constituents of size 50GB will be added
to FlexGroup "src_fg": 2.
```

```
Expanding the FlexGroup will cause the state of all Snapshot copies to
be set to "partial".
```

```
Partial Snapshot copies cannot be restored.
```

```
Do you want to continue? {y|n}: Y
```

```
[Job 146] Job succeeded: Successful
```

Lo stato di tutte le copie Snapshot eseguite prima dell'espansione del volume diventa parziale.

#### Espandere il volume FlexGroup di destinazione di una relazione SnapMirror

È possibile espandere il volume FlexGroup di destinazione e ristabilire la relazione SnapMirror automaticamente o manualmente. Per impostazione predefinita, la relazione di SnapMirror è impostata per l'espansione automatica e il volume FlexGroup di destinazione si espande automaticamente se il volume di origine si espande.

#### Di cosa hai bisogno

- Il volume FlexGroup di origine deve essere stato espanso.

- La relazione di SnapMirror deve essere in `SnapMirrored` stato.

La relazione di SnapMirror non deve essere interrotta o eliminata.

### A proposito di questa attività

- Quando viene creato il volume FlexGroup di destinazione, il volume viene impostato per l'espansione automatica per impostazione predefinita.

Se necessario, è possibile modificare il volume FlexGroup di destinazione per l'espansione manuale.



La procedura consigliata consiste nell'espandere automaticamente il volume FlexGroup di destinazione.

- Tutte le operazioni di SnapMirror non riescono fino a quando sia il volume FlexGroup di origine che il volume FlexGroup di destinazione non si sono espansi e hanno lo stesso numero di componenti.
- Se si espande il volume FlexGroup di destinazione dopo che la relazione SnapMirror è stata interrotta o eliminata, non è possibile risincronizzare la relazione originale.

Se si intende riutilizzare il volume FlexGroup di destinazione, non è necessario espandere il volume dopo aver eliminato la relazione SnapMirror.

### Scelte

- Eseguire un trasferimento di aggiornamento per espandere automaticamente il volume FlexGroup di destinazione:
  - a. Eseguire un trasferimento di aggiornamento di SnapMirror: `snapmirror update -destination -path svm:vol_name`
  - b. Verificare che lo stato della relazione SnapMirror sia in `SnapMirrored` stato: `snapmirror show`

```
cluster2::> snapmirror show
```

```
Progress
Source          Destination Mirror Relationship Total
Last
Path            Type Path            State Status Progress
Healthy Updated
-----
vs_src:src_fg
                XDP vs_dst:dst_fg
                                Snapmirrored
                                Idle           -      true
-
```

In base alle dimensioni e alla disponibilità degli aggregati, gli aggregati vengono selezionati automaticamente e i nuovi componenti che corrispondono ai componenti del volume FlexGroup di origine vengono aggiunti al volume FlexGroup di destinazione. Dopo l'espansione, viene attivata automaticamente

un'operazione di risincronizzazione.

- Espandere manualmente il volume FlexGroup di destinazione:

- a. Se la relazione di SnapMirror è in modalità di espansione automatica, impostare la relazione di SnapMirror sulla modalità di espansione manuale: `snapmirror modify -destination-path svm:vol_name -is-auto-expand-enabled false`

```
cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
-auto-expand-enabled false
Operation succeeded: snapmirror modify for the relationship with
destination "vs_dst:dst_fg".
```

- b. Interrompere la relazione di SnapMirror: `snapmirror quiesce -destination-path svm:vol_name`

```
cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
Operation succeeded: snapmirror quiesce for destination
"vs_dst:dst_fg".
```

- c. Espandere il volume FlexGroup di destinazione: `volume expand -vserver vs_server_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

- d. Risincronizzare la relazione SnapMirror: `snapmirror resync -destination-path svm:vol_name`

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

- e. Verificare che lo stato della relazione SnapMirror sia SnapMirrored: `snapmirror show`

```
cluster2::> snapmirror show
```

Progress	Source	Destination	Mirror	Relationship	Total	
Last	Path	Type	Path	State	Status	Progress
Healthy	Updated					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
vs_src:src_fg		XDP	vs_dst:dst_fg			
				Snapmirrored		
				Idle	-	true
-						

## Eseguire un ripristino di un singolo file SnapMirror da un volume FlexGroup

A partire da ONTAP 9.8, è possibile ripristinare un singolo file da un vault di FlexGroup SnapMirror o da una destinazione UDP.

### A proposito di questa attività

- È possibile eseguire il ripristino da un volume FlexGroup di qualsiasi geometria su un volume FlexGroup di qualsiasi geometria
- È supportato un solo file per operazione di ripristino
- È possibile eseguire il ripristino sul volume FlexGroup di origine originale o su un nuovo volume FlexGroup
- La ricerca remota dei file recintati non è supportata.

Il ripristino di un singolo file non riesce se il file di origine è protetto.

- È possibile riavviare o ripulire un ripristino di un singolo file interrotto
- È necessario eliminare un singolo trasferimento di ripristino del file non riuscito utilizzando `clean-up-failure` opzione di `snapmirror restore` comando
- L'espansione dei volumi FlexGroup è supportata quando è in corso un ripristino di un singolo file FlexGroup o in uno stato interrotto

### Fasi

1. Ripristinare un file da un volume FlexGroup: `snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot snapshot`

Di seguito viene riportato un esempio di operazione di ripristino di un singolo file del volume FlexGroup.

```
vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072ce1-d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631
```

```
[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for
the snapshot snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631.
vserverA::> snapmirror show
```

Source	Destination	Mirror	Relationship
Total Last			
Path	Type	Path	State
Healthy	Updated		Status
Progress			
-----	-----	-----	-----
-----	-----	-----	-----
vs0:v1d	RST	vs0:v2	-
true	09/19 11:38:42		Transferring Idle 83.12KB

```
vserverA::*> snapmirror show vs0:fg2
```

```
Source Path: vs0:fgd
Source Cluster: -
Source Vserver: vs0
Source Volume: fgd
Destination Path: vs0:fg2
Destination Cluster: -
Destination Vserver: vs0
Destination Volume: fg2
Relationship Type: RST
Relationship Group Type: none
Managing Vserver: vs0
SnapMirror Schedule: -
SnapMirror Policy Type: -
SnapMirror Policy: -
Tries Limit: -
Throttle (KB/sec): unlimited
Current Transfer Throttle (KB/sec): 2
Mirror State: -
Relationship Status: Transferring
File Restore File Count: 1
File Restore File List: f1
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631
Snapshot Progress: 2.87MB
Total Progress: 2.87MB
Network Compression Ratio: 1:1
Snapshot Checkpoint: 2.97KB
Newest Snapshot: -
Newest Snapshot Timestamp: -
Exported Snapshot: -
```

```
Exported Snapshot Timestamp: -
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
Relationship Capability: 8.2 and above
Lag Time: -
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
Is Catalog Enabled: false
```

### Ripristinare un volume FlexGroup da un backup SnapVault

È possibile eseguire un'operazione di ripristino completo dei volumi FlexGroup da una copia Snapshot nel volume secondario SnapVault. È possibile ripristinare il volume



FlexGroup sul volume di origine originale o su un nuovo volume FlexGroup.

### Prima di iniziare

È necessario tenere presente alcune considerazioni quando si esegue il ripristino dai backup di SnapVault per i volumi FlexGroup.

- Solo il ripristino baseline è supportato con copie Snapshot parziali da un backup SnapVault. Il numero di componenti nel volume di destinazione deve corrispondere al numero di componenti nel volume di origine quando è stata eseguita la copia Snapshot.
- Se un'operazione di ripristino non riesce, non sono consentite altre operazioni fino al completamento dell'operazione di ripristino. È possibile riprovare l'operazione di ripristino o eseguirlo con `cleanup` parametro.
- Un volume FlexGroup può essere il volume di origine di una sola relazione di backup o di ripristino. Un volume FlexGroup non può essere l'origine di due relazioni SnapVault, due relazioni di ripristino o una relazione SnapVault e una relazione di ripristino.
- Le operazioni di backup e ripristino di SnapVault non possono essere eseguite in parallelo. Quando è in corso un'operazione di ripristino di base o un'operazione di ripristino incrementale, è necessario interrompere le operazioni di backup.
- È necessario interrompere un'operazione di ripristino di una copia Snapshot parziale dal volume FlexGroup di destinazione. Non è possibile interrompere l'operazione di ripristino di una copia Snapshot parziale dal volume di origine.
- Se si interrompe un'operazione di ripristino, è necessario riavviare l'operazione di ripristino con la stessa copia Snapshot utilizzata per l'operazione di ripristino precedente.

### A proposito di questa attività

Tutte le regole di quota attive sul volume FlexGroup di destinazione vengono disattivate prima di eseguire il ripristino.

È possibile utilizzare `volume quota modify` comando per riattivare le regole di quota al termine dell'operazione di ripristino.

### Fasi

1. Ripristinare il volume FlexGroup: `snapmirror restore -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -snapshot snapshot_name`  
`snapshot_name` È la copia Snapshot che deve essere ripristinata dal volume di origine al volume di destinazione. Se la copia Snapshot non viene specificata, il volume di destinazione viene ripristinato dall'ultima copia Snapshot.

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

### Disattiva la protezione SVM su un volume FlexGroup

Quando il flag DR SVM è impostato su `protected` Su un volume FlexGroup, è possibile impostare il flag su `UnProtected` (non protetto) per disattivare il DR SVM `protection` Su

un volume FlexGroup.

#### Di cosa hai bisogno

- La relazione di DR SVM tra primario e secondario è buona.
- Il parametro di protezione DR SVM è impostato su `protected`.

#### Fasi

1. Disattivare la protezione utilizzando `volume modify` per modificare il comando `vserver-dr-protection` Parametro per il volume FlexGroup a. `unprotected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Aggiornare la SVM nel sito secondario: `snapmirror update -destination-path destination_svm_name: -source-path Source_svm_name:`
3. Verificare che la relazione di SnapMirror sia corretta: `snapmirror show`
4. Verificare che la relazione di FlexGroup SnapMirror sia stata rimossa: `snapmirror show -expand`

#### Abilitare la protezione SVM su un volume FlexGroup

Quando il flag di protezione DR SVM è impostato su `unprotected` Su un volume FlexGroup, è possibile impostare il flag su `protected` Per attivare la protezione DR SVM.

#### Di cosa hai bisogno

- La relazione di DR SVM tra primario e secondario è buona.
- Il parametro di protezione DR SVM è impostato su `unprotected`.

#### Fasi

1. Attivare la protezione utilizzando `volume modify` per modificare il `vserver-dr-protection` Parametro per il volume FlexGroup a. `protected`.

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. Aggiornare la SVM nel sito secondario: `snapmirror update -destination-path destination_svm_name -source-path source_svm_name`

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. Verificare che la relazione di SnapMirror sia corretta: `snapmirror show`

```
cluster2::> snapmirror show
```

Progress

Source	Destination	Mirror	Relationship	Total
--------	-------------	--------	--------------	-------

Last

Path	Type	Path	State	Status	Progress	Healthy
------	------	------	-------	--------	----------	---------

Updated

-----

-----

vs1:	XDP	vs1_dst:	Snapmirrored			
			Idle		-	true -

4. Verificare che la relazione di FlexGroup SnapMirror sia corretta: `snapmirror show -expand`

```
cluster2::> snapmirror show -expand
```

Progress	Source	Destination	Mirror	Relationship	Total		
Last	Path	Type	Path	State	Status	Progress	Healthy
Updated							
-----	----	-----	-----	-----	-----	-----	-----
	vs1:	XDP	vs1_dst:	Snapmirrored			
				Idle		-	true -
	vs1:fg_src	XDP	vs1_dst:fg_src	Snapmirrored			
				Idle		-	true -
	vs1:fg_src__0001						
		XDP	vs1_dst:fg_src__0001	Snapmirrored			
				Idle		-	true -
	vs1:fg_src__0002						
		XDP	vs1_dst:fg_src__0002	Snapmirrored			
				Idle		-	true -
	vs1:fg_src__0003						
		XDP	vs1_dst:fg_src__0003	Snapmirrored			
				Idle		-	true -
	vs1:fg_src__0004						
		XDP	vs1_dst:fg_src__0004	Snapmirrored			
				Idle		-	true -

6 entries were displayed.

## Converti volumi FlexVol in volumi FlexGroup

### Panoramica sulla conversione dei volumi FlexVol in volumi FlexGroup

Se si desidera espandere un volume FlexVol oltre il limite di spazio, è possibile convertire il volume FlexVol in un volume FlexGroup. A partire da ONTAP 9.7, è possibile convertire volumi FlexVol o FlexVol standalone in relazione a SnapMirror in volumi FlexGroup.

### Considerazioni per la conversione di volumi FlexVol in volumi FlexGroup

Prima di decidere di convertire i volumi FlexVol in volumi FlexGroup, è necessario conoscere le funzionalità e le operazioni supportate.

A partire da ONTAP 9.13.1, la protezione ransomware autonoma può rimanere attivata durante le conversioni.

Se la protezione è attiva, il FlexVol originale diventerà il costituente root di FlexGroup dopo la conversione. Se la protezione non è attiva, durante la conversione viene creato un nuovo FlexGroup e il FlexVol originale assume il ruolo di costituente root.

#### **Operazioni non supportate durante la conversione**

Le seguenti operazioni non sono consentite quando è in corso la conversione del volume:

- Spostamento del volume
- Autobalance dell'aggregato
- Ricollocazione di aggregati
- Takeover e giveback pianificati in una configurazione ad alta disponibilità
- Giveback manuale e automatico in una configurazione ad alta disponibilità
- Upgrade e revert del cluster
- Divisione del volume FlexClone
- Re-host del volume
- Modifica e dimensionamento automatico del volume
- Rinominare il volume
- Allegare un archivio di oggetti a un aggregato
- Switchover negoziato nella configurazione MetroCluster
- Operazioni di SnapMirror
- Ripristino da una copia Snapshot
- Operazioni di quota
- Operazioni di efficienza dello storage

È possibile eseguire queste operazioni sul volume FlexGroup dopo la conversione.

#### **Configurazioni non supportate con volumi FlexGroup**

- Volume offline o limitato
- Volume root SVM
- SAN
- SMB 1.0
- Spazi dei nomi NVMe
- Servizio di copia shadow del volume remoto (VSS)

#### **Convertire un volume FlexVol in un volume FlexGroup**

A partire da ONTAP 9.7, è possibile eseguire una conversione in-place di un volume FlexVol in un volume FlexGroup senza richiedere una copia dei dati o ulteriore spazio su disco.

#### **Di cosa hai bisogno**

- I volumi in transizione possono essere convertiti in volumi FlexGroup a partire da ONTAP 9.8. Se si sta convertendo un volume in transizione in FlexGroup, consultare l'articolo della Knowledge base ["Come"](#)

[convertire un FlexVol in transizione in FlexGroup](#)" per ulteriori informazioni.

- Il volume FlexVol in fase di conversione deve essere online.
- Le operazioni e le configurazioni sul volume FlexVol devono essere compatibili con il processo di conversione.

Se il volume FlexVol presenta incompatibilità e la conversione del volume viene interrotta, viene generato un messaggio di errore. È possibile intraprendere azioni correttive e riprovare la conversione.

- Se un volume FlexVol è molto grande (ad esempio, da 80 a 100 TB) e molto pieno (dal 80 al 100%), è necessario copiare i dati piuttosto che convertirli.



La conversione di un volume FlexGroup molto grande determina un componente membro del volume FlexGroup molto completo, che può creare problemi di performance. Per ulteriori informazioni, vedere la sezione "quando non creare un volume FlexGroup" nel TR ["FlexGroup Volumes - Guida alle Best practice e all'implementazione"](#).

## Fasi

1. Verificare che il volume FlexVol sia online: `volume show vol_name -volume-style -extended, state`

```
cluster-1::> volume show my_volume -fields volume-style-extended, state
vserver volume      state  volume-style-extended
-----
vs0      my_volume online flexvol
```

2. Verificare se il volume FlexVol può essere convertito senza problemi:

- a. Accedere alla modalità privilegi avanzata: `set -privilege advanced`
- b. Verificare il processo di conversione: `volume conversion start -vserver vs1 -volume flexvol -check-only true`

Correggere tutti gli errori prima di convertire il volume.



Non è possibile convertire di nuovo un volume FlexGroup in un volume FlexVol.

3. Avviare la conversione: `volume conversion start -vserver svm_name -volume vol_name`

```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
    will cause the state of all Snapshot copies from the volume to
be set
    to "pre-conversion". Pre-conversion Snapshot copies cannot be
    restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. Verificare che la conversione sia riuscita: `volume show vol_name -fields -volume-style -extended,state`

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume      state  volume-style-extended
-----
vs0      my_volume online flexgroup
```

## Risultati

Il volume FlexVol viene convertito in un volume FlexGroup a singolo membro.

## Al termine

È possibile espandere il volume FlexGroup, in base alle esigenze.

## Convertire una relazione SnapMirror di un volume FlexVol in una relazione SnapMirror di un volume FlexGroup

Per convertire una relazione SnapMirror di un volume FlexVol in una relazione SnapMirror di un volume FlexGroup in ONTAP, è necessario prima convertire il volume FlexVol di destinazione seguito dal volume FlexVol di origine.

## A proposito di questa attività

- La conversione FlexGroup è supportata solo per le relazioni SnapMirror asincrone.
- Il tempo di conversione dipende da diverse variabili. Alcune delle variabili includono:
  - CPU del controller
  - Utilizzo della CPU da parte di altre applicazioni
  - Quantità di dati nella copia Snapshot iniziale
  - Larghezza di banda della rete
  - Larghezza di banda utilizzata da altre applicazioni

## Prima di iniziare

- Il volume FlexVol in fase di conversione deve essere online.

- Il volume FlexVol di origine nella relazione SnapMirror non deve essere il volume di origine per più relazioni SnapMirror.

A partire da ONTAP 9.9.1, le relazioni SnapMirror fanout sono supportate per i volumi FlexGroup. Per ulteriori informazioni, vedere ["Considerazioni per la creazione di relazioni a cascata e fan-out di SnapMirror per FlexGroups"](#).

- Le operazioni e le configurazioni sul volume FlexVol devono essere compatibili con il processo di conversione.

Se il volume FlexVol presenta incompatibilità e la conversione del volume viene interrotta, viene generato un messaggio di errore. È possibile intraprendere azioni correttive e riprovare la conversione.

## Fasi

1. Verificare che la relazione di SnapMirror sia corretta:

```
snapmirror show
```

È possibile convertire solo le relazioni di mirroring del tipo XDP.

Esempio:

```
cluster2::> snapmirror show
```

Progress	Source	Destination	Mirror	Relationship	Total		
Last	Path	Type	Path	State	Status	Progress	Healthy
Updated							
-----	-----	-----	-----	-----	-----	-----	-----
-----	vs0:src_dp	DP	vs2:dst_dp	Snapmirrored			
				Idle	-	true	-
	vs0:src_xdp	XDP	vs2:dst_xdp	Snapmirrored			
				Idle	-	true	-

2. Verificare se il volume di origine è compatibile con la conversione:

- a. Accedere alla modalità privilegi avanzata:

```
set -privilege advanced
```

- b. Verificare il processo di conversione:



```
volume conversion start -vserver <src_svm_name> -volume <src_vol>
-check-only true
```

Esempio:

```
volume conversion start -vserver vs1 -volume src_vol -check-only true
```

+

Correggere tutti gli errori prima di convertire il volume.

### 3. Convertire il volume FlexVol di destinazione in un volume FlexGroup.

#### a. Interrompere la relazione di SnapMirror di FlexVol:

```
snapmirror quiesce -destination-path <dest_svm:dest_volume>
```

Esempio:

```
cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
```

#### b. Avviare la conversione:

```
volume conversion start -vserver <dest_svm> -volume <dest_volume>
```

Esempio:

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp
```

Warning: After the volume is converted to a FlexGroup, it will not be possible

to change it back to a flexible volume.

Do you want to continue? {y|n}: y

[Job 510] Job succeeded: SnapMirror destination volume "dst\_xdp" has been successfully converted to a FlexGroup volume.

You must now convert the relationship's source volume, "vs0:src\_xdp", to a FlexGroup.

Then, re-establish the SnapMirror relationship using the "snapmirror resync" command.

### 4. Convertire il volume FlexVol sorgente in volume FlexGroup: `

```
volume conversion start -vserver <src_svm_name> -volume <src_vol_name>
```

Esempio:

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
        will cause the state of all Snapshot copies from the volume to
be set
        to "pre-conversion". Pre-conversion Snapshot copies cannot be
        restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

5. Risincronizzare la relazione:

```
snapmirror resync -destination-path dest_svm_name:dest_volume
```

Esempio:

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

### Al termine

Quando il volume FlexGroup di origine viene espanso per includere più componenti, è necessario assicurarsi che anche il volume di destinazione venga espanso.

## Gestione dei volumi FlexCache

### Panoramica di FlexCache

La tecnologia NetApp FlexCache accelera l'accesso ai dati, riduce la latenza della WAN e diminuisce i costi della larghezza di banda della WAN per carichi di lavoro a elevato volume di letture, in particolare dove i client devono accedere ripetutamente agli stessi dati. Quando si crea un volume FlexCache, viene creata una cache remota di un volume già esistente (origine) che contiene solo i dati ad accesso attivo (dati hot) del volume di origine.

Quando un volume FlexCache riceve una richiesta di lettura dei dati hot contenuti, può rispondere più rapidamente del volume di origine perché i dati non devono spostarsi per raggiungere il client. Se un volume FlexCache riceve una richiesta di lettura per i dati letti raramente (dati cold), recupera i dati necessari dal volume di origine e li memorizza prima di fornire la richiesta del client. Le richieste di lettura successive per tali dati vengono quindi fornite direttamente dal volume FlexCache. Dopo la prima richiesta, i dati non devono più

attraversare la rete o essere serviti da un sistema caricato pesantemente. Ad esempio, supponiamo che si verifichino colli di bottiglia nel cluster in un singolo access point per i dati richiesti di frequente. È possibile utilizzare volumi FlexCache all'interno del cluster per fornire più punti di montaggio ai dati hot, riducendo pertanto i colli di bottiglia e aumentando le performance. Si supponga inoltre di dover diminuire il traffico di rete verso un volume a cui si accede da più cluster. Puoi utilizzare FlexCache Volumes per distribuire i dati hot dal volume di origine tra i cluster all'interno della rete. In questo modo si riduce il traffico WAN fornendo agli utenti access point più vicini.

Puoi anche utilizzare la tecnologia FlexCache per migliorare le performance negli ambienti cloud e di cloud ibrido. Un volume FlexCache può aiutarti a trasferire i carichi di lavoro nel cloud ibrido inserendo nella cache i dati da un data center on-premise nel cloud. Puoi anche utilizzare FlexCache Volumes per rimuovere i silos cloud inserendo i dati nel caching da un cloud provider a un altro o tra due aree dello stesso cloud provider.

A partire da ONTAP 9.10.1, è possibile ["attiva il blocco dei file globali"](#) In tutti i volumi FlexCache. Il blocco globale dei file impedisce a un utente di accedere a un file già aperto da un altro utente. Gli aggiornamenti del volume di origine vengono quindi distribuiti simultaneamente a tutti i volumi FlexCache.

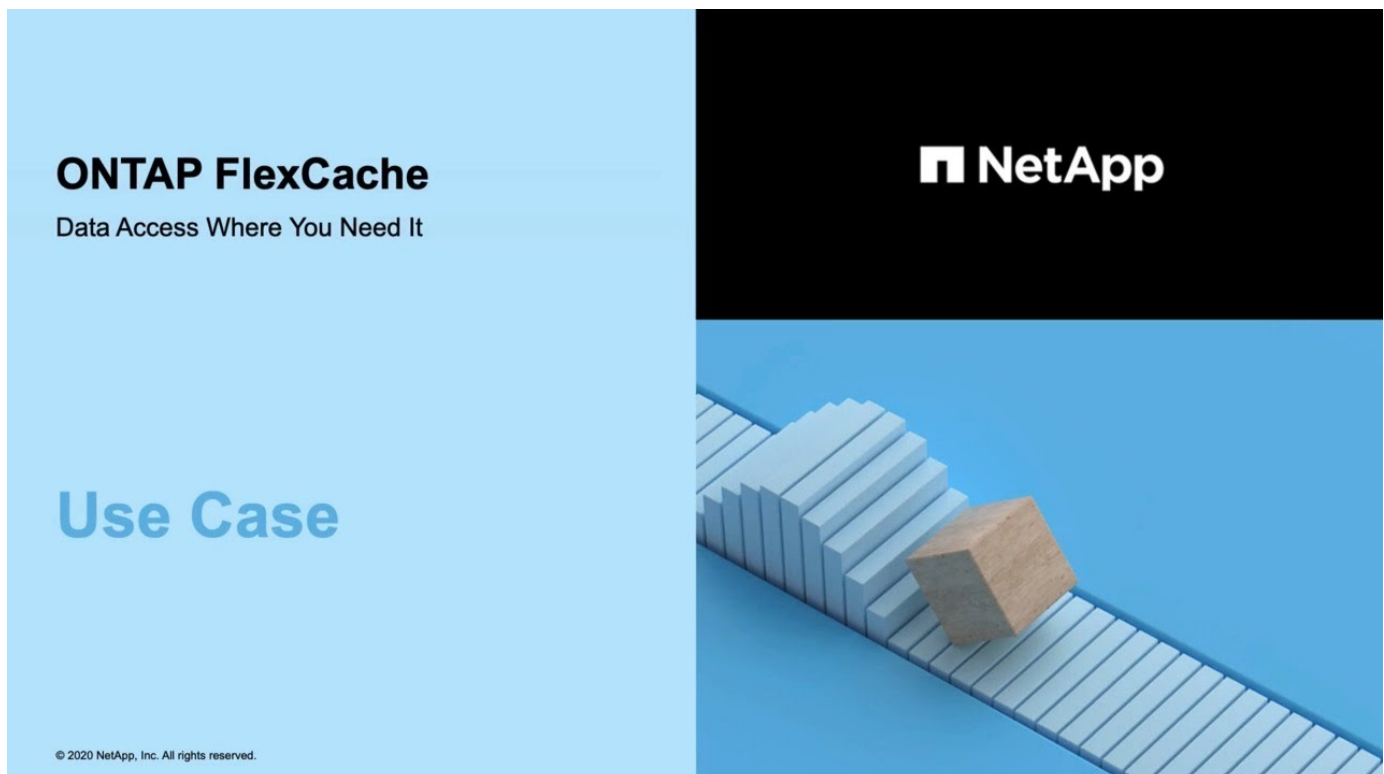
A partire da ONTAP 9.9.1, FlexCache Volumes mantiene un elenco di file non trovati. In questo modo si riduce il traffico di rete eliminando la necessità di inviare più chiamate all'origine quando i client cercano file inesistenti.

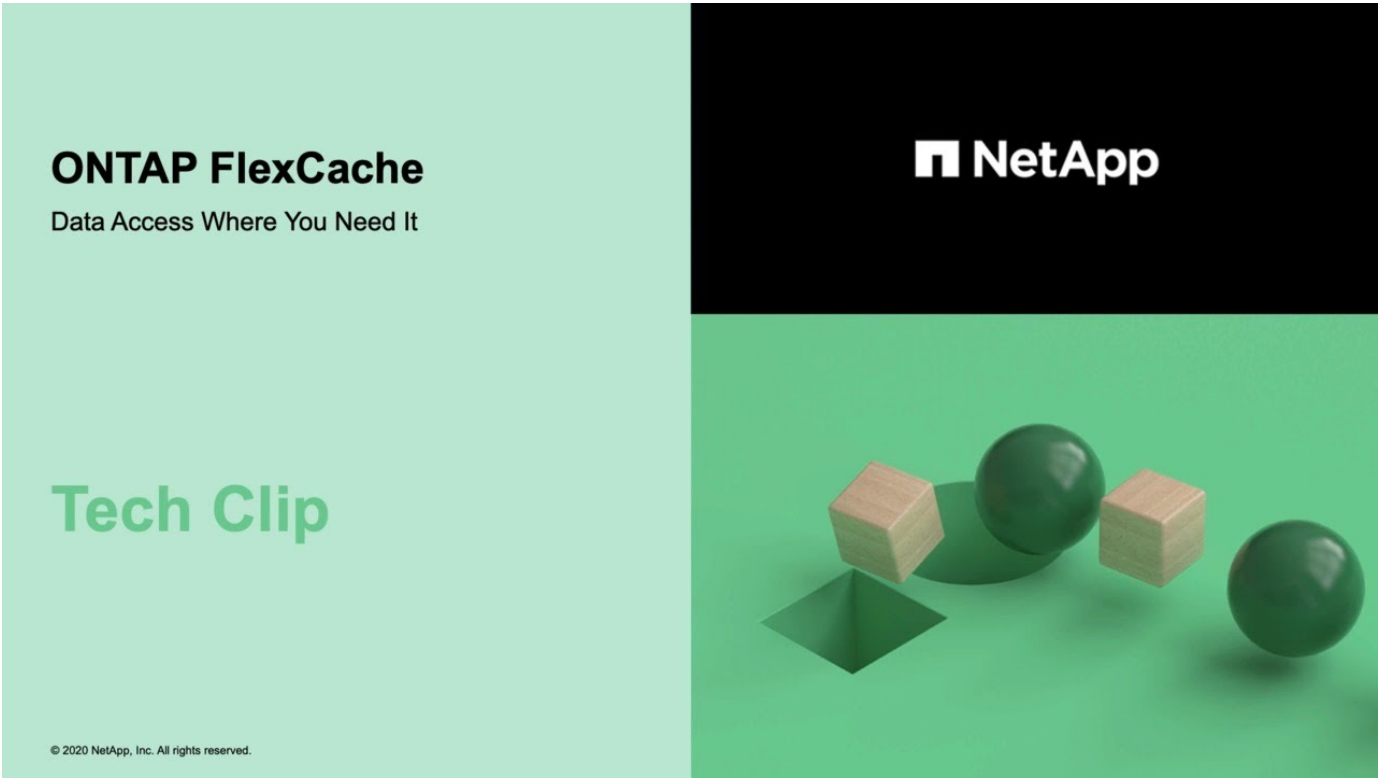
Un elenco di ulteriori ["Funzionalità supportate per i volumi FlexCache e i relativi volumi di origine"](#) È inoltre disponibile un elenco dei protocolli supportati dalla versione ONTAP.

Ulteriori informazioni sull'architettura della tecnologia ONTAP FlexCache sono disponibili in ["TR-4743: FlexCache in ONTAP"](#).

## Video

In che modo FlexCache può ridurre la latenza WAN e i tempi di lettura dei dati globali





**Funzionalità supportate e non supportate per FlexCache Volumes**

A partire da ONTAP 9,5, puoi configurare i volumi FlexCache. I volumi FlexVol sono supportati come volumi di origine e i volumi FlexGroup sono supportati come volumi FlexCache. A partire da ONTAP 9,7 sia il volume FlexVol che i volumi FlexGroup sono supportati come volumi di origine. Le funzionalità e i protocolli supportati per il volume di origine e il volume FlexCache variano.

**Protocolli supportati**


Protocollo	Supportato sul volume di origine?	Supportato dal volume FlexCache?
NFSv3	Sì	Sì


NFSv4	<p>Sì</p> <p>Per accedere ai volumi della cache utilizzando il protocollo NFSv4.x, i cluster di origine e cache devono utilizzare ONTAP 9.10.1 o versione successiva. Il cluster di origine e il cluster FlexCache possono avere diverse versioni di ONTAP, ma entrambe devono essere ONTAP 9.10.1 e versioni successive. Ad esempio, l'origine può avere ONTAP 9.10.1 e la cache può avere ONTAP 9.11.1.</p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9.10.1.</p> <p>Per accedere ai volumi della cache utilizzando il protocollo NFSv4.x, i cluster di origine e cache devono utilizzare ONTAP 9.10.1 o versione successiva. Il cluster di origine e il cluster FlexCache possono avere diverse versioni di ONTAP, ma entrambe devono essere ONTAP 9.10.1 e versioni successive. Ad esempio, l'origine può avere ONTAP 9.10.1 e la cache può avere ONTAP 9.11.1.</p>
NFSv4.2	Sì	No
PMI	Sì	<p>Sì</p> <p>Supportato a partire da ONTAP 9.8.</p>

## Funzionalità supportate

Funzione	Supportato sul volume di origine?	Supportato dal volume FlexCache?
Protezione autonoma dal ransomware	<p>Sì</p> <p>Supportato per i volumi di origine FlexVol a partire da ONTAP 9.10.1, non supportato per i volumi di origine FlexGroup.</p>	No
Antivirus	<p>Sì</p> <p>Supportato a partire da ONTAP 9,7.</p>	<p>Non applicabile</p> <p>Se si configura la scansione antivirus all'origine, non è necessaria nella cache. La scansione antivirus di origine rileva i file infettati da virus prima che le scritture siano confermate, indipendentemente dall'origine di scrittura. Per ulteriori informazioni sull'utilizzo della scansione antivirus con FlexCache, consultare la <a href="#">"Report tecnico su FlexCache with ONTAP"</a>.</p>

Controllo	<p>Sì</p> <p>Supportato a partire da ONTAP 9,7. Puoi controllare gli eventi di accesso ai file NFS nelle relazioni FlexCache utilizzando l'audit ONTAP nativo. Per ulteriori informazioni, vedere <a href="#">Considerazioni per il controllo dei volumi FlexCache</a></p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9,7. Puoi controllare gli eventi di accesso ai file NFS nelle relazioni FlexCache utilizzando l'audit ONTAP nativo. Per ulteriori informazioni, vedere <a href="#">Considerazioni per il controllo dei volumi FlexCache</a></p>
Cloud Volumes ONTAP	<p>Sì</p> <p>Supportato a partire da ONTAP 9.6</p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9.6</p>
Compattazione	<p>Sì</p> <p>Supportato a partire da ONTAP 9.6</p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9.7</p>
Compressione	<p>Sì</p> <p>Supportato a partire da ONTAP 9.6</p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9.6</p>
Deduplica	<p>Sì</p>	<p>Sì</p> <p>La deduplica inline è supportata sui volumi FlexCache a partire da ONTAP 9.6. La deduplica tra volumi è supportata sui volumi FlexCache a partire da ONTAP 9.7.</p>
FabricPool	<p>Sì</p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9.7</p>
Dr. FlexCache	<p>Sì</p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9.9.1, solo con protocollo NFSv3. I volumi FlexCache devono trovarsi in SVM separate o in cluster separati.</p>
Volume FlexGroup	<p>Sì</p> <p>Supportato a partire da ONTAP 9.7</p>	<p>Sì</p>
Volume FlexVol	<p>Sì</p>	<p>No</p>

FPolicy	<p>Sì</p> <p>Supportato a partire da ONTAP 9.7</p>	<p>Sì</p> <p>Supportato per NFS a partire da ONTAP 9,7. Supportato per SMB a partire da ONTAP 9.14.1.</p>
Configurazione di MetroCluster	<p>Sì</p> <p>Supportato a partire da ONTAP 9.7</p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9.7</p>
ODX (Microsoft Offloaded Data Transfer)	<p>Sì</p>	<p>No</p>
NetApp aggregate Encryption (NAE)	<p>Sì</p> <p>Supportato a partire da ONTAP 9.6</p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9.6</p>
NetApp Volume Encryption (NVE)	<p>Sì</p> <p>Supportato a partire da ONTAP 9.6</p>	<p>Sì</p> <p>Supportato a partire da ONTAP 9.6</p>
Bucket ONTAP S3 NAS	<p>Sì</p> <p>Supportato a partire da ONTAP 9.12.1</p>	<p>No</p>
QoS	<p>Sì</p>	<p>Sì</p> <div>  <p>La QoS a livello di file non è supportata per i volumi FlexCache.</p> </div>
Qtree	<p>Sì</p> <p>A partire da ONTAP 9.6, è possibile creare e modificare qtree. È possibile accedere ai qtree creati sull'origine dalla cache.</p>	<p>No</p>

Quote	<p>Sì</p> <p>A partire da ONTAP 9.6, l'imposizione delle quote sui volumi di origine FlexCache è supportata per utenti e gruppi.</p>	<p>No</p> <p>Con la modalità FlexCache Writeound (modalità predefinita), le scritture nella cache vengono inoltrate al volume di origine. Le quote vengono applicate all'origine.</p> <div>  <p>A partire da ONTAP 9.6, la quota remota (rquota) è supportata nei volumi FlexCache.</p> </div>
SMB Change Notify	Sì	<p>Sì</p> <p>A partire da ONTAP 9.14.1, SMB Change Notify è supportato nella cache.</p>
Volumi SnapLock	No	No
Relazioni asincrone SnapMirror*	Sì	No
	<p>*Origini di FlexCache:</p> <ul style="list-style-type: none"> <li>• È possibile disporre di un volume FlexCache da un FlexVol di origine</li> <li>• È possibile disporre di un volume FlexCache da un FlexGroup di origine</li> <li>• È possibile avere un volume FlexCache da un volume primario di origine in relazione SnapMirror.</li> <li>• A partire da ONTAP 9.8, un volume secondario SnapMirror può essere un volume di origine FlexCache.</li> </ul>	Relazioni sincroni di SnapMirror
No	No	SnapRestore
Sì	No	Copie Snapshot
Sì	No	Configurazione DR SVM



Sì	No	Access Guard a livello di storage (SLAG)
Supportato a partire da ONTAP 9.5. La SVM primaria di una relazione DR SVM può avere il volume di origine; tuttavia, se la relazione DR SVM viene interrotta, la relazione FlexCache deve essere ricreata con un nuovo volume di origine.	È possibile avere volumi FlexCache nelle SVM primarie, ma non nelle SVM secondarie. Qualsiasi volume FlexCache nella SVM primaria non viene replicato come parte della relazione di DR della SVM.	
No	No	Thin provisioning
Sì	Sì	Cloning di volumi
	Supportato a partire da ONTAP 9.7	
Sì	No	Spostamento del volume
La clonazione di un volume di origine e dei file nel volume di origine è supportata a partire da ONTAP 9.6.		
Sì	Sì (solo per i componenti del volume)	Re-host del volume
	Lo spostamento degli elementi costitutivi del volume FlexCache è supportato con ONTAP 9,6 e versioni successive.	
No	No	API vStorage per l'integrazione degli array (VAAI)



Nelle release di ONTAP 9 precedenti alla 9.5, i volumi FlexVol di origine possono fornire dati solo ai volumi FlexCache creati su sistemi che eseguono Data ONTAP 8.2.x in modalità 7. A partire da ONTAP 9.5, i volumi FlexVol di origine possono anche fornire dati ai volumi FlexCache sui sistemi ONTAP 9. Per informazioni sulla migrazione da FlexCache 7-mode a ONTAP 9 FlexCache, vedere ["Rapporto tecnico NetApp 4743: FlexCache in ONTAP"](#).

## Linee guida per il dimensionamento di un volume FlexCache

È necessario conoscere i limiti per i volumi FlexCache prima di iniziare il provisioning dei volumi.

Il limite di dimensione di un volume FlexVol è applicabile a un volume di origine. Le dimensioni di un volume FlexCache possono essere inferiori o uguali al volume di origine. La procedura consigliata per le dimensioni di un volume FlexCache è di almeno il 10% delle dimensioni del volume di origine.

È inoltre necessario conoscere i seguenti limiti aggiuntivi per i volumi FlexCache:

Limite	ONTAP 9.5-9.6	ONTAP 9.7	ONTAP 9.8 e versioni successive
Numero massimo di volumi FlexCache che è possibile creare da un volume di origine	10	10	100
Numero massimo consigliato di volumi di origine per nodo	10	100	100
Numero massimo consigliato di volumi FlexCache per nodo	10	100	100
Numero massimo consigliato di componenti FlexGroup in un volume FlexCache per nodo	40	800	800
Numero massimo di componenti per volume FlexCache per nodo	32	32	32

#### Informazioni correlate

["Interoperabilità NetApp"](#)

## Creare un volume FlexCache

È possibile creare un volume FlexCache nello stesso cluster per migliorare le prestazioni quando si accede a un oggetto hot. Se i data center si trovano in posizioni diverse, è possibile creare volumi FlexCache su cluster remoti per accelerare l'accesso ai dati.

#### A proposito di questa attività

- A partire da ONTAP 9,5, FlexCache supporta i volumi FlexVol come volumi di origine e i volumi FlexGroup come volumi FlexCache.
- A partire da ONTAP 9,7 sia il volume FlexVol che i volumi FlexGroup sono supportati come volumi di origine.
- A partire da ONTAP 9.14.0, è possibile creare un volume FlexCache non crittografato da un'origine crittografata.

#### Prima di iniziare

- È necessario eseguire ONTAP 9,5 o versione successiva.
- Se si utilizza ONTAP 9,6 o versione precedente, è necessario ["Aggiungere una licenza FlexCache"](#).

Non è richiesta una licenza FlexCache per ONTAP 9,7 o versioni successive. A partire da ONTAP 9,7, la funzionalità FlexCache è inclusa in ONTAP e non richiede più una licenza o attivazione.



Se è in uso una coppia ha ["Crittografia dei dischi SAS o NVMe \(SED, NSE, FIPS\)"](#), è necessario seguire le istruzioni riportate nell'argomento ["Ripristino di un'unità FIPS o SED in modalità non protetta"](#) Per tutti i dischi all'interno della coppia ha prima dell'inizializzazione del sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

## Esempio 4. Fasi

### System Manager

1. Se il volume FlexCache si trova su un cluster diverso da quello del volume di origine, creare una relazione di peer del cluster:
  - a. Nel cluster locale, fare clic su **protezione > Panoramica**.
  - b. Espandere **Impostazioni intercluster**, fare clic su **Aggiungi interfacce di rete** e aggiungere interfacce di rete intercluster per il cluster.

Ripetere questo passaggio sul cluster remoto.

  - c. Nel cluster remoto, fare clic su **protezione > Panoramica**. Fare clic su **⋮** Nella sezione Cluster Peers (peer cluster), fare clic su **generate Passphrase** (genera passphrase)
  - d. Copiare la passphrase generata e incollarla nel cluster locale.
  - e. Nel cluster locale, in Cluster Peers, fare clic su **Peer Clusters** e eseguire il peer dei cluster locali e remoti.
2. Se il volume FlexCache si trova sullo stesso cluster del volume di origine, ma si trova in una SVM differente, creare una relazione peer intercluster SVM di tipo "FlexCache":

In peer Storage VM, fare clic su **⋮** E poi **Peer Storage VM** per eseguire il peer delle VM di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Selezionare **Aggiungi**.
5. Selezionare **altre opzioni**, quindi selezionare **Aggiungi come cache per un volume remoto**.



Se si esegue ONTAP 9,8 o versioni successive e si desidera disattivare QoS o scegliere un criterio QoS personalizzato, fare clic su **altre opzioni**, quindi in **archiviazione e ottimizzazione**, selezionare **livello servizio prestazioni**.

### CLI

1. Se il volume FlexCache da creare si trova in un cluster diverso, creare una relazione peer del cluster:
  - a. Nel cluster di destinazione, creare una relazione di peer con il cluster di origine per la protezione dei dati:

```
cluster peer create -generate-passphrase -offer-expiration
MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addr
s <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,...|*
-ipospace <ipospace_name>
```

A partire da ONTAP 9.6, la crittografia TLS viene attivata per impostazione predefinita quando si crea una relazione peer del cluster. La crittografia TLS è supportata per la comunicazione tra i cluster tra i volumi di origine e FlexCache. Se necessario, è anche possibile disattivare la crittografia TLS per la relazione peer del cluster.

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *
```

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR  
Expiration Time: 6/7/2017 08:16:10 EST  
Initial Allowed Vserver Peers: \*  
Intercluster LIF IP: 192.140.112.101  
Peer Cluster Name: Clus\_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.

- a. Nel cluster di origine, autenticare il cluster di origine nel cluster di destinazione:

```
cluster peer create -peer-addr <peer_LIF_IPs> -ip-space <ip-space>
```

```
cluster01::> cluster peer create -peer-addr
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:  
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

2. Se il volume FlexCache si trova in una SVM diversa da quella del volume di origine, creare una relazione peer SVM con flexcache come applicazione:

- a. Se la SVM si trova in un cluster diverso, creare un permesso SVM per il peering delle SVM:

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

Nell'esempio seguente viene illustrato come creare un'autorizzazione peer SVM applicabile a tutte le SVM locali:

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache
```

Warning: This Vserver peer permission applies to all local Vservers. After that no explicit "vserver peer accept" command required for Vserver peer relationship creation request from peer cluster "cluster2" with any of the local Vservers. Do you want to continue? {y|n}: y

a. Creare la relazione di peer dell'SVM:

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. Creare un volume FlexCache:

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name>
```

Nell'esempio seguente viene creato un volume FlexCache e vengono selezionati automaticamente gli aggregati esistenti per il provisioning:

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

Nell'esempio seguente viene creato un volume FlexCache e impostato il percorso di giunzione:

```
cluster1::> flexcache create -vserver vs34 -volume fc4 -aggr-list
aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path /fc4
[Job 903] Job succeeded: Successful
```

4. Verificare la relazione FlexCache dal volume FlexCache e dal volume di origine.

a. Visualizzare la relazione di FlexCache nel cluster:

```
volume flexcache show
```

```
cluster1::> volume flexcache show
Vserver Volume      Size      Origin-Vserver Origin-Volume
Origin-Cluster
-----
vs_1      fc1        160MB     vs_1          vol_1
cluster1
```

- b. Visualizzare tutte le relazioni FlexCache nel cluster di origine:

```
volume flexcache origin show-caches
```

```
cluster::> volume flexcache origin show-caches
Origin-Vserver Origin-Volume  Cache-Vserver  Cache-Volume
Cache-Cluster
-----
vs0            ovol1        vs1            cfg1
clusA
vs0            ovol1        vs2            cfg2
clusB
vs_1           vol_1        vs_1           fc1
cluster1
```

## Risultato

Il volume FlexCache è stato creato correttamente. I client possono montare il volume utilizzando il percorso di giunzione del volume FlexCache.

## Informazioni correlate

["Peering di cluster e SVM"](#)

## Gestire volumi FlexCache

### Considerazioni per il controllo dei volumi FlexCache

A partire da ONTAP 9.7, è possibile controllare gli eventi di accesso ai file NFS nelle relazioni FlexCache utilizzando il controllo ONTAP nativo e la gestione delle policy dei file con FPolicy.

A partire da ONTAP 9.14.1, FPolicy è supportato per volumi FlexCache con NFS o SMB. In precedenza, FPolicy non era supportato per i volumi FlexCache con SMB.

Il controllo nativo e FPolicy vengono configurati e gestiti con gli stessi comandi CLI utilizzati per i volumi FlexVol. Tuttavia, i volumi FlexCache presentano un comportamento diverso.

## • Auditing nativo

- Non è possibile utilizzare un volume FlexCache come destinazione per i registri di controllo.
- Se si desidera controllare le operazioni di lettura e scrittura sui volumi FlexCache, è necessario configurare il controllo sia sulla cache SVM che sulla SVM di origine.

Questo perché le operazioni del file system vengono controllate dove vengono elaborate. Vale a dire, le letture vengono controllate sulla SVM della cache e le scritture vengono controllate sulla SVM di origine.

- Per tenere traccia dell'origine delle operazioni di scrittura, l'UUID SVM e l'ID MS vengono aggiunti nel registro di controllo per identificare il volume FlexCache da cui ha avuto origine la scrittura.
- Sebbene gli elenchi di controllo dell'accesso al sistema (SACL) possano essere impostati su un file utilizzando i protocolli NFSv4 o SMB, i volumi FlexCache supportano solo NFSv3. Pertanto, i SACL possono essere impostati solo sul volume di origine.

## • FPolicy

- Sebbene le scritture su un volume FlexCache siano assegnate al volume di origine, le configurazioni FPolicy monitorano le scritture sul volume cache. Ciò è diverso dal controllo nativo, in cui le scritture vengono controllate sul volume di origine.
- Sebbene ONTAP non richieda la stessa configurazione FPolicy sulla cache e sulle SVM di origine, si consiglia di implementare due configurazioni simili. È possibile farlo creando un nuovo criterio FPolicy per la cache, configurato come quello della SVM di origine, ma con l'ambito del nuovo criterio limitato alla SVM della cache.

## Sincronizzare le proprietà di un volume FlexCache da un volume di origine

Alcune delle proprietà del volume FlexCache devono sempre essere sincronizzate con quelle del volume di origine. Se le proprietà di un volume FlexCache non vengono sincronizzate automaticamente dopo la modifica delle proprietà nel volume di origine, è possibile sincronizzare manualmente le proprietà.

### A proposito di questa attività

Le seguenti proprietà di un volume FlexCache devono essere sempre sincronizzate con quelle del volume di origine:

- Stile di sicurezza (`-security-style`)
- Nome del volume (`-volume-name`)
- Dimensione massima directory (`-maxdir-size`)
- Valore minimo di lettura anticipata (`-min-readahead`)

### Fase

1. Dal volume FlexCache, sincronizzare le proprietà del volume:

```
volume flexcache sync-properties -vserver svm_name -volume flexcache_volume
```

```
cluster1::> volume flexcache sync-properties -vserver vs1 -volume fc1
```

## Aggiornare le configurazioni di una relazione FlexCache

Dopo eventi come lo spostamento del volume, il trasferimento dell'aggregato o il failover dello storage, le informazioni di configurazione del volume sul volume di origine e sul volume FlexCache vengono aggiornate automaticamente. Se gli aggiornamenti automatici non vengono eseguiti correttamente, viene generato un messaggio EMS, quindi è necessario aggiornare manualmente la configurazione per la relazione FlexCache.

Se il volume di origine e il volume FlexCache sono in modalità disconnessa, potrebbe essere necessario eseguire alcune operazioni aggiuntive per aggiornare manualmente una relazione FlexCache.

### A proposito di questa attività

Se si desidera aggiornare le configurazioni di un volume FlexCache, è necessario eseguire il comando dal volume di origine. Se si desidera aggiornare le configurazioni di un volume di origine, è necessario eseguire il comando dal volume FlexCache.

### Fase

1. Aggiornare la configurazione della relazione FlexCache:

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume  
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

## Abilitare gli aggiornamenti dei tempi di accesso al file

A partire da ONTAP 9.11.1, è possibile attivare `-atime-update` Sul volume FlexCache per consentire gli aggiornamenti dei tempi di accesso al file. È inoltre possibile impostare un periodo di aggiornamento dell'ora di accesso con `-atime-update-period` attributo. Il `-atime-update-period` attribute controlla la frequenza con cui possono essere eseguiti gli aggiornamenti dei tempi di accesso e quando possono propagarsi al volume di origine.

### Panoramica

ONTAP fornisce un campo a livello di volume chiamato `-atime-update`. Per gestire gli aggiornamenti dei tempi di accesso su file e directory letti utilizzando `READ`, `READLINK` e `REaddir`. `Atime` viene utilizzato per le decisioni relative al ciclo di vita dei dati per file e directory a cui si accede raramente. I file a cui si accede raramente vengono infine migrati nello storage di archiviazione e spesso vengono spostati su nastro in un secondo momento.

Il campo di aggiornamento `atime` è disattivato per impostazione predefinita sui volumi FlexCache esistenti e appena creati. Se si utilizzano volumi FlexCache con versioni di ONTAP precedenti alla 9.11.1, è necessario lasciare disattivato il campo `atime-update` in modo che le cache non vengano estromesse inutilmente quando viene eseguita un'operazione di lettura sul volume di origine. Tuttavia, con cache FlexCache di grandi dimensioni, gli amministratori utilizzano strumenti speciali per gestire i dati e garantire che i dati hot rimangano nella cache e che i dati cold vengano eliminati. Ciò non è possibile quando `aTime-update` è disattivato. Tuttavia, a partire da ONTAP 9.11.1, è possibile attivare `-atime-update` e `-atime-update-period`, e utilizzare gli strumenti necessari per gestire i dati memorizzati nella cache.



## Prima di iniziare

Tutti i volumi FlexCache devono eseguire ONTAP 9.11.1 o versione successiva.

## A proposito di questa attività

Impostazione `-atime-update-period` a 86400 secondi non consente più di un aggiornamento del tempo di accesso per un periodo di 24 ore, indipendentemente dal numero di operazioni di lettura eseguite su un file.

Impostazione di `-atime-update-period` a 0 invia messaggi all'origine per ogni accesso in lettura. L'origine informa quindi ciascun volume FlexCache che l'`atime` è obsoleto, con un impatto sulle performance.

## Fasi

1. Abilitare gli aggiornamenti del tempo di accesso al file e impostare la frequenza di aggiornamento:

```
volume modify -volume vol_name -vserver SVM_name -atime-update true -atime-update-period seconds
```

Nell'esempio seguente viene attivato `-atime-update` e `set -atime-update-period` a 86400 secondi o 24 ore:

```
c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime-update-period 86400
```

2. Verificare che `-atime-update` è attivato:

```
volume show -volume vol_name -fields atime-update,atime-update-period
```

```
c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-update-period
vserver volume          atime-update atime-update-period
-----
vs2_c1  cache1_origin1 true           86400
```

## Attiva il blocco globale dei file

A partire da ONTAP 9.10.1, è possibile applicare il blocco globale dei file per impedire la lettura di tutti i file memorizzati nella cache correlati.

Con il blocco globale dei file abilitato, le modifiche al volume di origine vengono sospese fino a quando tutti i volumi FlexCache non sono online. È necessario attivare il blocco globale dei file solo quando si ha il controllo sull'affidabilità delle connessioni tra la cache e l'origine a causa della sospensione e dei possibili timeout delle modifiche quando i volumi FlexCache sono offline.

## Prima di iniziare

- Il blocco globale dei file richiede che i cluster contenenti l'origine e tutte le cache associate eseguano ONTAP 9.9.1 o versione successiva. Il blocco globale dei file può essere attivato su volumi FlexCache nuovi o esistenti. Il comando può essere eseguito su un unico volume e si applica a tutti i volumi FlexCache associati.

- Per attivare il blocco globale dei file, è necessario essere nel livello di privilegio avanzato.
- Se si torna a una versione di ONTAP precedente alla 9.9.1, il blocco globale dei file deve essere prima disattivato nell'origine e nelle cache associate. Per disattivare, dal volume di origine, eseguire: `volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0`
- Il processo di attivazione del blocco dei file globale dipende dal fatto che l'origine disponga di cache esistenti:
  - [\[enable-gfl-new\]](#)
  - [\[enable-gfl-existing\]](#)

### Attiva il blocco globale dei file sui nuovi volumi FlexCache

#### Fasi

1. Creare il volume FlexCache con `-is-global-file-locking` imposta su `true`:

```
volume flexcache create volume volume_name -is-global-file-locking-enabled true
```



Il valore predefinito di `-is-global-file-locking` è `false`. In caso di successiva `volume flexcache create` i comandi vengono eseguiti su un volume e devono essere passati con `-is-global-file-locking enabled` impostare su `true`.

### Attiva il blocco globale dei file sui volumi FlexCache esistenti

#### Fasi

1. Il blocco globale dei file deve essere impostato dal volume di origine.
2. L'origine non può avere altre relazioni esistenti (ad esempio, SnapMirror). Tutte le relazioni esistenti devono essere dissociate. Tutte le cache e i volumi devono essere collegati al momento dell'esecuzione del comando. Per verificare lo stato della connessione, eseguire:

```
volume flexcache connection-status show
```

Lo stato di tutti i volumi elencati deve essere visualizzato come `connected`. Per ulteriori informazioni, vedere ["Visualizzare lo stato di una relazione FlexCache"](#) oppure ["Sincronizzare le proprietà di un volume FlexCache da un'origine"](#).

3. Attiva il blocco globale dei file nelle cache:

```
volume flexcache origin config show/modify -volume volume_name -is-global-file-locking-enabled true
```

### Precompilare un volume FlexCache

È possibile prepopolare un volume FlexCache per ridurre il tempo necessario per accedere ai dati memorizzati nella cache.

#### Di cosa hai bisogno

- È necessario essere un amministratore del cluster a livello di privilegi avanzati
- I percorsi per la prepopolazione devono esistere o l'operazione di prepopolazione non riesce.

## A proposito di questa attività

- La precompilazione legge solo i file e passa in rassegna le directory
- Il `-isRecursion` il flag si applica all'intero elenco di directory passate per il prepopolamento

## Fasi

### 1. Precompilare un volume FlexCache:

```
volume flexcache prepopulate -cache-vserver vs2 -cache-volume -path  
-list path_list -isRecursion true|false
```

- Il `-path-list` il parametro indica il percorso della directory relativa che si desidera prepopolare a partire dalla directory principale di origine. Ad esempio, se la directory principale di origine è denominata `/origin` e contiene directory `/origin/dir1` e `/origin/dir2`, è possibile specificare l'elenco dei percorsi come segue: `-path-list dir1, dir2` oppure `-path-list /dir1, /dir2`.
- Il valore predefinito di `-isRecursion` Il parametro è vero.

Questo esempio precompila un singolo percorso di directory:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache  
-volume fg_cachevol_1 -path-list /dir1  
(volume flexcache prepopulate start)  
[JobId 207]: FlexCache prepopulate job queued.
```

Questo esempio precompila i file da diverse directory:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache  
-volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4  
(volume flexcache prepopulate start)  
[JobId 208]: FlexCache prepopulate job queued.
```

Questo esempio precompila un singolo file:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache  
-volume fg_cachevol_1 -path-list /dir1/file1.txt  
(volume flexcache prepopulate start)  
[JobId 209]: FlexCache prepopulate job queued.
```

Questo esempio precompila tutti i file dall'origine:

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache  
-volume fg_cachevol_1 -path-list / -isRecursion true  
(volume flexcache prepopulate start)  
[JobId 210]: FlexCache prepopulate job queued.
```

Questo esempio include un percorso non valido per il prepopolamento:

```
cluster1::*> flexcache prepopulate start -cache-volume  
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list  
/dir1, dir5, dir6  
(volume flexcache prepopulate start)  
  
Error: command failed: Path(s) "dir5, dir6" does not exist in origin  
volume  
      "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. Visualizza il numero di file letti:

```
job show -id job_ID -ins
```

### Eliminare una relazione FlexCache

È possibile eliminare una relazione FlexCache e il volume FlexCache se non si richiede più il volume FlexCache.

#### Fasi

1. Dal cluster che dispone del volume FlexCache, portare il volume FlexCache offline:

```
volume offline -vserver svm_name -volume volume_name
```

2. Eliminare il volume FlexCache:

```
volume flexcache delete -vserver svm_name -volume volume_name
```

I dettagli della relazione FlexCache vengono rimossi dal volume di origine e dal volume FlexCache.

# Gestione della rete

## Inizia subito

### Panoramica sulla gestione della rete

Puoi utilizzare le seguenti informazioni per eseguire un'amministrazione di base della rete di storage usando System Manager o l'interfaccia CLI. È possibile configurare le porte di rete fisiche e virtuali (VLAN e gruppi di interfacce), creare LIF utilizzando IPv4 e IPv6, gestire i servizi di routing e risoluzione degli host nei cluster, utilizzare il bilanciamento del carico per ottimizzare il traffico di rete e monitorare un cluster utilizzando SNMP.

Se non diversamente specificato, le procedure CLI si applicano a tutte le versioni di ONTAP 9.

Per comprendere l'impatto delle funzionalità di rete disponibili in ogni versione di ONTAP 9, vedere la ["Note di rilascio di ONTAP"](#).

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per visualizzare un grafico che mostra i componenti e la configurazione della rete. A partire da ONTAP 9.12, è possibile visualizzare l'associazione di LIF e subnet nella griglia delle interfacce di rete. Se si utilizza Gestione sistema classico (disponibile solo in ONTAP 9.7 e versioni precedenti), vedere ["Gestione della rete"](#).

La nuova funzionalità di visualizzazione della rete consente agli utenti di visualizzare il percorso delle connessioni di rete tra host, porte, SVM, volumi e così via in un'interfaccia grafica.

Il grafico viene visualizzato quando si seleziona **rete > Panoramica** o quando si seleziona ➔ Dalla sezione **Network** della dashboard.

La figura mostra le seguenti categorie di componenti:


- Host
- Porte di storage
- Interfacce di rete
- VM di storage
- Componenti per l'accesso ai dati

Ogni sezione mostra ulteriori dettagli che è possibile spostare il mouse o selezionare per eseguire attività di configurazione e gestione della rete.

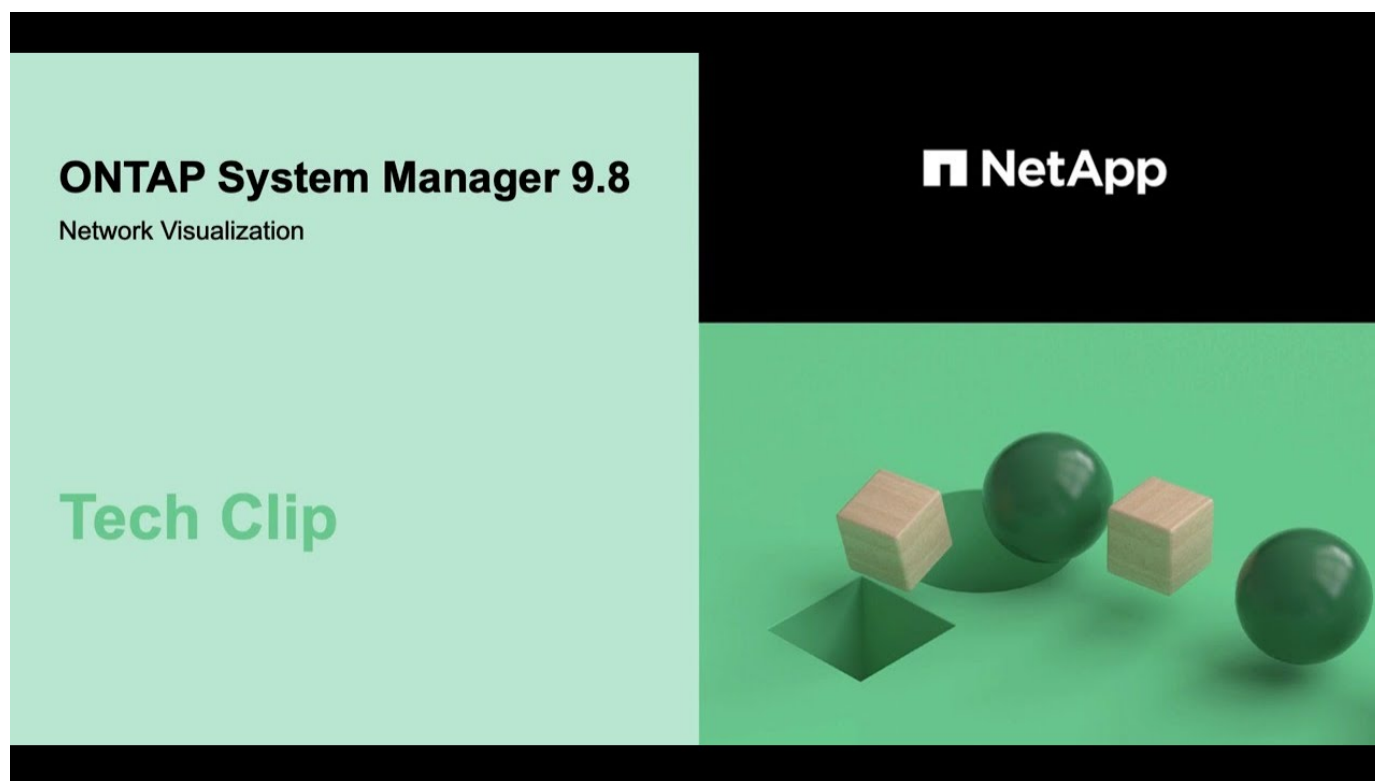
### Esempi

Di seguito sono riportati alcuni esempi dei diversi modi in cui è possibile interagire con la grafica per visualizzare i dettagli di ciascun componente o avviare azioni per gestire la rete:

- Fare clic su un host per visualizzarne la configurazione: Porte, interfacce di rete, VM di storage e componenti di accesso ai dati associati.
- Passare il mouse sul numero di volumi in una VM di storage per selezionare un volume e visualizzarne i dettagli.
- Selezionare un'interfaccia iSCSI per visualizzarne le prestazioni nell'ultima settimana.

- Fare clic su  accanto a un componente per avviare azioni per modificare tale componente.
- Determinare rapidamente dove potrebbero verificarsi problemi nella rete, indicato da una "X" accanto ai componenti non funzionanti.

## Video System Manager Network Visualization



## Verificare la configurazione di rete in seguito a un aggiornamento ONTAP da ONTAP 9,7x o versione precedente

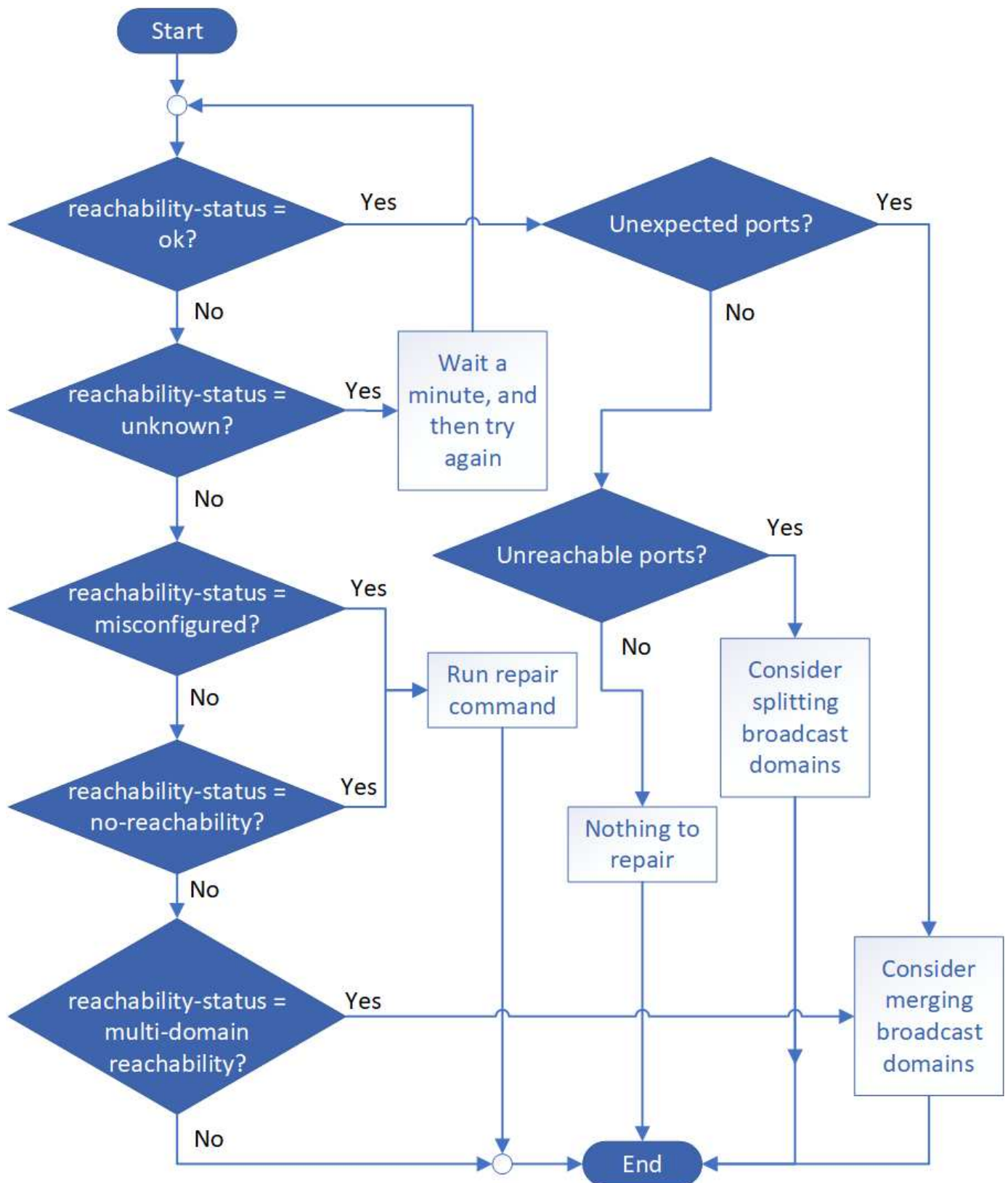
Dopo aver eseguito l'aggiornamento da ONTAP 9,7x o versione precedente a ONTAP 9,8 o versione successiva, è necessario verificare la configurazione di rete. Dopo l'aggiornamento, ONTAP monitora automaticamente la raggiungibilità di livello 2.

### Fase

1. Verificare che ogni porta sia raggiungibile dal proprio dominio di trasmissione previsto:

```
network port reachability show -detail
```

L'output del comando contiene i risultati di raggiungibilità. Utilizzare il seguente albero decisionale e la seguente tabella per comprendere i risultati di raggiungibilità (stato di raggiungibilità) e determinare cosa, se necessario, fare in seguito.



stato di raggiungibilità	Descrizione
--------------------------	-------------

ok	<p>La porta ha una capacità di livello 2 rispetto al dominio di trasmissione assegnato.</p> <p>Se lo stato di raggiungibilità è "ok", ma ci sono "porte impreviste", considerare la possibilità di unire uno o più domini di broadcast. Per ulteriori informazioni, vedere <a href="#">"Unire i domini di broadcast"</a>.</p> <p>Se lo stato di raggiungibilità è "ok", ma ci sono "porte irraggiungibili", considerare la possibilità di suddividere uno o più domini di broadcast. Per ulteriori informazioni, vedere <a href="#">"Suddividere i domini di broadcast"</a>.</p> <p>Se lo stato di raggiungibilità è "ok" e non ci sono porte impreviste o irraggiungibili, la configurazione è corretta.</p>
riconfigurazione non corretta	<p>La porta non dispone di capacità di livello 2 rispetto al dominio di trasmissione assegnato; tuttavia, la porta dispone di capacità di livello 2 rispetto a un dominio di trasmissione diverso.</p> <p>È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta al dominio di trasmissione a cui è possibile accedere:</p> <pre>network port reachability repair -node -port</pre> <p>Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
nessuna raggiungibilità	<p>La porta non dispone di capacità di livello 2 per nessun dominio di trasmissione esistente.</p> <p>È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta a un nuovo dominio di trasmissione creato automaticamente in IPspace predefinito:</p> <pre>network port reachability repair -node -port</pre> <p>Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
raggiungibilità multi-dominio	<p>La porta ha una raggiungibilità di livello 2 per il dominio di broadcast assegnato; tuttavia, ha anche una raggiungibilità di livello 2 per almeno un altro dominio di broadcast.</p> <p>Esaminare la connettività fisica e la configurazione dello switch per determinare se non è corretta o se il dominio di trasmissione assegnato alla porta deve essere Unito a uno o più domini di trasmissione.</p> <p>Per ulteriori informazioni, vedere <a href="#">"Unire i domini di broadcast"</a> oppure <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
sconosciuto	<p>Se lo stato di raggiungibilità è "sconosciuto", attendere alcuni minuti e provare a eseguire nuovamente il comando.</p>

Dopo aver riparato una porta, è necessario controllare e risolvere le LIF e le VLAN spostate. Se la porta faceva parte di un gruppo di interfacce, è necessario comprendere anche cosa è successo a quel gruppo di



interfacce. Per ulteriori informazioni, vedere ["Riparare la raggiungibilità delle porte"](#).

## Componenti di rete

### Panoramica dei componenti di rete di un cluster

Prima di configurare il cluster, è necessario acquisire familiarità con i componenti di rete di un cluster. La configurazione dei componenti fisici di rete di un cluster in componenti logici offre la flessibilità e la funzionalità multi-tenancy di ONTAP.

I vari componenti di rete in un cluster sono i seguenti:

- Porte fisiche

Le schede di interfaccia di rete (NIC) e gli host bus adapter (HBA) forniscono connessioni fisiche (Ethernet e Fibre Channel) da ciascun nodo alle reti fisiche (reti di gestione e dati).

Per i requisiti del sito, le informazioni sullo switch, il cablaggio delle porte e il cablaggio delle porte integrate del controller, consultare la Hardware Universe all'indirizzo ["hwu.netapp.com"](http://hwu.netapp.com).

- Porte logiche

Le Virtual Local Area Network (VLAN) e i gruppi di interfacce costituiscono le porte logiche. I gruppi di interfacce trattano diverse porte fisiche come una singola porta, mentre le VLAN suddividono una porta fisica in più porte separate.

- IPspaces

È possibile utilizzare un IPspace per creare uno spazio di indirizzi IP distinto per ogni SVM in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

- Domini di broadcast

Un dominio di broadcast risiede in un IPspace e contiene un gruppo di porte di rete, potenzialmente provenienti da molti nodi del cluster, appartenenti alla stessa rete Layer 2. Le porte del gruppo vengono utilizzate in una SVM per il traffico dati.

- Subnet

Una subnet viene creata all'interno di un dominio di broadcast e contiene un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Questo pool di indirizzi IP semplifica l'allocazione degli indirizzi IP durante la creazione di LIF.

- Interfacce logiche

Un'interfaccia logica (LIF) è un indirizzo IP o un nome di porta universale (WWPN) associato a una porta. È associato ad attributi come gruppi di failover, regole di failover e regole firewall. Una LIF comunica attraverso la rete attraverso la porta (fisica o logica) alla quale è attualmente associata.

I diversi tipi di LIF in un cluster sono LIF di dati, LIF di gestione con ambito cluster, LIF di gestione con ambito nodo, LIF di intercluster e LIF di cluster. La proprietà delle LIF dipende dalla SVM in cui risiede la LIF. Le LIF dei dati sono di proprietà delle SVM dei dati, le LIF di gestione con ambito del nodo, la gestione con ambito del cluster e le LIF tra cluster sono di proprietà delle SVM amministrative e le LIF del cluster

sono di proprietà delle SVM del cluster.

- Zone DNS

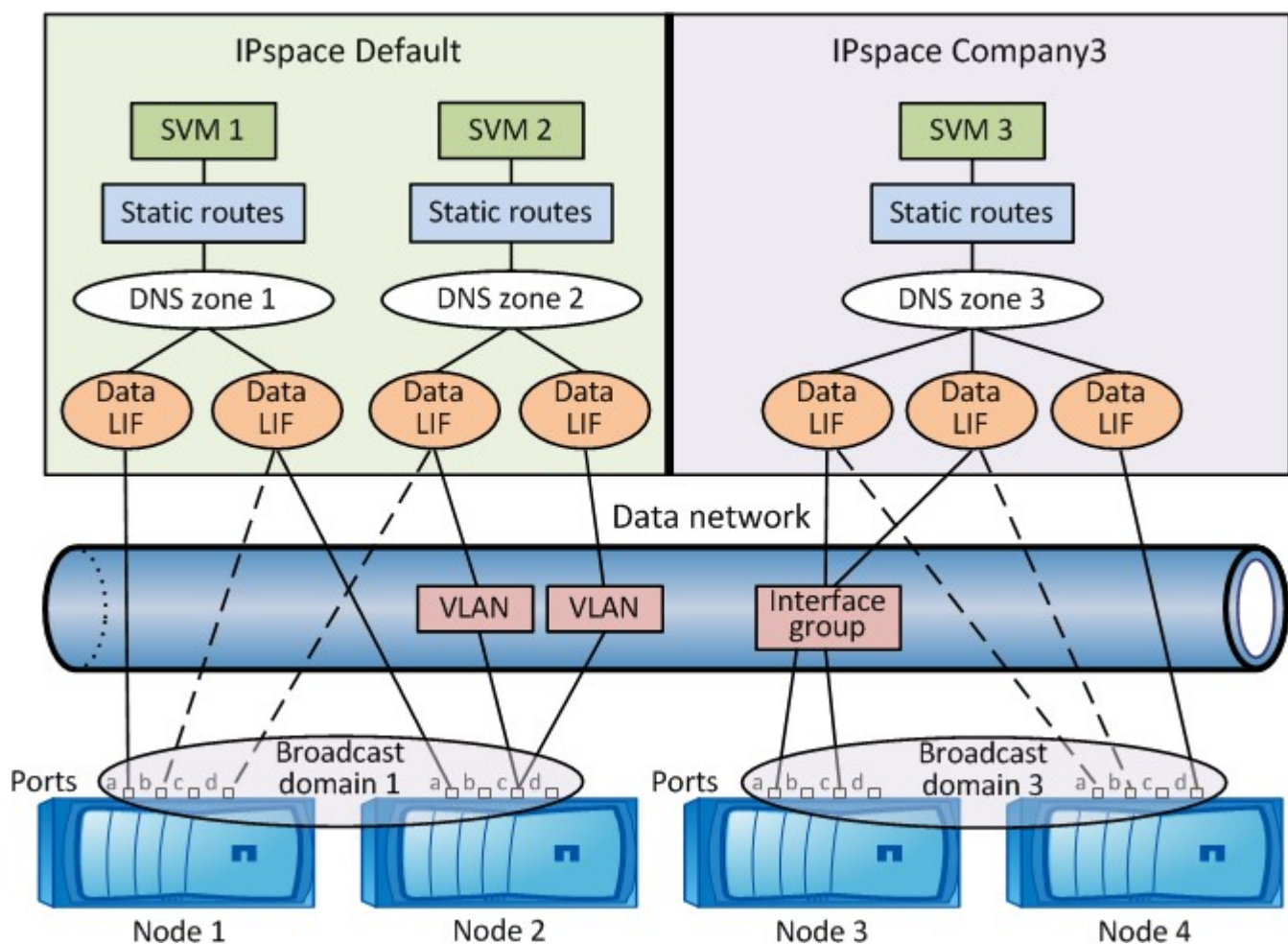
È possibile specificare la zona DNS durante la creazione della LIF, fornendo un nome per la LIF da esportare attraverso il server DNS del cluster. Più LIF possono condividere lo stesso nome, consentendo alla funzione di bilanciamento del carico DNS di distribuire gli indirizzi IP per il nome in base al carico.

Le SVM possono avere più zone DNS.

- Routing

Ogni SVM è autosufficiente per quanto riguarda il networking. Una SVM possiede LIF e route che possono raggiungere ciascuno dei server esterni configurati.

La seguente figura illustra come i diversi componenti di rete sono associati in un cluster a quattro nodi:



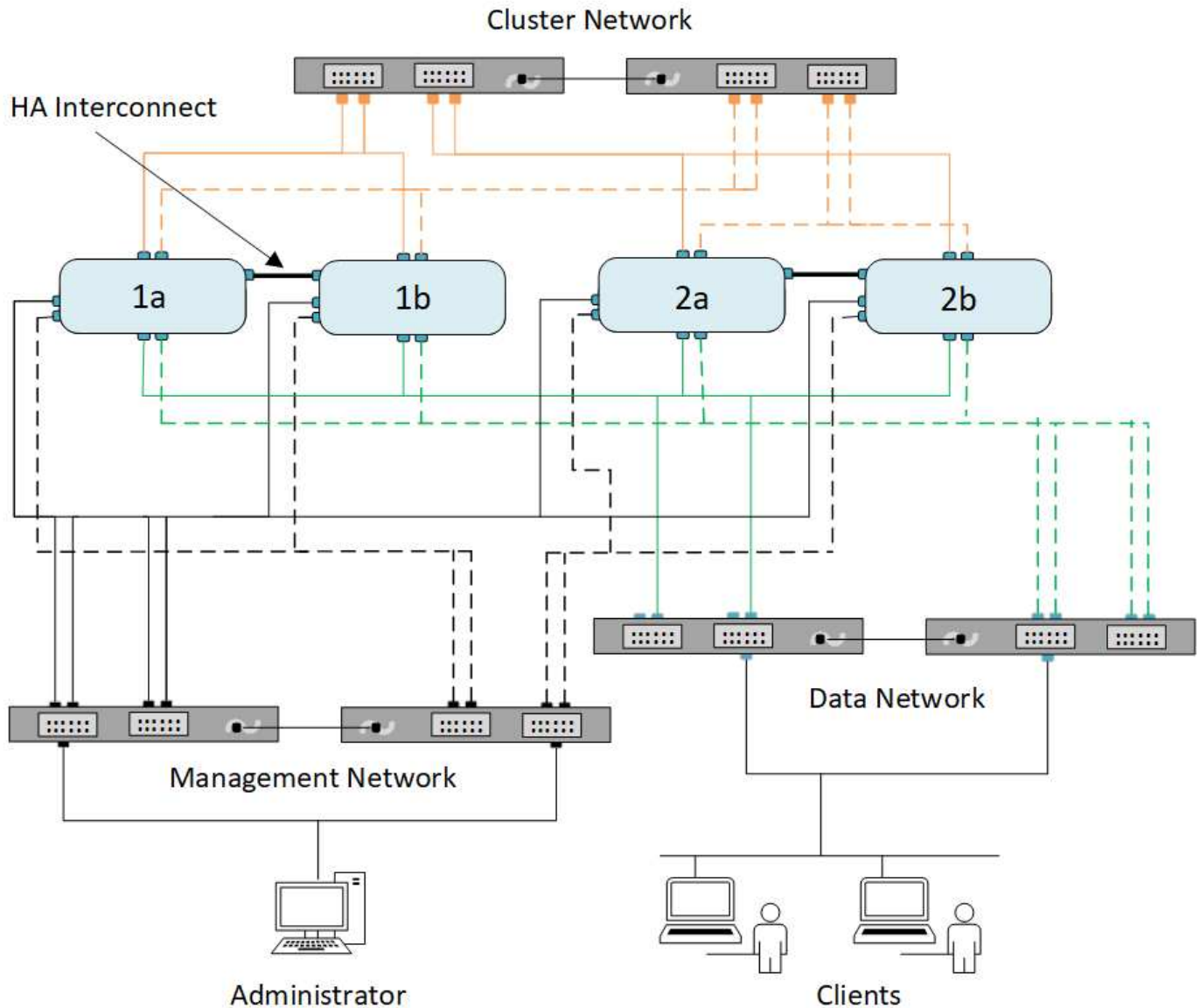
## Linee guida per il cablaggio di rete

Le Best practice per il cablaggio di rete separano il traffico nelle seguenti reti: Cluster, gestione e dati.

È necessario collegare un cluster in modo che il traffico del cluster si trovi su una rete separata da tutto il traffico. È una pratica facoltativa, ma consigliata, che prevede la separazione del traffico di gestione della rete dai dati e dal traffico intracluster. Mantenendo reti separate, è possibile ottenere performance migliori, facilità di

amministrazione e maggiore sicurezza e accesso di gestione ai nodi.

Il seguente diagramma illustra il cablaggio di rete di un cluster ha a quattro nodi che include tre reti separate:



Per il cablaggio delle connessioni di rete, seguire alcune linee guida:

- Ciascun nodo deve essere connesso a tre reti distinte.

Una rete è per la gestione, una per l'accesso ai dati e una per la comunicazione intracluster. Le reti di gestione e dati possono essere separate in modo logico.

- È possibile disporre di più connessioni di rete dati a ciascun nodo per migliorare il flusso di traffico (dati) del client.
- Un cluster può essere creato senza connessioni di rete dati, ma deve includere una connessione di interconnessione del cluster.
- Devono essere sempre presenti due o più connessioni cluster per ciascun nodo.

Per ulteriori informazioni sul cablaggio di rete, consultare ["Centro di documentazione dei sistemi AFF e FAS"](#) e

## Relazione tra domini di broadcast, gruppi di failover e policy di failover

I domini di broadcast, i gruppi di failover e le policy di failover lavorano insieme per determinare quale porta assume il controllo in caso di guasto del nodo o della porta su cui è configurato un LIF.

Un dominio di broadcast elenca tutte le porte raggiungibili nella stessa rete Ethernet Layer 2. Un pacchetto di trasmissione Ethernet inviato da una delle porte viene visto da tutte le altre porte nel dominio di trasmissione. Questa caratteristica di raggiungibilità comune di un dominio di broadcast è importante per i LIF perché se un LIF dovesse eseguire il failover su qualsiasi altra porta del dominio di broadcast, potrebbe comunque raggiungere tutti gli host locali e remoti raggiungibili dalla porta originale.

I gruppi di failover definiscono le porte all'interno di un dominio di broadcast che forniscono una copertura di failover LIF reciproca. Ogni dominio di broadcast dispone di un gruppo di failover che include tutte le porte. Questo gruppo di failover contenente tutte le porte nel dominio di broadcast è il gruppo di failover predefinito e consigliato per LIF. È possibile creare gruppi di failover con sottoinsiemi più piccoli definiti, ad esempio un gruppo di failover di porte con la stessa velocità di collegamento all'interno di un dominio di broadcast.

Una policy di failover determina il modo in cui una LIF utilizza le porte di un gruppo di failover quando un nodo o una porta non funziona. Considerare la policy di failover come un tipo di filtro applicato a un gruppo di failover. Le destinazioni di failover per una LIF (l'insieme di porte a cui una LIF può eseguire il failover) vengono determinate applicando la policy di failover della LIF al gruppo di failover della LIF nel dominio di broadcast.

È possibile visualizzare le destinazioni di failover per una LIF utilizzando il seguente comando CLI:

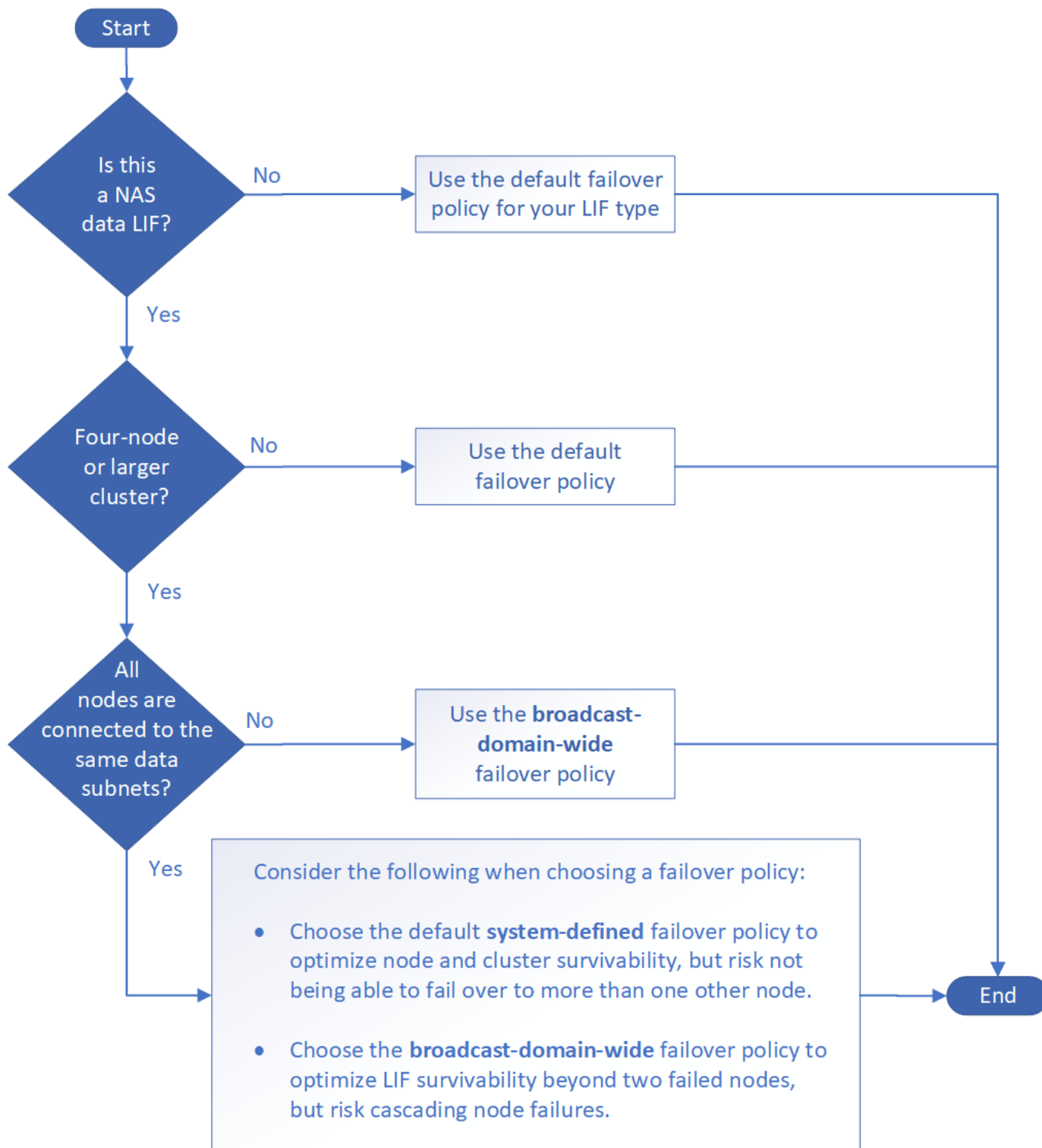
```
network interface show -failover
```

NetApp consiglia vivamente di utilizzare la policy di failover predefinita per il tipo di LIF.

### Decidere quale policy di failover LIF utilizzare

Decidere se utilizzare la policy di failover predefinita consigliata o se modificarla in base al tipo e all'ambiente LIF in uso.

#### Albero decisionale delle policy di failover



#### Policy di failover predefinite per tipo LIF

Tipo LIF	Policy di failover predefinita	Descrizione
LIF BGP	disattivato	LIF non esegue il failover su un'altra porta.
LIF del cluster	solo locale	LIF esegue il failover solo sulle porte dello stesso nodo.

LIF. Gestione cluster	broadcast-domain-wide	LIF esegue il failover su porte nello stesso dominio di broadcast, su qualsiasi nodo del cluster.
LIF di intercluster	solo locale	LIF esegue il failover solo sulle porte dello stesso nodo.
LIF dati NAS	definito dal sistema	LIF esegue il failover su un altro nodo che non è il partner ha.
LIF di gestione dei nodi	solo locale	LIF esegue il failover solo sulle porte dello stesso nodo.
LIF dati SAN	disattivato	LIF non esegue il failover su un'altra porta.

Il criterio di failover "sfo-partner-only" non è un criterio predefinito, ma può essere utilizzato quando si desidera che LIF esegue il failover su una porta solo sul nodo principale o sul partner SFO.

## Flusso di lavoro di failover del percorso NAS (ONTAP 9,8 e versioni successive)

### Informazioni sul failover del percorso NAS (ONTAP 9,8 e versioni successive)

Questo flusso di lavoro guida l'utente attraverso le fasi di configurazione della rete per impostare il failover del percorso NAS per ONTAP 9.8 e versioni successive. Questo flusso di lavoro presuppone quanto segue:

- Si desidera utilizzare le Best practice di failover del percorso NAS in un flusso di lavoro che semplifica la configurazione di rete.
- Si desidera utilizzare la CLI, non System Manager.
- Si sta configurando la rete su un nuovo sistema che esegue ONTAP 9.8 o versione successiva.

Se si esegue una versione di ONTAP precedente alla 9.8, è necessario utilizzare la seguente procedura di failover del percorso NAS per ONTAP da 9.0 a 9.7:

- ["Workflow di failover del percorso NAS ONTAP 9.0-9.7"](#)

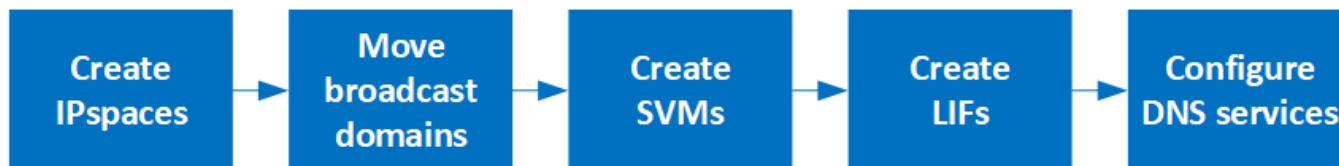
Se si desidera ottenere dettagli sulla gestione della rete, è necessario utilizzare il materiale di riferimento per la gestione della rete:

- [Panoramica sulla gestione della rete](#)

### Flusso di lavoro (ONTAP 9,8 e versioni successive)

Se hai già familiarità con i concetti di base del networking, potresti risparmiare tempo nell'impostazione della rete esaminando questo flusso di lavoro pratico per la configurazione del failover del percorso NAS.

Un LIF NAS esegue automaticamente la migrazione a una porta di rete esistente dopo un errore di collegamento sulla porta corrente. Per gestire il failover del percorso, è possibile fare affidamento sulle impostazioni predefinite di ONTAP.



Un LIF SAN non esegue la migrazione (a meno che non venga spostato manualmente dopo l'errore di collegamento). Invece, la tecnologia multipathing sull'host trasferisce il traffico a un LIF diverso. Per ulteriori informazioni, vedere ["Amministrazione SAN"](#).

1

### "Completare il foglio di lavoro"

Utilizzare il foglio di lavoro per pianificare il failover del percorso NAS.

2

### "Creare IPspaces"

Crea uno spazio di indirizzi IP distinto per ciascuna SVM in un cluster.

3

### "Spostare i domini di broadcast negli IPspaces"

Spostare i domini di broadcast in IPspace.

4

### "Creare SVM"

Creazione di SVM per fornire dati ai client.

5

### "Creare LIF"

Creare LIF sulle porte che servono per accedere ai dati.

6

### "Configurare i servizi DNS per la SVM"

Configurare i servizi DNS per la SVM prima di creare un server NFS o SMB.

## Foglio di lavoro per la configurazione del failover del percorso NAS (ONTAP 9,8 e versioni successive)

Completare tutte le sezioni del foglio di lavoro prima di configurare il failover del percorso NAS.

### Configurazione di IPspace

È possibile utilizzare un IPspace per creare uno spazio di indirizzi IP distinto per ogni SVM in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

Informazioni	Necessario?	I tuoi valori
--------------	-------------	---------------

IPSpace name (Nome IPSpace): Identificativo univoco di IPSpace.	Sì	
---	----	--

### Configurazione del dominio di trasmissione

Un dominio di trasmissione raggruppa le porte che appartengono alla stessa rete Layer 2 e imposta la MTU per le porte del dominio di trasmissione.

I domini di broadcast vengono assegnati a un IPSpace. Un IPSpace può contenere uno o più domini di broadcast.



La porta a cui si verifica il failover di LIF deve essere membro del gruppo di failover per LIF. Per ogni dominio di broadcast creato da ONTAP, viene creato anche un gruppo di failover con lo stesso nome che contiene tutte le porte nel dominio di broadcast.

Informazioni	Necessario?	I tuoi valori
<p>IPSpace name (Nome IPSpace): L'IPSpace a cui è assegnato il dominio di trasmissione.</p> <p>Questo IPSpace deve esistere.</p>	Sì	
<p>Broadcast domain name (Nome dominio di trasmissione): Il nome del dominio di trasmissione.</p> <p>Questo nome deve essere univoco in IPSpace.</p>	Sì	
<p>MTU il valore massimo dell'unità di trasmissione per il dominio di trasmissione, generalmente impostato su <b>1500</b> o <b>9000</b>.</p> <p>Il valore MTU viene applicato a tutte le porte nel dominio di trasmissione e a tutte le porte che vengono successivamente aggiunte al dominio di trasmissione.</p> <p>Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete. Tenere presente che la MTU non deve superare i 1500 byte per la gestione della porta e0M e il traffico del processore di servizio.</p>	Sì	



<p>Porte le porte vengono assegnate ai domini di trasmissione in base alla raggiungibilità. Una volta completata l'assegnazione delle porte, verificare la raggiungibilità eseguendo il <code>network port reachability show</code> comando.</p> <p>Queste porte possono essere porte fisiche, VLAN o gruppi di interfacce.</p>	Sì	
---	----	--

## Configurazione della subnet

Una subnet contiene pool di indirizzi IP e un gateway predefinito che può essere assegnato alle LIF utilizzate dalle SVM che risiedono nell'IPSpace.

- Quando si crea una LIF su una SVM, è possibile specificare il nome della subnet invece di fornire un indirizzo IP e una subnet.
- Poiché una subnet può essere configurata con un gateway predefinito, non è necessario creare il gateway predefinito in una fase separata durante la creazione di una SVM.
- Un dominio di broadcast può contenere una o più subnet.
- È possibile configurare le LIF SVM presenti su sottoreti diverse associando più di una subnet al dominio di trasmissione di IPspace.
- Ogni subnet deve contenere indirizzi IP che non si sovrappongono agli indirizzi IP assegnati ad altre subnet dello stesso IPspace.
- È possibile assegnare indirizzi IP specifici alle LIF dei dati SVM e creare un gateway predefinito per la SVM invece di utilizzare una subnet.

Informazioni	Necessario?	I tuoi valori
<p>IPSpace name (Nome IPspace): L'IPspace a cui verrà assegnata la subnet.</p> <p>Questo IPspace deve esistere.</p>	Sì	
<p>Subnet name (Nome subnet): Il nome della subnet.</p> <p>Questo nome deve essere univoco in IPspace.</p>	Sì	
<p>Broadcast domain name (Nome dominio di trasmissione): Il dominio di trasmissione a cui verrà assegnata la subnet.</p> <p>Questo dominio di trasmissione deve risiedere nell'IPspace specificato.</p>	Sì	
<p>Subnet name e mask la subnet e la maschera in cui risiedono gli indirizzi IP.</p>	Sì	

<p>Gateway (Gateway): È possibile specificare un gateway predefinito per la subnet.</p> <p>Se non si assegna un gateway durante la creazione della subnet, è possibile assegnarne uno in un secondo momento.</p>	No	
<p>Intervalli di indirizzi IP è possibile specificare un intervallo di indirizzi IP o indirizzi IP specifici.</p> <p>Ad esempio, è possibile specificare un intervallo come:</p> <p>192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145</p> <p>Se non si specifica un intervallo di indirizzi IP, l'intero intervallo di indirizzi IP nella subnet specificata sarà disponibile per l'assegnazione ai file LIF.</p>	No	
<p>Force update of LIF associations (forza aggiornamento delle associazioni LIF): Specifica se forzare l'aggiornamento delle associazioni LIF esistenti.</p> <p>Per impostazione predefinita, la creazione della subnet non riesce se le interfacce del service processor o di rete utilizzano gli indirizzi IP degli intervalli forniti.</p> <p>L'utilizzo di questo parametro consente di associare qualsiasi interfaccia indirizzata manualmente alla subnet e di eseguire correttamente il comando.</p>	No	

## Configurazione SVM

Utilizzate le SVM per fornire dati a client e host.

I valori registrati servono per la creazione di una SVM di dati predefinita. Se si sta creando una SVM di origine MetroCluster, consultare ["Guida all'installazione e alla configurazione di Fabric-Attached MetroCluster"](#) o il ["Guida all'installazione e alla configurazione di Stretch MetroCluster"](#).

Informazioni	Necessario?	I tuoi valori
SVM name (Nome SVM): Nome di dominio completo (FQDN) dell'SVM. Questo nome deve essere univoco per tutti i campionati di cluster.	Sì	
Root volume name (Nome volume root): Il nome del volume root SVM.	Sì	

Aggregate name (Nome aggregato): Il nome dell'aggregato che contiene il volume root SVM. Questo aggregato deve esistere.	Sì	
Security Style (stile di sicurezza): Lo stile di sicurezza per il volume root SVM. I valori possibili sono <b>ntfs</b> , <b>unix</b> e <b>misto</b> .	Sì	
IPSpace name (Nome IPspace): L'IPspace a cui è assegnata la SVM. Questo IPspace deve esistere.	No	
Lingua SVM impostazione della lingua predefinita da utilizzare per SVM e i relativi volumi. Se non si specifica una lingua predefinita, la lingua SVM predefinita viene impostata su <b>C.UTF-8</b> . L'impostazione della lingua SVM determina il set di caratteri utilizzato per visualizzare i nomi dei file e i dati di tutti i volumi NAS nella SVM. È possibile modificare la lingua dopo la creazione di SVM.	No	

## Configurazione LIF

Una SVM fornisce i dati ai client e agli host attraverso una o più interfacce logiche di rete (LIF).

Informazioni	Necessario?	I tuoi valori
SVM name (Nome SVM): Il nome della SVM per la LIF.	Sì	
LIF name (Nome LIF): Il nome della LIF. È possibile assegnare più LIF di dati per nodo ed è possibile assegnare LIF a qualsiasi nodo del cluster, a condizione che il nodo disponga di porte dati disponibili. Per garantire la ridondanza, è necessario creare almeno due LIF di dati per ciascuna subnet di dati e assegnare le LIF assegnate a una determinata subnet a porte home su nodi diversi. <b>Importante:</b> se si configura un server SMB per ospitare Hyper-V o SQL Server su SMB per soluzioni operative senza interruzioni, SVM deve disporre di almeno una LIF di dati su ogni nodo del cluster.	Sì	
Politica di servizio Politica di servizio per LIF. La politica di servizio definisce quali servizi di rete possono utilizzare la LIF. I servizi integrati e le policy di servizio sono disponibili per la gestione del traffico di dati e di gestione su SVM di dati e di sistema.	Sì	

Protocolli consentiti i LIF basati su IP non richiedono protocolli consentiti, utilizzare invece la riga della policy di servizio. Specificare i protocolli consentiti per LE LIF SAN sulle porte FibreChannel. Questi sono i protocolli che possono utilizzare tale LIF. I protocolli che utilizzano la LIF non possono essere modificati dopo la creazione della LIF. Specificare tutti i protocolli quando si configura la LIF.	No	
Nodo home il nodo a cui la LIF restituisce quando la LIF viene riportata alla porta home. È necessario registrare un nodo principale per ciascun LIF di dati.	Sì	
La porta principale o il dominio di broadcast hanno scelto una delle seguenti opzioni: <b>Port</b> (porta): Specificare la porta a cui l'interfaccia logica restituisce quando la LIF viene riportata alla porta home. Questa operazione viene eseguita solo per il primo LIF nella subnet di un IPspace, altrimenti non è necessaria. <b>Broadcast Domain</b> (dominio di trasmissione): Specificare il dominio di trasmissione e il sistema selezionerà la porta appropriata a cui l'interfaccia logica restituisce quando LIF viene riportato alla porta home.	Sì	
Subnet name (Nome subnet): La subnet da assegnare alla SVM. Tutti i dati LIF utilizzati per creare connessioni SMB continuamente disponibili ai server applicazioni devono trovarsi sulla stessa sottorete.	Sì (se si utilizza una subnet)	

## Configurazione DNS

È necessario configurare il DNS sulla SVM prima di creare un server NFS o SMB.

Informazioni	Necessario?	I tuoi valori
SVM name (Nome SVM): Il nome della SVM su cui si desidera creare un server NFS o SMB.	Sì	
DNS domain name (Nome dominio DNS): Elenco di nomi di dominio da aggiungere a un nome host durante l'esecuzione della risoluzione dei nomi da host a IP. Elencare prima il dominio locale, seguito dai nomi di dominio per i quali vengono eseguite più spesso query DNS.	Sì	

Indirizzi IP dei server DNS elenco degli indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server NFS o SMB. I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server SMB farà parte. Il record SRV viene utilizzato per associare il nome di un servizio al nome del computer DNS di un server che offre tale servizio. La creazione del server SMB non riesce se ONTAP non riesce a ottenere i record di posizione del servizio tramite query DNS locali. Il modo più semplice per garantire che ONTAP possa individuare i record SRV di Active Directory consiste nel configurare i server DNS integrati come server DNS di SVM. È possibile utilizzare server DNS non integrati in Active Directory, a condizione che l'amministratore DNS abbia aggiunto manualmente i record SRV alla zona DNS che contiene informazioni sui controller di dominio Active Directory. Per informazioni sui record SRV integrati in Active Directory, vedere l'argomento <a href="#">"Come funziona il supporto DNS per Active Directory su Microsoft TechNet"</a> .	Sì	
--	----	--

## Configurazione DNS dinamica

Prima di poter utilizzare il DNS dinamico per aggiungere automaticamente le voci DNS ai server DNS integrati in Active Directory, è necessario configurare il DNS dinamico (DDNS) su SVM.

I record DNS vengono creati per ogni LIF di dati sulla SVM. Creando più LIFS di dati su SVM, è possibile bilanciare il carico delle connessioni client agli indirizzi IP dei dati assegnati. Il carico DNS bilancia le connessioni effettuate utilizzando il nome host con gli indirizzi IP assegnati in modo round-robin.

Informazioni	Necessario?	I tuoi valori
Nome SVM la SVM su cui si desidera creare un server NFS o SMB.	Sì	
Se utilizzare DDNS specifica se utilizzare DDNS. I server DNS configurati su SVM devono supportare DDNS. Per impostazione predefinita, il DDNS è disattivato.	Sì	

Se utilizzare DDNS sicuro DDNS sicuro è supportato solo con DNS integrato in Active Directory. Se il DNS integrato in Active Directory consente solo aggiornamenti DDNS sicuri, il valore di questo parametro deve essere true. Per impostazione predefinita, il DDNS sicuro è disattivato. È possibile attivare il DDNS sicuro solo dopo la creazione di un server SMB o di un account Active Directory per SVM.	No	
FQDN del dominio DNS l'FQDN del dominio DNS. È necessario utilizzare lo stesso nome di dominio configurato per i servizi dei nomi DNS su SVM.	No	

## Flusso di lavoro di failover del percorso NAS (ONTAP 9,7 e versioni precedenti)

### Configurazione del failover del percorso NAS (ONTAP 9,7 e versioni precedenti)

Questo flusso di lavoro guida l'utente attraverso le fasi di configurazione della rete per impostare il failover del percorso NAS per ONTAP 9.0 - 9.7. Questo flusso di lavoro presuppone quanto segue:

- Si desidera utilizzare le Best practice di failover del percorso NAS che semplificano la configurazione di rete.
- Si desidera utilizzare la CLI, non System Manager.
- Si sta configurando la rete su un nuovo sistema che esegue ONTAP da 9.0 a 9.7.

Se si esegue una versione di ONTAP successiva alla 9.7, è necessario utilizzare la procedura di failover del percorso NAS per ONTAP 9.8 o versione successiva:

- [Workflow di failover del percorso NAS di ONTAP 9.8 e versioni successive](#)

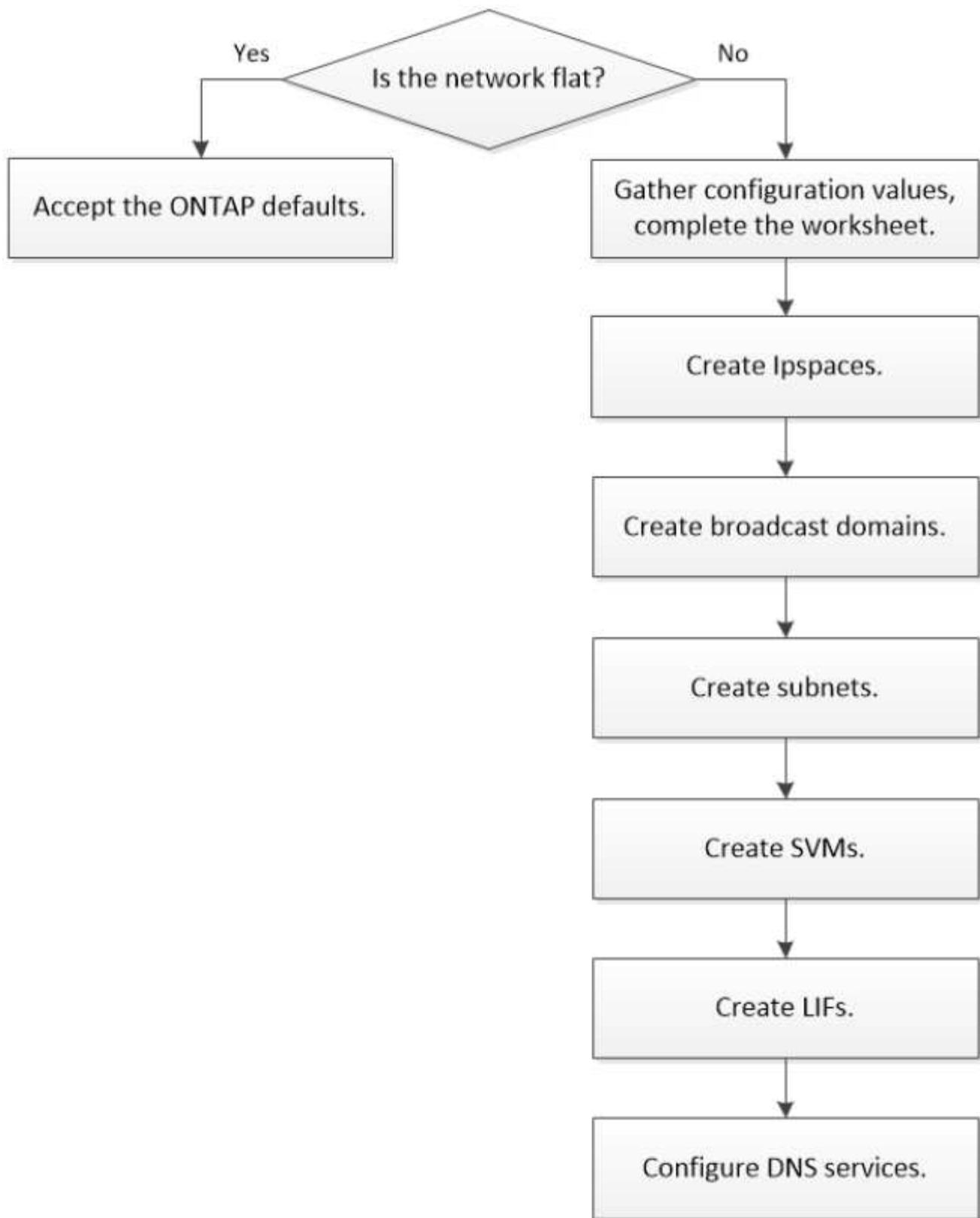
Per ulteriori informazioni sui componenti di rete e sulla gestione, è necessario utilizzare il materiale di riferimento per la gestione della rete:

- [Panoramica sulla gestione della rete](#)

### Flusso di lavoro (ONTAP 9,7 e versioni precedenti)

Se hai già familiarità con i concetti di base del networking, potresti risparmiare tempo nell'impostazione della rete esaminando questo flusso di lavoro pratico per la configurazione del failover del percorso NAS.

Un LIF NAS esegue automaticamente la migrazione a una porta di rete esistente dopo un errore di collegamento sulla porta corrente. Se la rete è piatta, è possibile utilizzare le impostazioni predefinite di ONTAP per gestire il failover del percorso. In caso contrario, è necessario configurare il failover del percorso seguendo i passaggi di questo flusso di lavoro.



Un LIF SAN non esegue la migrazione (a meno che non venga spostato manualmente dopo l'errore di collegamento). Invece, la tecnologia multipathing sull'host trasferisce il traffico a un LIF diverso. Per ulteriori informazioni, vedere ["Amministrazione SAN"](#).

**1****"Completare il foglio di lavoro"**

Utilizzare il foglio di lavoro per pianificare il failover del percorso NAS.

**2****"Creare IPspaces"**

Crea uno spazio di indirizzi IP distinto per ciascuna SVM in un cluster.

**3****"Creare domini di broadcast"**

Creare domini di broadcast.

**4****"Creare sottoreti"**

Creare subnet.

**5****"Creare SVM"**

Creazione di SVM per fornire dati ai client.

**6****"Creare LIF"**

Creare LIF sulle porte che servono per accedere ai dati.

**7****"Configurare i servizi DNS per la SVM"**

Configurare i servizi DNS per la SVM prima di creare un server NFS o SMB.

## Foglio di lavoro per la configurazione del failover del percorso NAS (ONTAP 9,7 e versioni precedenti)

Completare tutte le sezioni del foglio di lavoro prima di configurare il failover del percorso NAS.

### Configurazione di IPSpace

È possibile utilizzare un IPSpace per creare uno spazio di indirizzi IP distinto per ogni SVM in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

Informazioni	Necessario?	I tuoi valori
--------------	-------------	---------------



Nome IPSpace	Sì	
<ul style="list-style-type: none"> <li>• Il nome di IPSpace.</li> <li>• Il nome deve essere univoco nel cluster.</li> </ul>		

## Configurazione del dominio di trasmissione


Un dominio di trasmissione raggruppa le porte che appartengono alla stessa rete Layer 2 e imposta la MTU per le porte del dominio di trasmissione.

I domini di broadcast vengono assegnati a un IPSpace. Un IPSpace può contenere uno o più domini di broadcast.



La porta a cui si verifica il failover di LIF deve essere membro del gruppo di failover per LIF. Quando si crea un dominio di broadcast, ONTAP crea automaticamente un gruppo di failover con lo stesso nome. Il gruppo di failover contiene tutte le porte assegnate al dominio di trasmissione.

Informazioni	Necessario?	I tuoi valori
Nome IPSpace	Sì	
<ul style="list-style-type: none"> <li>• L'IPSpace a cui è assegnato il dominio di trasmissione.</li> <li>• IPSpace deve esistere.</li> </ul>		
Nome di dominio di trasmissione	Sì	
<ul style="list-style-type: none"> <li>• Il nome del dominio di trasmissione.</li> <li>• Questo nome deve essere univoco in IPSpace.</li> </ul>		

<p>MTU</p> <ul style="list-style-type: none"> <li>• MTU del dominio di trasmissione.</li> <li>• Generalmente impostato su <b>1500</b> o <b>9000</b>.</li> <li>• Il valore MTU viene applicato a tutte le porte nel dominio di trasmissione e a tutte le porte che vengono successivamente aggiunte al dominio di trasmissione.</li> </ul> <div>  <p>Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete. Tenere presente che la MTU non deve superare i 1500 byte per la gestione della porta e0M e il traffico del processore di servizio.</p> </div>	<p>Sì</p>	
<p>Porte</p> <ul style="list-style-type: none"> <li>• Le porte di rete da aggiungere al dominio di trasmissione.</li> <li>• Le porte assegnate al dominio di trasmissione possono essere porte fisiche, VLAN o gruppi di interfacce (ifgroup).</li> <li>• Se una porta si trova in un altro dominio di trasmissione, deve essere rimossa prima di poter essere aggiunta al dominio di trasmissione.</li> <li>• Le porte vengono assegnate specificando sia il nome del nodo che la porta, ad esempio node1:e0d.</li> </ul>	<p>Sì</p>	

## Configurazione della subnet

Una subnet contiene pool di indirizzi IP e un gateway predefinito che può essere assegnato alle LIF utilizzate dalle SVM che risiedono nell'IPSpace.

- Quando si crea una LIF su una SVM, è possibile specificare il nome della subnet invece di fornire un indirizzo IP e una subnet.

- Poiché una subnet può essere configurata con un gateway predefinito, non è necessario creare il gateway predefinito in una fase separata durante la creazione di una SVM.
- Un dominio di broadcast può contenere una o più subnet. È possibile configurare le LIF SVM presenti su sottoreti diverse associando più di una subnet al dominio di trasmissione di IPspace.
- Ogni subnet deve contenere indirizzi IP che non si sovrappongono agli indirizzi IP assegnati ad altre subnet dello stesso IPspace.
- È possibile assegnare indirizzi IP specifici alle LIF dei dati SVM e creare un gateway predefinito per la SVM invece di utilizzare una subnet.

Informazioni	Necessario?	I tuoi valori
<b>Nome IPspace</b> <ul style="list-style-type: none"> <li>• L'IPspace a cui verrà assegnata la subnet.</li> <li>• IPspace deve esistere.</li> </ul>	Sì	
<b>Nome della subnet</b> <ul style="list-style-type: none"> <li>• Il nome della subnet.</li> <li>• Il nome deve essere univoco in IPspace.</li> </ul>	Sì	
<b>Nome di dominio di trasmissione</b> <ul style="list-style-type: none"> <li>• Il dominio di trasmissione a cui verrà assegnata la subnet.</li> <li>• Il dominio di trasmissione deve risiedere nell'IPspace specificato.</li> </ul>	Sì	
<b>Subnet name e mask</b> <ul style="list-style-type: none"> <li>• Subnet e maschera in cui risiedono gli indirizzi IP.</li> </ul>	Sì	
<b>Gateway</b> <ul style="list-style-type: none"> <li>• È possibile specificare un gateway predefinito per la subnet.</li> <li>• Se non si assegna un gateway quando si crea la subnet, è possibile assegnarne uno in qualsiasi momento.</li> </ul>	No	

<p>Intervalli di indirizzi IP</p> <ul style="list-style-type: none"> <li>• È possibile specificare un intervallo di indirizzi IP o indirizzi IP specifici. Ad esempio, è possibile specificare un intervallo come: 192.168.1.1– 192.168.1.100, 192.168.1.112, 192.168.1.145</li> <li>• Se non si specifica un intervallo di indirizzi IP, l'intero intervallo di indirizzi IP nella subnet specificata sarà disponibile per l'assegnazione ai file LIF.</li> </ul>	No	
<p>Forzare l'aggiornamento delle associazioni LIF</p> <ul style="list-style-type: none"> <li>• Specifica se forzare l'aggiornamento delle associazioni LIF esistenti.</li> <li>• Per impostazione predefinita, la creazione della subnet non riesce se le interfacce del service processor o di rete utilizzano gli indirizzi IP degli intervalli forniti.</li> <li>• L'utilizzo di questo parametro consente di associare qualsiasi interfaccia indirizzata manualmente alla subnet e di eseguire correttamente il comando.</li> </ul>	No	

## Configurazione SVM

Utilizzate le SVM per fornire dati a client e host.

I valori registrati servono per la creazione di una SVM di dati predefinita. Se si sta creando una SVM di origine MetroCluster, consultare ["Installare un MetroCluster collegato al fabric"](#) o il ["Installare un MetroCluster stretch"](#).

Informazioni	Necessario?	I tuoi valori
--------------	-------------	---------------


<p>Nome SVM</p> <ul style="list-style-type: none"> <li>• Il nome della SVM.</li> <li>• È necessario utilizzare un nome di dominio completo (FQDN) per garantire nomi SVM univoci nei vari campionati di cluster.</li> </ul>	Sì	
<p>Nome del volume root</p> <ul style="list-style-type: none"> <li>• Il nome del volume root SVM.</li> </ul>	Sì	
<p>Nome dell'aggregato</p> <ul style="list-style-type: none"> <li>• Il nome dell'aggregato che contiene il volume root SVM.</li> <li>• Questo aggregato deve esistere.</li> </ul>	Sì	
<p>Stile di sicurezza</p> <ul style="list-style-type: none"> <li>• Lo stile di sicurezza per il volume root SVM.</li> <li>• I valori possibili sono <b>ntfs</b>, <b>unix</b> e <b>misto</b>.</li> </ul>	Sì	
<p>Nome IPSpace</p> <ul style="list-style-type: none"> <li>• L'IPSpace a cui è assegnata la SVM.</li> <li>• Questo IPSpace deve esistere.</li> </ul>	No	

<p>Impostazione della lingua SVM</p> <ul style="list-style-type: none"> <li>• La lingua predefinita da utilizzare per SVM e i relativi volumi.</li> <li>• Se non si specifica una lingua predefinita, la lingua SVM predefinita viene impostata su <b>C.UTF-8</b>.</li> <li>• L'impostazione della lingua SVM determina il set di caratteri utilizzato per visualizzare i nomi dei file e i dati di tutti i volumi NAS nella SVM. È possibile modificare la lingua dopo la creazione di SVM.</li> </ul>	No	
---	----	--

## Configurazione LIF

Una SVM fornisce i dati ai client e agli host attraverso una o più interfacce logiche di rete (LIF).

Informazioni	Necessario?	I tuoi valori
<p>Nome SVM</p> <ul style="list-style-type: none"> <li>• Il nome della SVM per la LIF.</li> </ul>	Sì	
<p>Nome LIF</p> <ul style="list-style-type: none"> <li>• Il nome del LIF.</li> <li>• È possibile assegnare più LIF di dati per nodo ed è possibile assegnare LIF a qualsiasi nodo del cluster, a condizione che il nodo disponga di porte dati disponibili.</li> <li>• Per garantire la ridondanza, è necessario creare almeno due LIF di dati per ciascuna subnet di dati e assegnare le LIF assegnate a una determinata subnet a porte home su nodi diversi. <b>Importante:</b> se si configura un server SMB per ospitare Hyper-V o SQL Server su SMB per soluzioni operative senza interruzioni, SVM deve disporre di almeno una LIF di dati su ogni nodo del cluster.</li> </ul>	Sì	

<p>Ruolo LIF</p> <ul style="list-style-type: none"> <li>• Il ruolo della LIF.</li> <li>• Ai file LIF dei dati viene assegnato il ruolo dei dati.</li> </ul>	<p>Sì, estratto da ONTAP 9.6</p>	<p>dati</p>
<p>Politica di servizio</p> <p>Politica di servizio per LIF. La politica di servizio definisce quali servizi di rete possono utilizzare la LIF. I servizi integrati e le policy di servizio sono disponibili per la gestione del traffico di dati e di gestione su SVM di dati e di sistema.</p>	<p>Sì, a partire da ONTAP 9.6</p>	
<p>Protocolli consentiti</p> <ul style="list-style-type: none"> <li>• I protocolli che possono utilizzare LIF.</li> <li>• Per impostazione predefinita, SMB, NFS e FlexCache sono consentiti. Il protocollo FlexCache consente di utilizzare un volume come volume di origine per un volume FlexCache su un sistema che esegue Data ONTAP in modalità 7.</li> </ul> <div>  <p>I protocolli che utilizzano la LIF non possono essere modificati dopo la creazione della LIF. Specificare tutti i protocolli quando si configura la LIF.</p> </div>	<p>No</p>	
<p>Nodo principale</p> <ul style="list-style-type: none"> <li>• Il nodo a cui la LIF restituisce quando la LIF viene riportata alla porta home.</li> <li>• È necessario registrare un nodo principale per ciascun LIF di dati.</li> </ul>	<p>Sì</p>	

Porta home o dominio di broadcast <ul style="list-style-type: none"> <li>• La porta a cui l'interfaccia logica ritorna quando la LIF viene riportata alla porta home.</li> <li>• È necessario registrare una porta home per ciascun LIF di dati.</li> </ul>	Sì	
Nome della subnet <ul style="list-style-type: none"> <li>• Subnet da assegnare alla SVM.</li> <li>• Tutti i dati LIF utilizzati per creare connessioni SMB continuamente disponibili ai server applicazioni devono trovarsi sulla stessa sottorete.</li> </ul>	Sì (se si utilizza una subnet)	

## Configurazione DNS

È necessario configurare il DNS sulla SVM prima di creare un server NFS o SMB.

Informazioni	Necessario?	I tuoi valori
Nome SVM <ul style="list-style-type: none"> <li>• Il nome della SVM su cui si desidera creare un server NFS o SMB.</li> </ul>	Sì	
Nome di dominio DNS <ul style="list-style-type: none"> <li>• Un elenco di nomi di dominio da aggiungere a un nome host quando si esegue la risoluzione dei nomi da host a IP.</li> <li>• Elencare prima il dominio locale, seguito dai nomi di dominio per i quali vengono eseguite più spesso query DNS.</li> </ul>	Sì	



<p>Indirizzi IP dei server DNS</p> <ul style="list-style-type: none"> <li>• Elenco di indirizzi IP dei server DNS che forniscono la risoluzione dei nomi per il server NFS o SMB.</li> <li>• I server DNS elencati devono contenere i record di posizione del servizio (SRV) necessari per individuare i server LDAP di Active Directory e i controller di dominio per il dominio a cui il server SMB farà parte. Il record SRV viene utilizzato per associare il nome di un servizio al nome del computer DNS di un server che offre tale servizio. La creazione del server SMB non riesce se ONTAP non riesce a ottenere i record di posizione del servizio tramite query DNS locali. Il modo più semplice per garantire che ONTAP possa individuare i record SRV di Active Directory consiste nel configurare i server DNS integrati come server DNS di SVM. È possibile utilizzare server DNS non integrati in Active Directory, a condizione che l'amministratore DNS abbia aggiunto manualmente i record SRV alla zona DNS che contiene informazioni sui controller di dominio Active Directory.</li> <li>• Per informazioni sui record SRV integrati in Active Directory, vedere l'argomento <a href="#">"Come funziona il supporto DNS per Active Directory su Microsoft TechNet"</a>.</li> </ul>	<p>Sì</p>	
---	-----------	--

## Configurazione DNS dinamica

Prima di poter utilizzare il DNS dinamico per aggiungere automaticamente le voci DNS ai server DNS integrati in Active Directory, è necessario configurare il DNS dinamico (DDNS) su SVM.

I record DNS vengono creati per ogni LIF di dati sulla SVM. Creando più LIFS di dati su SVM, è possibile bilanciare il carico delle connessioni client agli indirizzi IP dei dati assegnati. Il carico DNS bilancia le

connessioni effettuate utilizzando il nome host con gli indirizzi IP assegnati in modo round-robin.

Informazioni	Necessario?	I tuoi valori
<b>Nome SVM</b> <ul style="list-style-type: none"><li>• SVM su cui si desidera creare un server NFS o SMB.</li></ul>	Sì	
<b>Se utilizzare DDNS</b> <ul style="list-style-type: none"><li>• Specifica se utilizzare DDNS.</li><li>• I server DNS configurati su SVM devono supportare DDNS. Per impostazione predefinita, il DDNS è disattivato.</li></ul>	Sì	
<b>Se utilizzare DDNS sicuro</b> <ul style="list-style-type: none"><li>• Il DDNS sicuro è supportato solo con il DNS integrato in Active Directory.</li><li>• Se il DNS integrato in Active Directory consente solo aggiornamenti DDNS sicuri, il valore di questo parametro deve essere true.</li><li>• Per impostazione predefinita, il DDNS sicuro è disattivato.</li><li>• È possibile attivare il DDNS sicuro solo dopo la creazione di un server SMB o di un account Active Directory per SVM.</li></ul>	No	
<b>FQDN del dominio DNS</b> <ul style="list-style-type: none"><li>• L'FQDN del dominio DNS.</li><li>• È necessario utilizzare lo stesso nome di dominio configurato per i servizi dei nomi DNS su SVM.</li></ul>	No	

## Porte di rete

### Configurare le porte di rete

Le porte sono porte fisiche (NIC) o virtualizzate, ad esempio gruppi di interfacce o VLAN.

Le Virtual Local Area Network (VLAN) e i gruppi di interfacce costituiscono le porte virtuali. I gruppi di interfacce trattano diverse porte fisiche come una singola porta, mentre le VLAN suddividono una porta fisica in più porte logiche separate.

- **Porte fisiche:** Le LIF possono essere configurate direttamente su porte fisiche.
- **Interface group (Gruppo di interfacce):** Aggregato di porte contenente due o più porte fisiche che fungono da singola porta di linea. Un gruppo di interfacce può essere monomodale, multimodale o multimodale dinamica.
- **VLAN:** Porta logica che riceve e invia traffico con tag VLAN (standard IEEE 802.1Q). Le caratteristiche della porta VLAN includono l'ID VLAN della porta. Le porte fisiche sottostanti o del gruppo di interfacce sono considerate porte di trunk VLAN e le porte dello switch connesso devono essere configurate per collegare gli ID VLAN.

La porta fisica sottostante o le porte del gruppo di interfacce per una porta VLAN possono continuare a ospitare le LIF, che trasmettono e ricevono traffico senza tag.

- **Virtual IP (VIP) port (porta IP virtuale):** Porta logica utilizzata come porta home per un LIF VIP. Le porte VIP vengono create automaticamente dal sistema e supportano solo un numero limitato di operazioni. Le porte VIP sono supportate a partire da ONTAP 9.5.

La convenzione di denominazione delle porte è *enumberletter*:

- Il primo carattere descrive il tipo di porta. "E" rappresenta Ethernet.
- Il secondo carattere indica lo slot numerato in cui si trova l'adattatore porta.
- Il terzo carattere indica la posizione della porta su un adattatore multiporta. "a" indica la prima porta, "b" la seconda porta e così via.

Ad esempio, e0b Indica che una porta Ethernet è la seconda porta sulla scheda madre del nodo.

Le VLAN devono essere denominate utilizzando la sintassi `port_name-vlan-id`.

`port_name` specifica la porta fisica o il gruppo di interfacce.

`vlan-id` Specifica l'identificazione della VLAN sulla rete. Ad esempio, e1c-80 È un nome VLAN valido.

## Configurare le porte di rete

### Combina le porte fisiche per creare gruppi di interfacce

Un gruppo di interfacce, noto anche come LAG (link Aggregation Group), viene creato combinando due o più porte fisiche sullo stesso nodo in una singola porta logica. La porta logica offre maggiore resilienza, maggiore disponibilità e condivisione del carico.

#### Tipi di gruppi di interfacce

Il sistema storage supporta tre tipi di gruppi di interfacce: Single-mode, static multimode e Dynamic Multimode. Ciascun gruppo di interfacce fornisce diversi livelli di tolleranza agli errori. I gruppi di interfacce multimodali forniscono metodi per il bilanciamento del carico del traffico di rete.

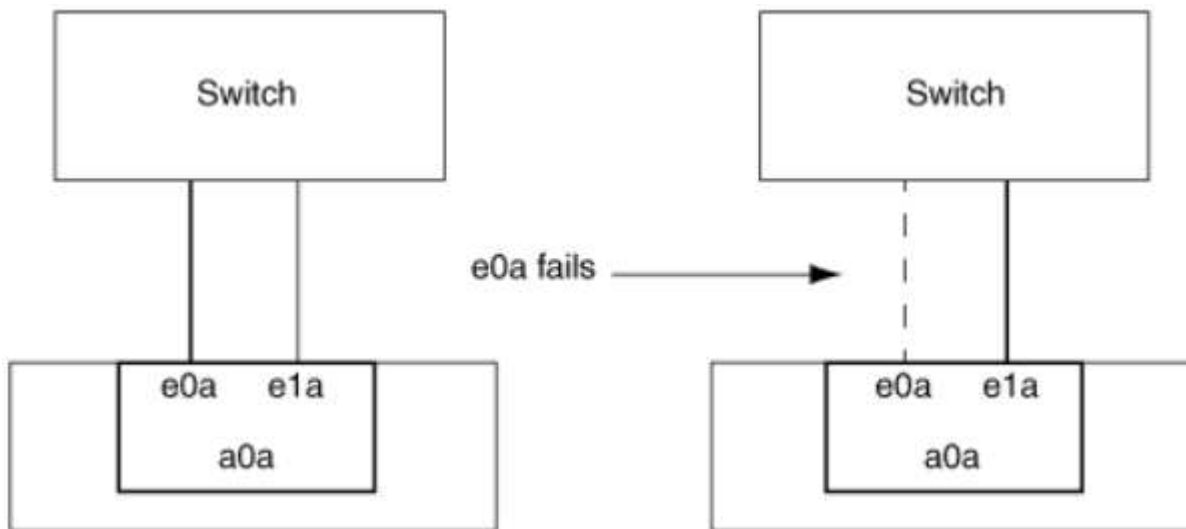
## Caratteristiche dei gruppi di interfacce single-mode

In un gruppo di interfacce a modalità singola, è attiva solo una delle interfacce del gruppo di interfacce. Le altre interfacce sono in standby, pronte per essere utilizzate in caso di guasto dell'interfaccia attiva.

Caratteristiche di un gruppo di interfacce single-mode:

- Per il failover, il cluster monitora il collegamento attivo e controlla il failover. Poiché il cluster monitora il collegamento attivo, non è necessaria alcuna configurazione dello switch.
- In un gruppo di interfacce a modalità singola, in standby possono essere presenti più interfacce.
- Se un gruppo di interfacce single-mode si estende su più switch, è necessario collegare gli switch con un collegamento Inter-Switch (ISL).
- Per un gruppo di interfacce a modalità singola, le porte dello switch devono trovarsi nello stesso dominio di trasmissione.
- I pacchetti ARP per il monitoraggio dei collegamenti, che hanno un indirizzo di origine 0.0.0.0, vengono inviati sulle porte per verificare che le porte si trovino nello stesso dominio di trasmissione.

La figura riportata di seguito mostra un esempio di gruppo di interfacce a modalità singola. Nella figura, e0a ed e1a fanno parte del gruppo di interfacce single-mode di a0a. Se l'interfaccia attiva, e0a, si guasta, l'interfaccia e1a di standby assume il controllo e mantiene la connessione allo switch.



Per ottenere la funzionalità single-mode, si consiglia di utilizzare i gruppi di failover. Utilizzando un gruppo di failover, la seconda porta può ancora essere utilizzata per altre LIF e non deve rimanere inutilizzata. Inoltre, i gruppi di failover possono estendersi su più di due porte e possono estendersi su più nodi.

## Caratteristiche dei gruppi di interfacce statiche multimodali

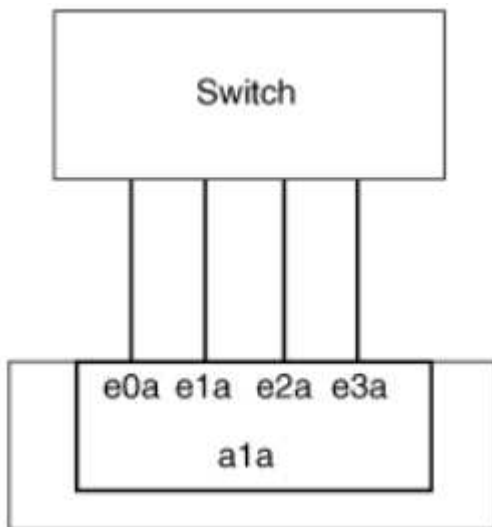
L'implementazione del gruppo di interfacce statiche multimodali in ONTAP è conforme allo standard IEEE 802.3ad (statico). Qualsiasi switch che supporti gli aggregati, ma non dispone di uno scambio di pacchetti di controllo per la configurazione di un aggregato, può essere utilizzato con gruppi di interfacce statiche multimodali.

I gruppi di interfacce statiche multimodali non sono conformi allo standard IEEE 802.3ad (dinamico), noto anche come link Aggregation Control Protocol (LACP). LACP è equivalente al protocollo di aggregazione delle porte (PAgP), il protocollo di aggregazione dei collegamenti proprietario di Cisco.

Di seguito sono riportate le caratteristiche di un gruppo di interfacce statiche multimodali:

- Tutte le interfacce del gruppo di interfacce sono attive e condividono un singolo indirizzo MAC.
  - Più connessioni individuali sono distribuite tra le interfacce nel gruppo di interfacce.
  - Ogni connessione o sessione utilizza un'interfaccia all'interno del gruppo di interfacce. Quando si utilizza lo schema di bilanciamento del carico sequenziale, tutte le sessioni vengono distribuite tra i collegamenti disponibili pacchetti per pacchetto e non sono associate a una particolare interfaccia del gruppo di interfacce.
- I gruppi di interfacce statiche multimodali possono essere ripristinati da un guasto di un massimo di interfacce "n-1", dove n è il numero totale di interfacce che formano il gruppo di interfacce.
- Se una porta non funziona o viene scollegata, il traffico che stava attraversando il collegamento guasto viene automaticamente ridistribuito a una delle interfacce rimanenti.
- I gruppi di interfacce statiche multimodali possono rilevare una perdita di collegamento, ma non possono rilevare una perdita di connettività al client o configurazioni errate dello switch che potrebbero influire sulla connettività e sulle prestazioni.
- Un gruppo di interfacce statiche multimodali richiede uno switch che supporti l'aggregazione di collegamenti su più porte di switch. Lo switch è configurato in modo che tutte le porte a cui sono collegati i collegamenti di un gruppo di interfacce facciano parte di una singola porta logica. Alcuni switch potrebbero non supportare l'aggregazione di collegamenti delle porte configurate per i frame jumbo. Per ulteriori informazioni, consultare la documentazione del fornitore dello switch.
- Sono disponibili diverse opzioni di bilanciamento del carico per distribuire il traffico tra le interfacce di un gruppo di interfacce statiche multimodali.

La figura riportata di seguito mostra un esempio di gruppo di interfacce multimodali statiche. Le interfacce e0a, e1a, e2a e e3a fanno parte del gruppo di interfacce multimodali a1a. Tutte e quattro le interfacce nel gruppo di interfacce multimodali a1a sono attive.



Esistono diverse tecnologie che consentono di distribuire il traffico in un singolo collegamento aggregato su più switch fisici. Le tecnologie utilizzate per abilitare questa funzionalità variano a seconda dei prodotti di rete. I gruppi di interfacce statiche multimodali in ONTAP sono conformi agli standard IEEE 802.3. Se si dice che una particolare tecnologia di aggregazione di collegamenti a switch multipli interagiti con o sia conforme agli standard IEEE 802.3, dovrebbe funzionare con ONTAP.

Lo standard IEEE 802.3 stabilisce che la periferica trasmittente in un collegamento aggregato determina l'interfaccia fisica per la trasmissione. Pertanto, ONTAP è responsabile solo della distribuzione del traffico in

uscita e non può controllare il modo in cui arrivano i frame in entrata. Se si desidera gestire o controllare la trasmissione del traffico in entrata su un collegamento aggregato, tale trasmissione deve essere modificata sul dispositivo di rete direttamente connesso.

## **Gruppo di interfacce Multimode dinamiche**

I gruppi di interfacce dinamiche multimodali implementano il protocollo LACP (Link Aggregation Control Protocol) per comunicare l'appartenenza del gruppo allo switch direttamente collegato. LACP consente di rilevare lo stato di perdita del collegamento e l'impossibilità per il nodo di comunicare con la porta dello switch direct-attached.

L'implementazione del gruppo di interfacce multimodali dinamiche in ONTAP è conforme allo standard IEEE 802.3 ad (802.1 AX). ONTAP non supporta il protocollo di aggregazione delle porte (PAgP), un protocollo di aggregazione dei collegamenti proprietario di Cisco.

Un gruppo di interfacce multimodali dinamiche richiede uno switch che supporti LACP.

ONTAP implementa LACP in modalità attiva non configurabile che funziona bene con gli switch configurati in modalità attiva o passiva. ONTAP implementa i timer LACP lunghi e brevi (per l'utilizzo con valori non configurabili 3 secondi e 90 secondi), come specificato in IEEE 802.3 ad (802.1AX).

L'algoritmo di bilanciamento del carico ONTAP determina la porta membro da utilizzare per trasmettere il traffico in uscita e non controlla la modalità di ricezione dei frame in entrata. Lo switch determina il membro (singola porta fisica) del proprio gruppo di canali di porte da utilizzare per la trasmissione, in base all'algoritmo di bilanciamento del carico configurato nel gruppo di canali di porte dello switch. Pertanto, la configurazione dello switch determina la porta membro (singola porta fisica) del sistema di storage per ricevere il traffico. Per ulteriori informazioni sulla configurazione dello switch, consultare la documentazione del fornitore dello switch.

Se una singola interfaccia non riesce a ricevere pacchetti di protocollo LACP successivi, quella singola interfaccia viene contrassegnata come "lag\_inactive" nell'output del comando "ifgrp status". Il traffico esistente viene automaticamente reindirizzato a tutte le interfacce attive rimanenti.

Quando si utilizzano gruppi di interfacce multimodali dinamiche, si applicano le seguenti regole:

- I gruppi di interfacce multimodali dinamiche devono essere configurati per utilizzare i metodi di bilanciamento del carico basati su porta, IP, MAC o round robin.
- In un gruppo di interfacce multimodali dinamiche, tutte le interfacce devono essere attive e condividere un singolo indirizzo MAC.

La figura riportata di seguito mostra un esempio di gruppo di interfacce multimodali dinamiche. Le interfacce e0a, e1a, e2a e e3a fanno parte del gruppo di interfacce multimodali a1a. Tutte e quattro le interfacce nel gruppo di interfacce dinamiche multimodali a1a sono attive.



### Bilanciamento del carico in gruppi di interfacce multimodali

È possibile garantire che tutte le interfacce di un gruppo di interfacce multimodali siano utilizzate in modo uguale per il traffico in uscita utilizzando l'indirizzo IP, l'indirizzo MAC, i metodi di bilanciamento del carico sequenziali o basati su porta per distribuire il traffico di rete in modo uniforme sulle porte di rete di un gruppo di interfacce multimodali.

Il metodo di bilanciamento del carico per un gruppo di interfacce multimodali può essere specificato solo quando viene creato il gruppo di interfacce.

**Best Practice:** Si consiglia di eseguire il bilanciamento del carico basato su porta quando possibile. Utilizzare il bilanciamento del carico basato su porta, a meno che non vi sia un motivo o una limitazione specifica nella rete che lo impedisca.

### Bilanciamento del carico basato su porta

Il metodo consigliato è il bilanciamento del carico basato su porta.

È possibile equalizzare il traffico su un gruppo di interfacce multimodali in base alle porte TCP/UDP (Transport Layer) utilizzando il metodo di bilanciamento del carico basato su porta.

Il metodo di bilanciamento del carico basato su porta utilizza un algoritmo di hashing rapido sugli indirizzi IP di origine e di destinazione insieme al numero di porta del layer di trasporto.

### Bilanciamento del carico degli indirizzi IP e MAC

Il bilanciamento del carico degli indirizzi IP e MAC è un metodo per equalizzare il traffico su gruppi di interfacce multimodali.

Questi metodi di bilanciamento del carico utilizzano un algoritmo di hashing rapido sugli indirizzi di origine e di destinazione (indirizzo IP e indirizzo MAC). Se il risultato dell'algoritmo di hashing viene mappato su un'interfaccia che non si trova nello stato UP link, viene utilizzata la successiva interfaccia attiva.



Non selezionare il metodo di bilanciamento del carico dell'indirizzo MAC quando si creano gruppi di interfacce su un sistema che si connette direttamente a un router. In tale configurazione, per ogni frame IP in uscita, l'indirizzo MAC di destinazione è l'indirizzo MAC del router. Di conseguenza, viene utilizzata una sola interfaccia del gruppo di interfacce.

Il bilanciamento del carico degli indirizzi IP funziona allo stesso modo per gli indirizzi IPv4 e IPv6.

### **Bilanciamento sequenziale del carico**

È possibile utilizzare il bilanciamento del carico sequenziale per distribuire in modo uguale pacchetti tra più link utilizzando un algoritmo round robin. È possibile utilizzare l'opzione sequenziale per il bilanciamento del carico del traffico di una singola connessione su più collegamenti per aumentare il throughput di una singola connessione.

Tuttavia, poiché il bilanciamento del carico sequenziale può causare l'erogazione di pacchetti fuori servizio, le performance possono risultare estremamente scarse. Pertanto, il bilanciamento del carico sequenziale non è generalmente consigliato.

### **Creare un gruppo di interfacce o un LAG**

È possibile creare un gruppo di interfacce o un LAG (single-mode, static multimode o Dynamic Multimode (LACP)) per presentare una singola interfaccia ai client combinando le funzionalità delle porte di rete aggregate.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:



## System Manager

### Utilizzare System Manager per creare un LAG

#### Fasi

1. Selezionare **Network > Ethernet port > + link Aggregation Group** per creare un LAG.
2. Selezionare il nodo dall'elenco a discesa.
3. Scegliere tra le seguenti opzioni:
  - a. ONTAP (Seleziona dominio broadcast) per **selezionare automaticamente il dominio di broadcast (scelta consigliata)**.
  - b. Per selezionare manualmente un dominio di trasmissione.
4. Selezionare le porte per il LAG.
5. Selezionare la modalità:
  - a. Singolo: Viene utilizzata una sola porta alla volta.
  - b. Multiplo: Tutte le porte possono essere utilizzate contemporaneamente.
  - c. LACP: Il protocollo LACP determina le porte che è possibile utilizzare.
6. Selezionare il bilanciamento del carico:
  - a. Basato su IP
  - b. Basato SU MAC
  - c. Porta
  - d. Sequenziale
7. Salvare le modifiche.

The screenshot shows the 'Add Link Aggregation Group' configuration page in the ONTAP System Manager. The left sidebar contains a navigation menu with categories: DASHBOARD, INSIGHTS, STORAGE, and NETWORK. The 'NETWORK' section is expanded, showing 'Ethernet Ports' as the selected option. The main content area is titled 'Add Link Aggregation Group' and includes the following configuration options:

- NODE:** A dropdown menu showing 'sti47-vsrm-ucs521e'.
- BROADCAST DOMAIN:** A dropdown menu with the option 'Automatically select broadcast domain (Recommended)'. A red arrow points to this dropdown with a note: 'Note: Instead of a global switch or checkbox, what if we expose BD dropdown with "Automatic" as a default selection?'.
- PORTS TO INCLUDE:** Two checkboxes labeled 'e0e' and 'e0f', both of which are unchecked.
- MODE:** Three radio button options: 'Single' (selected), 'Multiple', and 'LACP'. Descriptions are provided for each mode: 'Single' (Only one port is used at a time), 'Multiple' (All ports can be used simultaneously), and 'LACP' (The LACP protocol determines the ports that can be used).
- LOAD DISTRIBUTION:** Two radio button options: 'IP based' (selected) and 'MAC based'. Descriptions are provided for each: 'IP based' (Network traffic is distributed based on the destination IP address) and 'MAC based' (Network traffic is distributed based on the next-hop MAC addresses).

#### CLI

## Utilizzare la CLI per creare un gruppo di interfacce

Per un elenco completo delle restrizioni di configurazione applicabili ai gruppi di interfacce delle porte, vedere `network port ifgrp add-port` pagina man.

Quando si crea un gruppo di interfacce multimodali, è possibile specificare uno dei seguenti metodi di bilanciamento del carico:

- `port`: Il traffico di rete viene distribuito in base alle porte TCP/UDP (Transport Layer). Si tratta del metodo consigliato per il bilanciamento del carico.
- `mac`: Il traffico di rete viene distribuito in base agli indirizzi MAC.
- `ip`: Il traffico di rete viene distribuito in base agli indirizzi IP.
- `sequential`: Il traffico di rete viene distribuito man mano che viene ricevuto.



L'indirizzo MAC di un gruppo di interfacce è determinato dall'ordine delle porte sottostanti e dalla modalità di inizializzazione di queste porte durante l'avvio. Pertanto, non si deve presumere che l'indirizzo MAC di ifgrp sia persistente durante i riavvii o gli aggiornamenti ONTAP.

### Fase

Utilizzare `network port ifgrp create` per creare un gruppo di interfacce.

I gruppi di interfacce devono essere denominati utilizzando la sintassi `a<number><letter>`. Ad esempio, `a0a`, `a0b`, `a1c` e `a2a` sono nomi di gruppi di interfacce validi.

Per ulteriori informazioni su questo comando, vedere ["Comandi di ONTAP 9"](#).

Nell'esempio seguente viene illustrato come creare un gruppo di interfacce denominato `a0a` con una funzione di distribuzione di porta e una modalità di multimode:

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

## Aggiungere una porta a un gruppo di interfacce o LAG

È possibile aggiungere fino a 16 porte fisiche a un gruppo di interfacce o LAG per tutte le velocità delle porte.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

### Utilizzare System Manager per aggiungere una porta a un LAG

#### Fasi

1. Selezionare **Network > Ethernet port > LAG** (rete > porta Ethernet > LAG\*) per modificare un LAG.
2. Selezionare porte aggiuntive sullo stesso nodo da aggiungere al LAG.
3. Salvare le modifiche.

#### CLI

### Utilizzare la CLI per aggiungere porte a un gruppo di interfacce

#### Fase

Aggiungere le porte di rete al gruppo di interfacce:

```
network port ifgrp add-port
```

Per ulteriori informazioni su questo comando, vedere ["Comandi di ONTAP 9"](#).

Nell'esempio seguente viene illustrato come aggiungere la porta e0c a un gruppo di interfacce denominato a0a:

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

A partire da ONTAP 9.8, i gruppi di interfacce vengono inseriti automaticamente in un dominio di trasmissione appropriato circa un minuto dopo l'aggiunta della prima porta fisica al gruppo di interfacce. Se non si desidera che ONTAP esegua questa operazione e si preferisce inserire manualmente ifgrp in un dominio di trasmissione, specificare `-skip-broadcast-domain-placement` come parte di `ifgrp add-port` comando.

### Rimuovere una porta da un gruppo di interfacce o LAG

È possibile rimuovere una porta da un gruppo di interfacce che ospita le LIF, purché non sia l'ultima porta del gruppo di interfacce. Non è necessario che il gruppo di interfacce non debba ospitare LIF o che il gruppo di interfacce non debba essere la porta home di una LIF, considerando che non si sta rimuovendo l'ultima porta dal gruppo di interfacce. Tuttavia, se si rimuove l'ultima porta, è necessario migrare o spostare i file LIF dal gruppo di interfacce.

#### A proposito di questa attività

È possibile rimuovere fino a 16 porte (interfacce fisiche) da un gruppo di interfacce o LAG.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

### Utilizzare System Manager per rimuovere una porta da un LAG

#### Fasi

1. Selezionare **Network > Ethernet port > LAG** (rete > porta Ethernet > LAG\*) per modificare un LAG.
2. Selezionare le porte da rimuovere dal LAG.
3. Salvare le modifiche.

#### CLI

### Utilizzare la CLI per rimuovere le porte da un gruppo di interfacce

#### Fase

Rimuovere le porte di rete da un gruppo di interfacce:

```
network port ifgrp remove-port
```

Nell'esempio seguente viene illustrato come rimuovere la porta e0c da un gruppo di interfacce denominato a0a:

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

### Eliminare un gruppo di interfacce o un LAG

È possibile eliminare i gruppi di interfacce o i LAG se si desidera configurare le LIF direttamente sulle porte fisiche sottostanti o si decide di modificare il gruppo di interfacce o la modalità LAG o la funzione di distribuzione.

#### Prima di iniziare

- Il gruppo di interfacce o il LAG non deve ospitare una LIF.
- Il gruppo di interfacce o LAG non deve essere né la porta home né la destinazione di failover di una LIF.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

### Utilizzare System Manager per eliminare un LAG

#### Fasi

1. Selezionare **Network > Ethernet port > LAG** (rete > porta Ethernet > LAG\*) per eliminare un LAG.
2. Selezionare il LAG che si desidera rimuovere.
3. Eliminare il LAG.

#### CLI

### Utilizzare la CLI per eliminare un gruppo di interfacce

#### Fase

Utilizzare `network port ifgrp delete` comando per eliminare un gruppo di interfacce.

Per ulteriori informazioni su questo comando, vedere ["Comandi di ONTAP 9"](#).

Nell'esempio seguente viene illustrato come eliminare un gruppo di interfacce denominato a0b:

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

## Configurare VLAN su porte fisiche

È possibile utilizzare le VLAN in ONTAP per fornire la segmentazione logica delle reti creando domini di broadcast separati definiti in base alla porta dello switch rispetto ai domini di broadcast tradizionali, definiti in base ai confini fisici.

Una VLAN può estendersi su più segmenti di rete fisici. Le stazioni finali appartenenti a una VLAN sono correlate in base alla funzione o all'applicazione.

Ad esempio, le stazioni finali in una VLAN possono essere raggruppate in base a reparti, ad esempio tecnici e contabili, o in base a progetti, ad esempio release1 e release2. Poiché la prossimità fisica delle stazioni finali non è essenziale in una VLAN, è possibile disperdere le stazioni finali geograficamente e contenere ancora il dominio di trasmissione in una rete commutata.

In ONTAP 9.13.1 e 9.14.1, le porte senza tag non utilizzate da interfacce logiche (LIF) e prive di connettività VLAN nativa sullo switch connesso vengono contrassegnate come degradate. Ciò consente di identificare le porte non utilizzate e non indica un'interruzione. Le VLAN native consentono il traffico non tagged sulla porta base ifgrp, come le trasmissioni ONTAP CFM. Configurare VLAN native sullo switch per impedire il blocco del traffico non tagged.

È possibile gestire le VLAN creando, eliminando o visualizzando le relative informazioni.



Non creare una VLAN su un'interfaccia di rete con lo stesso identificativo della VLAN nativa dello switch. Ad esempio, se l'interfaccia di rete e0b si trova sulla VLAN nativa 10, non creare una VLAN e0b-10 su tale interfaccia.

## Creare una VLAN

È possibile creare una VLAN per mantenere domini di trasmissione separati all'interno dello stesso dominio di rete utilizzando System Manager o l'`network port vlan create` comando.

## Prima di iniziare

Verificare che siano soddisfatti i seguenti requisiti:

- Gli switch implementati nella rete devono essere conformi agli standard IEEE 802.1Q o disporre di un'implementazione delle VLAN specifica del vendor.
- Per supportare più VLAN, una stazione finale deve essere configurata staticamente per appartenere a una o più VLAN.
- La VLAN non è collegata a una porta che ospita una LIF del cluster.
- La VLAN non è collegata alle porte assegnate a Cluster IPspace.
- La VLAN non viene creata su una porta del gruppo di interfacce che non contiene porte membro.

## A proposito di questa attività

La creazione di una VLAN collega la VLAN alla porta di rete di un nodo specificato in un cluster.

Quando si configura una VLAN su una porta per la prima volta, la porta potrebbe spegnersi, causando una disconnessione temporanea della rete. Le successive aggiunte di VLAN alla stessa porta non influiscono sullo stato della porta.



Non creare una VLAN su un'interfaccia di rete con lo stesso identificativo della VLAN nativa dello switch. Ad esempio, se l'interfaccia di rete e0b si trova sulla VLAN nativa 10, non creare una VLAN e0b-10 su tale interfaccia.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

### Utilizzare System Manager per creare una VLAN

A partire da ONTAP 9.12.0, è possibile selezionare automaticamente il dominio di trasmissione o manualmente dall'elenco. In precedenza, i domini di broadcast venivano sempre selezionati automaticamente in base alla connettività di livello 2. Se si seleziona manualmente un dominio di trasmissione, viene visualizzato un avviso che indica che la selezione manuale di un dominio di trasmissione potrebbe causare la perdita di connettività.

#### Fasi

1. Selezionare **Network > Ethernet port > + VLAN**.
2. Selezionare il nodo dall'elenco a discesa.
3. Scegliere tra le seguenti opzioni:
  - a. ONTAP (Seleziona dominio broadcast) per **selezionare automaticamente il dominio di broadcast (scelta consigliata)**.
  - b. Per selezionare manualmente un dominio di trasmissione dall'elenco.
4. Selezionare le porte per la VLAN.
5. Specificare l'ID VLAN.
6. Salvare le modifiche.

#### CLI

### Utilizzare la CLI per creare una VLAN

In alcuni casi, se si desidera creare la porta VLAN su una porta degradata senza correggere il problema hardware o la configurazione errata del software, è possibile impostare `-ignore-health-status` del parametro `network port modify` comando `as true`.

#### Fasi

1. Utilizzare `network port vlan create` Per creare una VLAN.
2. Specificare il `vlan-name` o il `port e. vlan-id` Opzioni per la creazione di una VLAN. Il nome della VLAN è una combinazione del nome della porta (o del gruppo di interfacce) e dell'identificatore della VLAN dello switch di rete, con un trattino nel mezzo. Ad esempio, `e0c-24` e `e1c-80` Sono nomi VLAN validi.

Nell'esempio seguente viene illustrato come creare una VLAN `e1c-80` collegato alla porta di rete `e1c` sul nodo `cluster-1-01`:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

A partire da ONTAP 9.8, le VLAN vengono automaticamente collocate nei domini di trasmissione appropriati circa un minuto dopo la loro creazione. Se non si desidera che ONTAP esegua questa operazione e si preferisce inserire manualmente la VLAN in un dominio di trasmissione, specificare `-skip-broadcast-domain-placement` come parte di `vlan create` comando.

Per ulteriori informazioni su questo comando, vedere ["Comandi di ONTAP 9"](#).

## Modificare una VLAN

È possibile modificare il dominio di trasmissione o disattivare una VLAN.

### Utilizzare System Manager per modificare una VLAN

A partire da ONTAP 9.12.0, è possibile selezionare automaticamente il dominio di trasmissione o manualmente dall'elenco. In precedenza, i domini broadcast venivano sempre selezionati automaticamente in base alla connettività di livello 2. Se si seleziona manualmente un dominio di trasmissione, viene visualizzato un avviso che indica che la selezione manuale di un dominio di trasmissione potrebbe causare la perdita di connettività.

#### Fasi

1. Selezionare **Network > Ethernet port > VLAN**.
2. Selezionare l'icona di modifica.
3. Effettuare una delle seguenti operazioni:
  - Modificare il dominio di trasmissione selezionandone uno diverso dall'elenco.
  - Deselezionare la casella di controllo **Enabled**.
4. Salvare le modifiche.

### Eliminare una VLAN

Potrebbe essere necessario eliminare una VLAN prima di rimuovere una NIC dal relativo slot. Quando si elimina una VLAN, questa viene automaticamente rimossa da tutte le regole e i gruppi di failover che la utilizzano.

#### Prima di iniziare

Assicurarsi che non vi siano LIF associati alla VLAN.

#### A proposito di questa attività

L'eliminazione dell'ultima VLAN da una porta potrebbe causare la disconnessione temporanea della rete dalla porta.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:



## System Manager

### Utilizzare System Manager per eliminare una VLAN

#### Fasi

1. Selezionare **Network > Ethernet port > VLAN**.
2. Selezionare la VLAN che si desidera rimuovere.
3. Fare clic su **Delete** (Elimina).

#### CLI

### Utilizzare la CLI per eliminare una VLAN

#### Fase

Utilizzare `network port vlan delete` Comando per eliminare una VLAN.

Nell'esempio seguente viene illustrato come eliminare la VLAN `e1c-80` dalla porta di rete `e1c` sul nodo `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

## Modificare gli attributi delle porte di rete

È possibile modificare le impostazioni di negoziazione automatica, duplex, controllo di flusso, velocità e stato di una porta di rete fisica.

### Prima di iniziare

La porta che si desidera modificare non deve ospitare le LIF.

### A proposito di questa attività

- Si sconsiglia di modificare le impostazioni amministrative delle interfacce di rete 100 GbE, 40 GbE, 10 GbE o 1 GbE.

I valori impostati per la modalità duplex e la velocità della porta vengono definiti impostazioni amministrative. A seconda delle limitazioni di rete, le impostazioni amministrative possono differire dalle impostazioni operative (ovvero, la modalità duplex e la velocità effettivamente utilizzate dalla porta).

- Si sconsiglia di modificare le impostazioni amministrative delle porte fisiche sottostanti in un gruppo di interfacce.

Il `-up-admin` parameter (disponibile a livello di privilegio avanzato) modifica le impostazioni amministrative della porta.

- Si sconsiglia di impostare `-up-admin` Impostazione amministrativa su `false` per tutte le porte su un nodo o per la porta che ospita l'ultimo LIF del cluster operativo su un nodo.
- Si sconsiglia di modificare le dimensioni MTU della porta di gestione, `e0M`.
- La dimensione MTU di una porta in un dominio di trasmissione non può essere modificata dal valore MTU impostato per il dominio di trasmissione.

- Le dimensioni MTU di una VLAN non possono superare il valore delle dimensioni MTU della porta di base.

## Fasi

1. Modificare gli attributi di una porta di rete:

```
network port modify
```

2. È possibile impostare `-ignore-health-status` campo su `vero` per specificare che il sistema può ignorare lo stato di integrità della porta di rete di una porta specificata.

Lo stato di integrità della porta di rete viene modificato automaticamente da degradato a integro e questa porta può essere utilizzata per ospitare i file LIF. Impostare il controllo di flusso delle porte del cluster su `none`. Per impostazione predefinita, il controllo di flusso è impostato su `full`.

Il seguente comando disattiva il controllo di flusso sulla porta `e0b` impostando il controllo di flusso su `NONE`:

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

## Converti le porte NIC da 40 GbE in più porte da 10 GbE per la connettività da 10 GbE

È possibile convertire le schede di interfaccia di rete (NIC) X1144A-R6 e X91440A-R6 40GbE per supportare quattro porte 10 GbE.

Se si connette una piattaforma hardware che supporta una di queste schede di rete a un cluster che supporta l'interconnessione del cluster a 10 GbE e le connessioni dati del cliente, la scheda di rete deve essere convertita per fornire le connessioni a 10 GbE necessarie.

### Prima di iniziare

È necessario utilizzare un cavo breakout supportato.

### A proposito di questa attività

Per un elenco completo delle piattaforme che supportano le schede di rete, vedere ["Hardware Universe"](#).



Sulla scheda NIC X1144A-R6, è possibile convertire solo la porta A per supportare le quattro connessioni 10GbE. Una volta convertita la porta A, la porta e non è disponibile per l'uso.

## Fasi

1. Accedere alla modalità di manutenzione.
2. Conversione della scheda di rete dal supporto da 40 GbE al supporto da 10 GbE.

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. Dopo aver utilizzato il comando `convert`, arrestare il nodo.
4. Installare o sostituire il cavo.
5. A seconda del modello hardware, utilizzare il SP (Service Processor) o BMC (Baseboard Management Controller) per spegnere e riaccendere il nodo in modo che la conversione sia effettiva.

## Rimozione di una scheda di rete dal nodo (ONTAP 9,8 e versioni successive)

Questo argomento è valido per ONTAP 9,8 e versioni successive. Potrebbe essere necessario rimuovere una scheda NIC difettosa dal relativo slot o spostarla in un altro slot per scopi di manutenzione.

### Fasi

1. Spegnerne il nodo.
2. Rimuovere fisicamente la scheda NIC dal relativo slot.
3. Accendere il nodo.
4. Verificare che la porta sia stata eliminata:

```
network port show
```



ONTAP rimuove automaticamente la porta da qualsiasi gruppo di interfacce. Se la porta era l'unico membro di un gruppo di interfacce, il gruppo di interfacce viene cancellato.

5. Se sulla porta sono configurate delle VLAN, queste vengono spostate. È possibile visualizzare le VLAN smontate utilizzando il seguente comando:

```
cluster controller-replacement network displaced-vlans show
```



Il `displaced-interface show`, `displaced-vlans show`, e `displaced-vlans restore` i comandi sono univoci e non richiedono il nome completo del comando, che inizia con `cluster controller-replacement network`.

6. Queste VLAN vengono eliminate, ma possono essere ripristinate utilizzando il seguente comando:

```
displaced-vlans restore
```

7. Se sulla porta sono configurate delle LIF, ONTAP sceglie automaticamente nuove porte home per quelle LIF su un'altra porta nello stesso dominio di trasmissione. Se sullo stesso filer non viene trovata alcuna porta home adatta, tali LIF vengono considerati spostati. È possibile visualizzare i file LIF spostati utilizzando il seguente comando:

```
displaced-interface show
```

8. Quando viene aggiunta una nuova porta al dominio di trasmissione sullo stesso nodo, le porte home per i file LIF vengono ripristinate automaticamente. In alternativa, è possibile impostare la porta home utilizzando `network interface modify -home-port -home-node` o usare il `displaced-interface restore` comando.

## Rimozione di una scheda di rete dal nodo (ONTAP 9,7 o versione precedente)

Questo argomento riguarda ONTAP 9.7 o versioni precedenti. Potrebbe essere

necessario rimuovere una scheda NIC difettosa dal relativo slot o spostarla in un altro slot per scopi di manutenzione.

### Prima di iniziare

- Tutte le LIF ospitate sulle porte NIC devono essere state migrate o eliminate.
- Nessuna delle porte NIC può essere la porta principale di qualsiasi LIF.
- Per eliminare le porte da una scheda NIC, è necessario disporre di privilegi avanzati.

### Fasi

1. Eliminare le porte dalla scheda NIC:

```
network port delete
```

2. Verificare che le porte siano state eliminate:

```
network port show
```

3. Ripetere il passaggio 1 se l'output del comando di visualizzazione della porta di rete mostra ancora la porta eliminata.

### Monitorare le porte di rete

#### Monitorare lo stato delle porte di rete

La gestione ONTAP delle porte di rete include il monitoraggio automatico dello stato di salute e un set di monitor per aiutare a identificare le porte di rete che potrebbero non essere adatte per l'hosting di LIF.

#### A proposito di questa attività

Se un monitor dello stato di salute determina che una porta di rete non è funzionante, avvisa gli amministratori tramite un messaggio EMS o contrassegna la porta come danneggiata. ONTAP evita l'hosting di LIF su porte di rete degradate se sono presenti destinazioni di failover alternative sane per tale LIF. Una porta può diventare degradata a causa di un errore di tipo soft, come ad esempio il link flapping (link che rimbalzano rapidamente tra up e down) o la partizione di rete:

- Le porte di rete nell'IPSpace del cluster vengono contrassegnate come degradate quando si verificano lo sfarfallio del collegamento o la perdita di raggiungibilità Layer 2 (L2) ad altre porte di rete nel dominio di trasmissione.
- Le porte di rete negli spazi IP non cluster vengono contrassegnate come degradate quando si verifica lo sfarfallio dei collegamenti.

È necessario conoscere i seguenti comportamenti di una porta danneggiata:

- Una porta degradata non può essere inclusa in una VLAN o in un gruppo di interfacce.

Se una porta membro di un gruppo di interfacce è contrassegnata come degradata, ma il gruppo di interfacce è ancora contrassegnato come integro, i file LIF possono essere ospitati su quel gruppo di interfacce.

- Le LIF vengono migrate automaticamente dalle porte degradate alle porte integre.
- Durante un evento di failover, una porta degradata non viene considerata come destinazione di failover. Se

non sono disponibili porte integre, le porte degradate ospitano le LIF in base alla normale policy di failover.

- Non è possibile creare, migrare o ripristinare una LIF su una porta degradata.

È possibile modificare `ignore-health-status` impostazione della porta di rete su `true`. È quindi possibile ospitare una LIF sulle porte sane.

## Fasi

1. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

2. Controllare quali monitor di stato sono abilitati per il monitoraggio dello stato delle porte di rete:

```
network options port-health-monitor show
```

Lo stato di salute di una porta è determinato dal valore dei monitor di stato.

I seguenti monitor di stato sono disponibili e abilitati per impostazione predefinita in ONTAP:

- Monitor di stato link-flapping: Monitora il link flapping

Se una porta presenta uno sfarfallio del collegamento più di una volta in cinque minuti, questa porta viene contrassegnata come degradata.

- L2 Reachability Health Monitor: Monitora se tutte le porte configurate nello stesso dominio di trasmissione hanno una raggiungibilità L2 l'una rispetto all'altra

Questo monitor dello stato di salute segnala problemi di raggiungibilità L2 in tutti gli spazi IP; tuttavia, contrassegna solo le porte nell'IPSpace del cluster come degradate.

- Monitor CRC: Monitora le statistiche CRC sulle porte

Questo monitor dello stato di salute non contrassegna una porta come degradata, ma genera un messaggio EMS quando si osserva un tasso di guasti CRC molto elevato.

3. Attivare o disattivare i monitor di stato di un IPspace come desiderato utilizzando `network options port-health-monitor modify` comando.

4. Visualizzazione dello stato dettagliato di una porta:

```
network port show -health
```

L'output del comando visualizza lo stato di salute della porta, `ignore health status` impostazione ed elenco dei motivi per cui la porta è contrassegnata come degradata.

Lo stato di integrità della porta può essere `healthy` oppure `degraded`.

Se il `ignore health status` l'impostazione è `true`, indica che lo stato di salute della porta è stato

modificato da `degraded` a `healthy` dall'amministratore.

Se il `ignore health status` l'impostazione è `false`, lo stato delle porte viene determinato automaticamente dal sistema.

#### **Monitorare la raggiungibilità delle porte di rete (ONTAP 9.8 e versioni successive)**

Il monitoraggio della raggiungibilità è integrato in ONTAP 9.8 e versioni successive. Utilizzare questo monitoraggio per identificare quando la topologia fisica della rete non corrisponde alla configurazione ONTAP. In alcuni casi, ONTAP può riparare la raggiungibilità delle porte. In altri casi, sono necessari ulteriori passaggi.

#### **A proposito di questa attività**

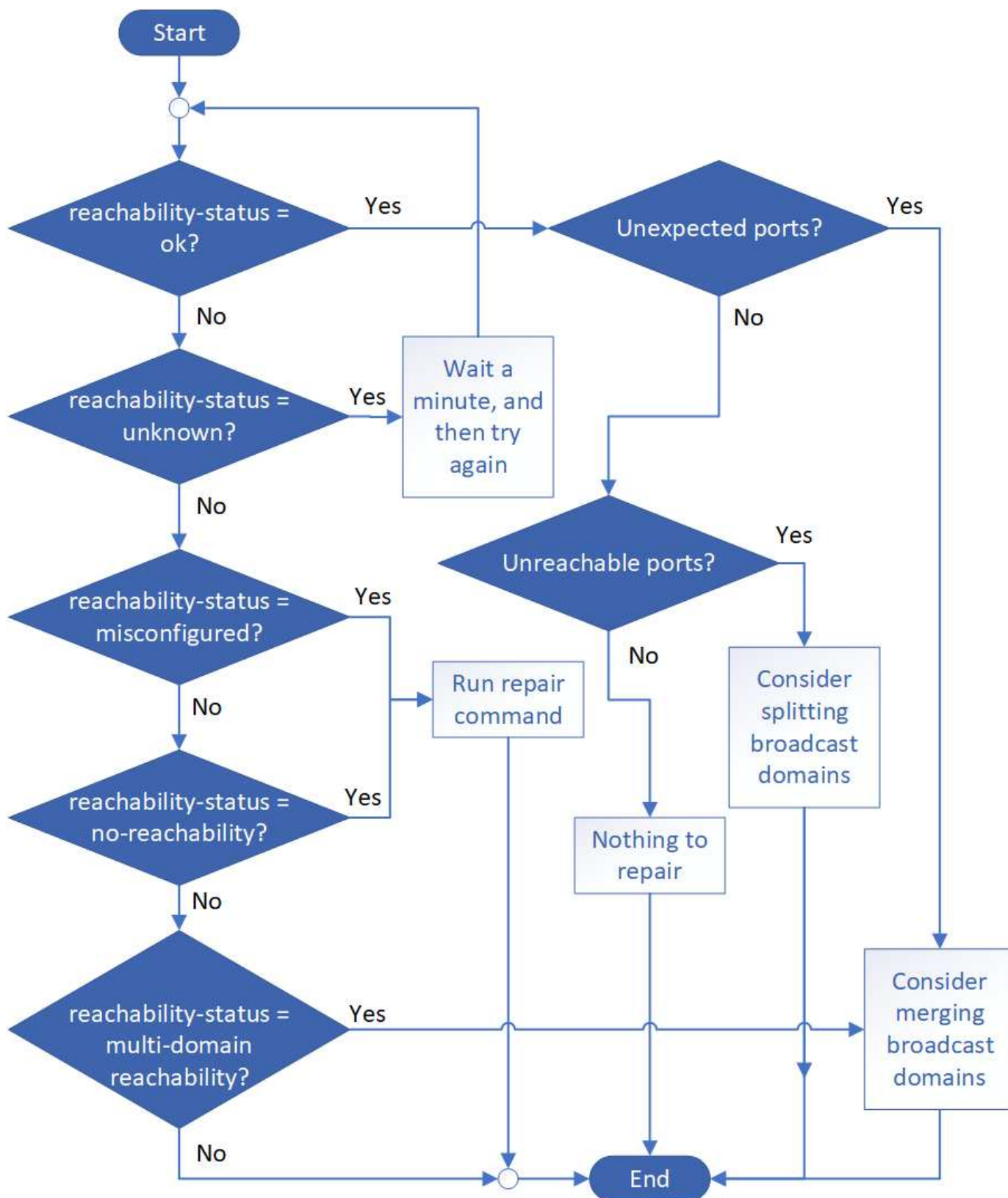
Utilizzare questi comandi per verificare, diagnosticare e riparare le configurazioni errate della rete derivanti dalla configurazione ONTAP che non corrisponde al cablaggio fisico o alla configurazione dello switch di rete.

#### **Fase**

1. Visualizzazione della raggiungibilità delle porte:

```
network port reachability show
```

2. Utilizzare la seguente struttura decisionale e la seguente tabella per determinare la fase successiva, se presente.



Stato di raggiungibilità	Descrizione
--------------------------	-------------

ok	<p>La porta ha una capacità di livello 2 rispetto al dominio di trasmissione assegnato. Se lo stato di raggiungibilità è "ok", ma ci sono "porte impreviste", considerare la possibilità di unire uno o più domini di broadcast. Per ulteriori informazioni, consulta la seguente riga <i>Unexpected ports</i>.</p> <p>Se lo stato di raggiungibilità è "ok", ma ci sono "porte irraggiungibili", considerare la possibilità di suddividere uno o più domini di broadcast. Per ulteriori informazioni, consultare la riga <i>Unreachable ports</i> riportata di seguito.</p> <p>Se lo stato di raggiungibilità è "ok" e non ci sono porte impreviste o irraggiungibili, la configurazione è corretta.</p>
Porte impreviste	<p>La porta ha una raggiungibilità di livello 2 per il dominio di broadcast assegnato; tuttavia, ha anche una raggiungibilità di livello 2 per almeno un altro dominio di broadcast.</p> <p>Esaminare la connettività fisica e la configurazione dello switch per determinare se non è corretta o se il dominio di trasmissione assegnato alla porta deve essere Unito a uno o più domini di trasmissione.</p> <p>Per ulteriori informazioni, vedere <a href="#">"Unire i domini di broadcast"</a>.</p>
Porte non raggiungibili	<p>Se un singolo dominio di broadcast è stato suddiviso in due diversi set di raggiungibilità, è possibile suddividere un dominio di broadcast per sincronizzare la configurazione ONTAP con la topologia fisica della rete.</p> <p>In genere, l'elenco delle porte irraggiungibili definisce il set di porte che devono essere suddivise in un altro dominio di trasmissione dopo aver verificato che la configurazione fisica e quella dello switch sono accurate.</p> <p>Per ulteriori informazioni, vedere <a href="#">"Suddividere i domini di broadcast"</a>.</p>
riconfigurazione non corretta	<p>La porta non dispone di capacità di livello 2 rispetto al dominio di trasmissione assegnato; tuttavia, la porta dispone di capacità di livello 2 rispetto a un dominio di trasmissione diverso.</p> <p>È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta al dominio di trasmissione a cui è possibile accedere:</p> <p>`network port reachability repair -node -port` Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
nessuna raggiungibilità	<p>La porta non dispone di capacità di livello 2 per nessun dominio di trasmissione esistente.</p> <p>È possibile riparare la raggiungibilità delle porte. Quando si esegue il seguente comando, il sistema assegna la porta a un nuovo dominio di trasmissione creato automaticamente in IPspace predefinito:</p> <p>`network port reachability repair -node -port` Per ulteriori informazioni, vedere <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>



raggiungibilità multi-dominio	<p>La porta ha una raggiungibilità di livello 2 per il dominio di broadcast assegnato; tuttavia, ha anche una raggiungibilità di livello 2 per almeno un altro dominio di broadcast.</p> <p>Esaminare la connettività fisica e la configurazione dello switch per determinare se non è corretta o se il dominio di trasmissione assegnato alla porta deve essere Unito a uno o più domini di trasmissione.</p> <p>Per ulteriori informazioni, vedere <a href="#">"Unire i domini di broadcast"</a> oppure <a href="#">"Riparare la raggiungibilità delle porte"</a>.</p>
sconosciuto	Se lo stato di raggiungibilità è "sconosciuto", attendere alcuni minuti e provare a eseguire nuovamente il comando.

Dopo aver riparato una porta, è necessario controllare e risolvere le LIF e le VLAN spostate. Se la porta faceva parte di un gruppo di interfacce, è necessario comprendere anche cosa è successo a quel gruppo di interfacce. Per ulteriori informazioni, vedere ["Riparare la raggiungibilità delle porte"](#).

### Panoramica delle porte ONTAP

Alcune porte note sono riservate per le comunicazioni ONTAP con servizi specifici. I conflitti di porta si verificano se il valore di una porta nell'ambiente di rete dello storage è lo stesso della porta ONTAP.

La seguente tabella elenca le porte TCP e UDP utilizzate da ONTAP.

Servizio	Porta/protocollo	Descrizione
ssh	22/TCP	Login shell sicuro
telnet	23/TCP	Accesso remoto
DNS	53/TCP	DNS con bilanciamento del carico
http	80/TCP	Hyper Text Transfer Protocol
rpcbind	111/TCP	Chiamata di procedura remota
rpcbind	111/UDP	Chiamata di procedura remota
ntp	123/UDP	Network Time Protocol
msrpc	135/UDP	MSRPC
netbios-sn	139/TCP	Sessione del servizio NetBIOS
snmp	161/UDP	Protocollo di gestione di rete semplice
https	443/TCP	HTTP su TLS
microsoft-ds	445/TCP	Microsoft-ds
montare	635/TCP	Montaggio NFS
montare	635/UDP	Montaggio NFS
con nome	953/UDP	Nome daemon

nfs	2049/UDP	Daemon del server NFS
nfs	2049/TCP	Daemon del server NFS
nrv	2050/TCP	Protocollo NetApp Remote Volume
iscsi	3260/TCP	Porta di destinazione iSCSI
blocco	4045/TCP	Daemon di blocco NFS
blocco	4045/UDP	Daemon di blocco NFS
NSM	4046/TCP	Network Status Monitor (Monitor di stato della rete)
NSM	4046/UDP	Network Status Monitor (Monitor di stato della rete)
rquotad	4049/UDP	Protocollo NFS rquotad
krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Porta HTTPS - protocollo binario di ascolto
https	8443/TCP	7MTT GUI Tool tramite https
ndmp	10000/TCP	Network Data Management Protocol
Peering dei cluster	11104/TCP	Peering dei cluster, bidirezionale
Peering dei cluster, bidirezionale	11105/TCP	Peering dei cluster
NDMP	18600 - 18699/TCP	NDMP
NDMP	30000/TCP	accetta connessioni di controllo su prese sicure
porta del testimone cifs	40001/TCP	porta del testimone cifs
tls	50000/TCP	Sicurezza del livello di trasporto
iscsi	65200/TCP	Porta iSCSI

#### Porte interne ONTAP

La tabella seguente elenca le porte TCP e UDP utilizzate internamente da ONTAP. Queste porte vengono utilizzate per stabilire una comunicazione LIF intracluster:

Porta/protocollo	Descrizione
514	Syslog
900	RPC cluster di NetApp
902	RPC cluster di NetApp
904	RPC cluster di NetApp
905	RPC cluster di NetApp
910	RPC cluster di NetApp
911	RPC cluster di NetApp

913	RPC cluster di NetApp
914	RPC cluster di NetApp
915	RPC cluster di NetApp
918	RPC cluster di NetApp
920	RPC cluster di NetApp
921	RPC cluster di NetApp
924	RPC cluster di NetApp
925	RPC cluster di NetApp
927	RPC cluster di NetApp
928	RPC cluster di NetApp
929	RPC cluster di NetApp
931	RPC cluster di NetApp
932	RPC cluster di NetApp
933	RPC cluster di NetApp
934	RPC cluster di NetApp
935	RPC cluster di NetApp
936	RPC cluster di NetApp
937	RPC cluster di NetApp
939	RPC cluster di NetApp
940	RPC cluster di NetApp
951	RPC cluster di NetApp
954	RPC cluster di NetApp
955	RPC cluster di NetApp
956	RPC cluster di NetApp
958	RPC cluster di NetApp
961	RPC cluster di NetApp
963	RPC cluster di NetApp
964	RPC cluster di NetApp
966	RPC cluster di NetApp
967	RPC cluster di NetApp
982	RPC cluster di NetApp
983	RPC cluster di NetApp
5125	Porta di controllo alternativa per il disco
5133	Porta di controllo alternativa per il disco

5144	Porta di controllo alternativa per il disco
65502	SSH. Ambito nodo
65503	Condivisione LIF
7810	RPC cluster di NetApp
7811	RPC cluster di NetApp
7812	RPC cluster di NetApp
7813	RPC cluster di NetApp
7814	RPC cluster di NetApp
7815	RPC cluster di NetApp
7816	RPC cluster di NetApp
7817	RPC cluster di NetApp
7818	RPC cluster di NetApp
7819	RPC cluster di NetApp
7820	RPC cluster di NetApp
7821	RPC cluster di NetApp
7822	RPC cluster di NetApp
7823	RPC cluster di NetApp
7824	RPC cluster di NetApp
8023	Ambito del nodo TELNET
8514	Scope del nodo RSH
9877	Porta client KMIP (solo host locale interno)

## IPspaces

### Configurare la panoramica degli IPspace

Gli IPspaces consentono di configurare un singolo cluster ONTAP in modo che i client possano accedervi da più di un dominio di rete separato a livello amministrativo, anche se questi client utilizzano lo stesso intervallo di subnet di indirizzi IP. Ciò consente la separazione del traffico client per la privacy e la sicurezza.

Un IPspace definisce uno spazio di indirizzi IP distinto in cui risiedono le macchine virtuali di storage (SVM). Le porte e gli indirizzi IP definiti per un IPspace sono applicabili solo all'interno di tale IPspace. Viene mantenuta una tabella di routing distinta per ogni SVM all'interno di un IPspace; pertanto, non si verifica alcun routing del traffico cross-SVM o cross-IPspace.



Gli IPspaces supportano indirizzi IPv4 e IPv6 nei rispettivi domini di routing.

Se si gestisce lo storage per una singola organizzazione, non è necessario configurare gli IPspaces. Se si gestisce lo storage per più aziende su un singolo cluster ONTAP e si è certi che nessuno dei clienti dispone di

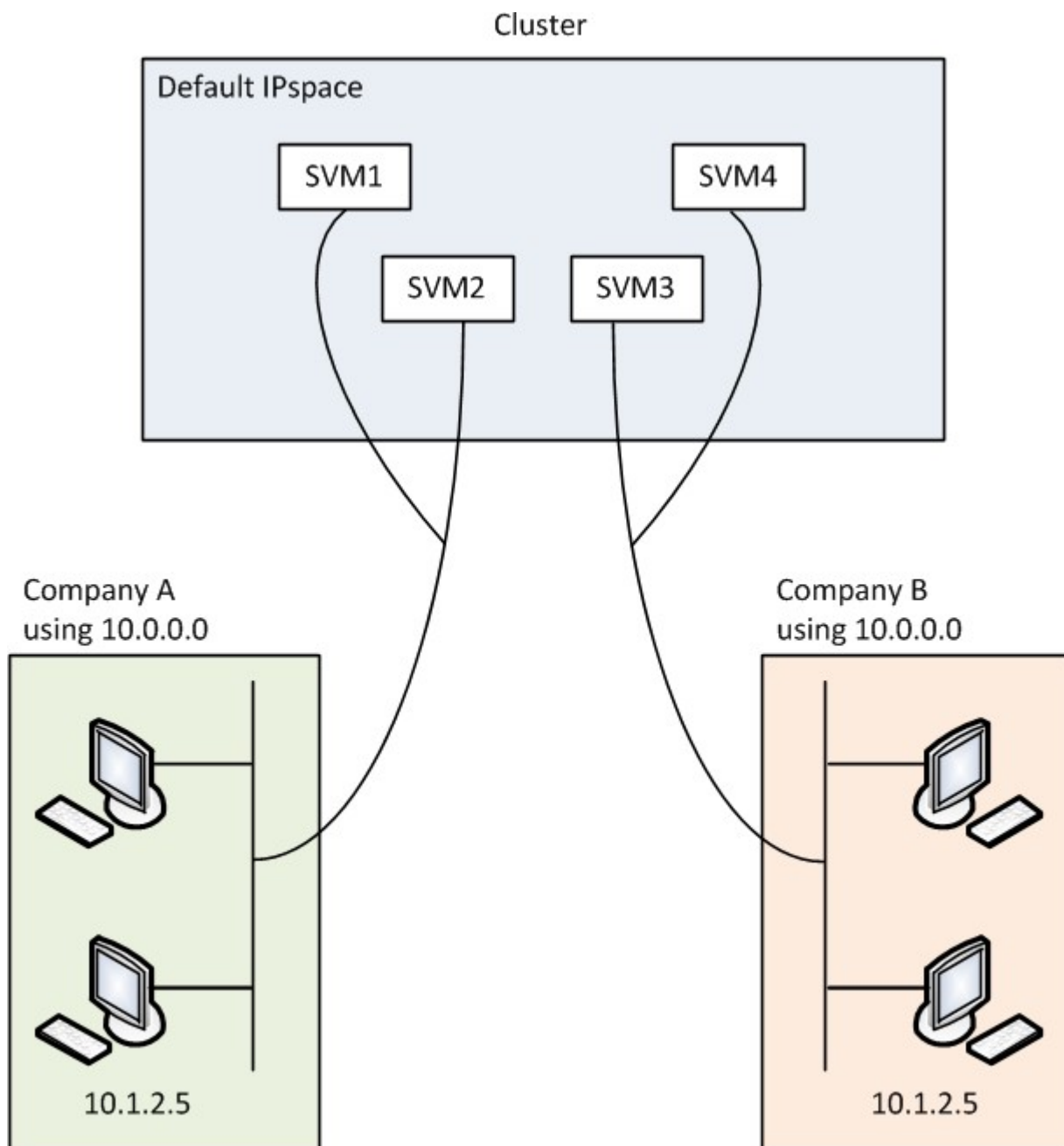
configurazioni di rete in conflitto, non è necessario utilizzare gli IPspaces. In molti casi, l'utilizzo di macchine virtuali di storage (SVM), con le proprie tabelle di routing IP distinte, può essere utilizzato per separare configurazioni di rete uniche invece di utilizzare gli spazi IPspace.

### Esempio di utilizzo di IPspaces

Un'applicazione comune per l'utilizzo di IPspaces è quando un provider di servizi di storage (SSP) deve connettere i clienti delle aziende A e B a un cluster ONTAP in loco e entrambe le aziende utilizzano gli stessi intervalli di indirizzi IP privati.

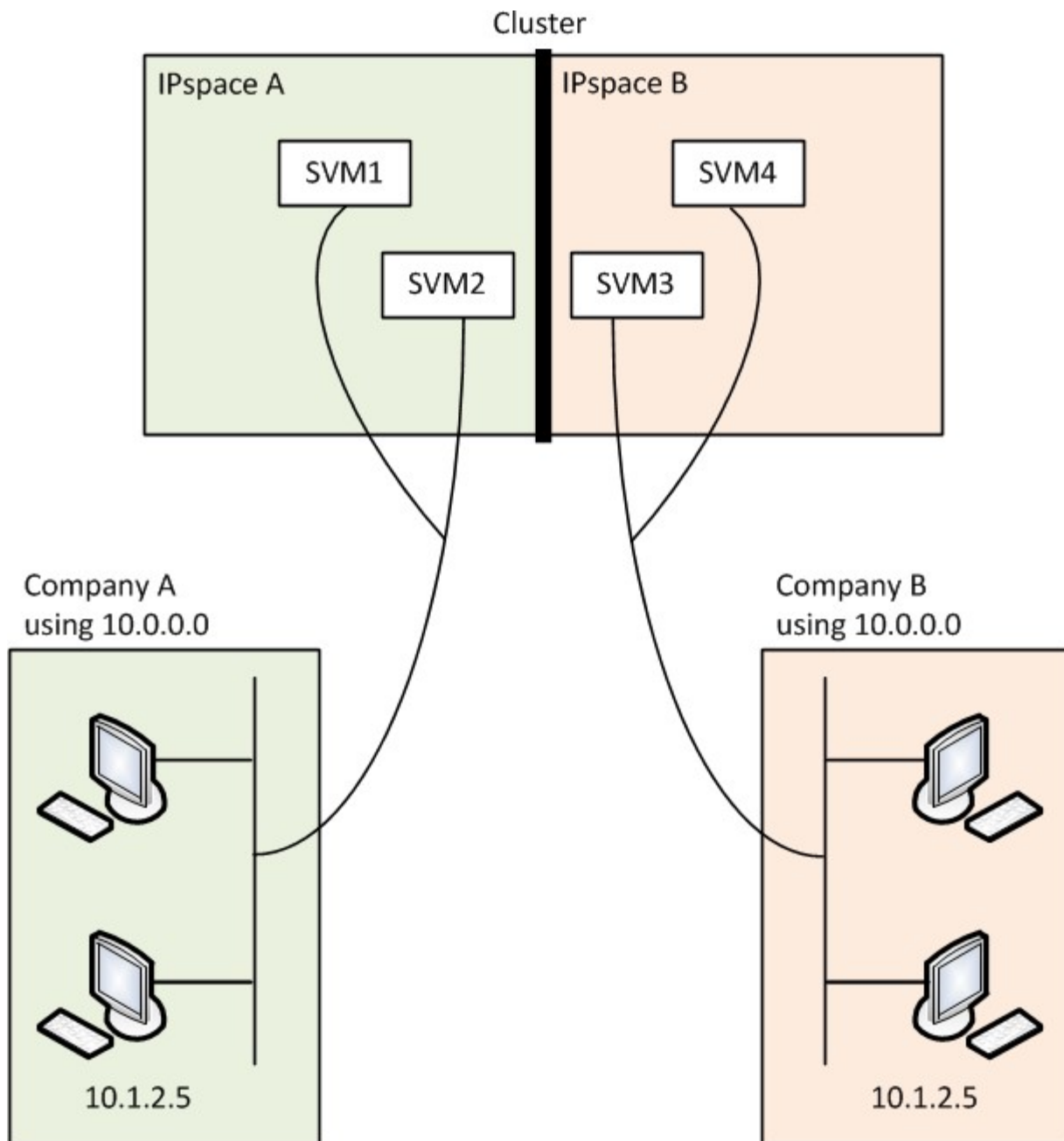
SSP crea SVM sul cluster per ciascun cliente e fornisce un percorso di rete dedicato da due SVM alla rete dell'azienda A e dalle altre due SVM alla rete dell'azienda B.

Questo tipo di implementazione viene illustrato nella figura seguente e funziona se entrambe le aziende utilizzano intervalli di indirizzi IP non privati. Tuttavia, l'illustrazione mostra entrambe le aziende che utilizzano gli stessi intervalli di indirizzi IP privati, causando problemi.



Entrambe le aziende utilizzano la subnet dell'indirizzo IP privato 10.0.0.0, causando i seguenti problemi:

- Le SVM nel cluster nella posizione SSP presentano indirizzi IP in conflitto se entrambe le aziende decidono di utilizzare lo stesso indirizzo IP per le rispettive SVM.
- Anche se le due aziende concordano sull'utilizzo di indirizzi IP diversi per le proprie SVM, possono insorgere problemi.
- Ad esempio, se un client nella rete Di A ha lo stesso indirizzo IP di un client nella rete di B, i pacchetti destinati a un client nello spazio degli indirizzi Di A potrebbero essere instradati a un client nello spazio degli indirizzi di B e viceversa.
- Se le due società decidono di utilizzare spazi di indirizzi che si escludono a vicenda (Ad esempio, A utilizza 10.0.0.0 con una maschera di rete di 255.128.0.0 e B utilizza 10.128.0.0 con una maschera di rete di 255.128.0.0), L'SSP deve configurare percorsi statici sul cluster per instradare il traffico in modo appropriato alle reti Di A e B.
- Questa soluzione non è scalabile (a causa di percorsi statici) né sicura (il traffico broadcast viene inviato a tutte le interfacce del cluster).per superare questi problemi, SSP definisce due spazi IPsul cluster, uno per ciascuna azienda. Poiché non viene instradato alcun traffico multiIPSpace, i dati di ciascuna azienda vengono instradati in modo sicuro alla rispettiva rete anche se tutte le SVM sono configurate nello spazio degli indirizzi 10.0.0.0, come mostrato nella seguente illustrazione:



Inoltre, gli indirizzi IP a cui si fa riferimento dai vari file di configurazione, ad esempio `/etc/hosts` file, il `/etc/hosts.equiv` file, e. the `/etc/rc` Sono relativi a tale IPspace. Pertanto, gli IPspaces consentono a SSP di configurare lo stesso indirizzo IP per i dati di configurazione e autenticazione per più SVM, senza conflitti.

### Proprietà standard di IPspaces

Gli IPspaces speciali vengono creati per impostazione predefinita al momento della creazione del cluster. Inoltre, vengono create speciali macchine virtuali di storage (SVM) per ogni IPspace.

Due IPspaces vengono creati automaticamente quando il cluster viene inizializzato:

- IPspace "predefinito"

IPspace è un container per porte, subnet e SVM che servono dati. Se la configurazione non richiede spazi IP separati per i client, è possibile creare tutti gli SVM in questo spazio IPspace. Questo IPspace contiene

anche le porte di gestione del cluster e dei nodi.

- IPSpace "cluster"

Questo IPSpace contiene tutte le porte del cluster di tutti i nodi del cluster. Viene creato automaticamente al momento della creazione del cluster. Fornisce connettività alla rete interna del cluster privato. Man mano che altri nodi si uniscono al cluster, le porte del cluster da tali nodi vengono aggiunte all'IPSpace "Cluster".

Esiste una SVM di "sistema" per ogni IPSpace. Quando si crea un IPSpace, viene creata una SVM di sistema predefinita con lo stesso nome:

- La SVM di sistema per l'IPSpace "Cluster" trasporta il traffico del cluster tra i nodi di un cluster sulla rete interna del cluster privato.

È gestito dall'amministratore del cluster e ha il nome "Cluster".

- La SVM di sistema per l'IPSpace "predefinito" trasporta il traffico di gestione per il cluster e i nodi, incluso il traffico tra cluster.

Viene gestito dall'amministratore del cluster e utilizza lo stesso nome del cluster.

- La SVM di sistema per un IPSpace personalizzato creato trasporta il traffico di gestione per tale SVM.

Viene gestito dall'amministratore del cluster e utilizza lo stesso nome di IPSpace.

Una o più SVM per client possono esistere in un IPSpace. Ogni SVM client dispone di volumi e configurazioni dati propri e viene amministrato indipendentemente dalle altre SVM.

## Creare IPspaces

Gli IPspaces sono spazi di indirizzi IP distinti in cui risiedono le macchine virtuali di storage (SVM). È possibile creare spazi IP quando è necessario che le SVM dispongano di storage, amministrazione e routing sicuri. È possibile utilizzare un IPSpace per creare uno spazio di indirizzi IP distinto per ogni SVM in un cluster. In questo modo, i client in domini di rete separati a livello amministrativo possono accedere ai dati del cluster utilizzando indirizzi IP sovrapposti dallo stesso intervallo di subnet di indirizzi IP.

### A proposito di questa attività

Esiste un limite di 512 IPspaces a livello di cluster. Il limite a livello di cluster è ridotto a 256 IPSpace per i cluster che contengono nodi con 6 GB di RAM. Consulta il Hardware Universe per determinare se sono applicati limiti aggiuntivi alla tua piattaforma.

["NetApp Hardware Universe"](#)



Un nome IPSpace non può essere "tutto" perché "tutto" è un nome riservato al sistema.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

### Fase

1. Creare un IPSpace:



```
network ipspace create -ipspace ipspace_name
```

ipspace\_name È il nome dell'IPSpace che si desidera creare. Il seguente comando crea IPSpace ipspace1 su un cluster:

```
network ipspace create -ipspace ipspace1
```

## 2. Visualizzare gli IPSpace:

```
network ipspace show
```

IPspace	Vserver List	Broadcast Domains
Cluster	Cluster	Cluster
Default	Cluster1	Default
ipspace1	ipspace1	-

Viene creato IPSpace, insieme alla SVM di sistema per IPSpace. Il sistema SVM trasporta il traffico di gestione.

### Al termine

Se si crea un IPSpace in un cluster con una configurazione MetroCluster, gli oggetti IPSpace devono essere replicati manualmente nei cluster partner. Qualsiasi SVM creata e assegnata a un IPSpace prima della replica di IPSpace non verrà replicata nei cluster partner.

I domini di broadcast vengono creati automaticamente in IPSpace "Default" e possono essere spostati tra gli IPSpaces utilizzando il seguente comando:

```
network port broadcast-domain move
```

Ad esempio, se si desidera spostare un dominio di trasmissione da "Default" a "ips1", utilizzare il seguente comando:

```
network port broadcast-domain move -ipspace Default -broadcast-domain  
Default -to-ipspace ips1
```

## Visualizzare gli IPSpaces

È possibile visualizzare l'elenco degli IPSpace presenti in un cluster ed è possibile visualizzare le macchine virtuali di storage (SVM), i domini di trasmissione e le porte assegnati a ciascun IPSpace.

### Fase

Visualizzare gli IPspaces e le SVM in un cluster:

```
network ipspace show [-ip space ipspace_name]
```

Il seguente comando visualizza tutti gli IPspaces, le SVM e i domini di broadcast nel cluster:

```
network ipspace show
IPspace          Vserver List          Broadcast Domains
-----          -
Cluster
Default          Cluster              Cluster
                  vs1, cluster-1        Default
ipspace1         vs3, vs4, ipspace1    bcast1
```

Il seguente comando visualizza i nodi e le porte che fanno parte di IPSpace ipspace1:

```
network ipspace show -ip space ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

## Eliminare un IPSpace

Se non è più necessario un IPSpace, è possibile eliminarlo.

### Prima di iniziare

Non devono essere presenti domini di broadcast, interfacce di rete o SVM associati all'IPSpace che si desidera eliminare.

Gli IPspace "Default" e "Cluster" definiti dal sistema non possono essere cancellati.

### Fase

Eliminazione di un IPSpace:

```
network ipspace delete -ip space ipspace_name
```

Il seguente comando elimina IPSpace ipspace1 dal cluster:

```
network ipspace delete -ip space ipspace1
```

# Domini di broadcast

## Dominio di broadcast (ONTAP 9,8 e versioni successive)

### Panoramica del dominio di trasmissione (ONTAP 9,8 e versioni successive)

I domini di broadcast sono destinati a raggruppare le porte di rete che appartengono alla stessa rete Layer 2. Le porte del gruppo possono quindi essere utilizzate da una macchina virtuale di storage (SVM) per il traffico di dati o di gestione.

Un dominio di broadcast risiede in un IPSpace. Durante l'inizializzazione del cluster, il sistema crea due domini di broadcast predefiniti:

- Il dominio di trasmissione "predefinito" contiene le porte che si trovano nello spazio IPSpace "predefinito".

Queste porte vengono utilizzate principalmente per la gestione dei dati. Anche le porte di gestione del cluster e dei nodi si trovano in questo dominio di broadcast.

- Il dominio di trasmissione "Cluster" contiene le porte che si trovano nell'IPSpace "Cluster".

Queste porte vengono utilizzate per la comunicazione del cluster e includono tutte le porte del cluster di tutti i nodi del cluster.

Se necessario, il sistema crea ulteriori domini di broadcast nell'IPSpace predefinito. Il dominio di trasmissione "predefinito" contiene la porta home della LIF di gestione, oltre a tutte le altre porte che hanno la capacità di raggiungere tale porta di livello 2. I domini di broadcast aggiuntivi sono denominati "Default-1", "Default-2" e così via.

### Esempio di utilizzo di domini di broadcast

Un dominio di broadcast è un insieme di porte di rete nello stesso IPSpace che ha anche la raggiungibilità di livello 2 l'una rispetto all'altra, incluse generalmente le porte di molti nodi del cluster.

L'illustrazione mostra le porte assegnate a tre domini di broadcast in un cluster a quattro nodi:

- Il dominio di broadcast "Cluster" viene creato automaticamente durante l'inizializzazione del cluster e contiene le porte a e b di ciascun nodo del cluster.
- Il dominio broadcast "Default" viene creato automaticamente anche durante l'inizializzazione del cluster e contiene le porte c e d di ciascun nodo del cluster.
- Il sistema crea automaticamente eventuali domini di broadcast aggiuntivi durante l'inizializzazione del cluster in base alla raggiungibilità della rete di livello 2. Questi domini di broadcast aggiuntivi sono denominati Default-1, Default-2 e così via.



Viene creato automaticamente un gruppo di failover con lo stesso nome e con le stesse porte di rete di ciascuno dei domini di trasmissione. Questo gruppo di failover viene gestito automaticamente dal sistema, il che significa che quando le porte vengono aggiunte o rimosse dal dominio di broadcast, vengono automaticamente aggiunte o rimosse da questo gruppo di failover.

### Aggiungere un dominio di broadcast

I domini di broadcast raggruppano le porte di rete nel cluster che appartengono alla stessa rete Layer 2. Le porte possono quindi essere utilizzate dalle SVM.

A partire da ONTAP 9.8, i domini di broadcast vengono creati automaticamente durante l'operazione di creazione o Unione del cluster. A partire da ONTAP 9.12.0, oltre ai domini di broadcast creati automaticamente, è possibile aggiungere manualmente un dominio di broadcast in Gestore di sistema.

### Prima di iniziare

Le porte che si desidera aggiungere al dominio di trasmissione non devono appartenere a un altro dominio di trasmissione. Se le porte che si desidera utilizzare appartengono a un altro dominio di trasmissione, ma non sono utilizzate, rimuoverle dal dominio di trasmissione originale.

### A proposito di questa attività

- Tutti i nomi di dominio di trasmissione devono essere univoci all'interno di un IPspace.
- Le porte aggiunte a un dominio di broadcast possono essere porte di rete fisiche, VLAN o gruppi di aggregazione di collegamenti/gruppi di interfacce (LAG/ifgrps).
- Se le porte che si desidera utilizzare appartengono a un altro dominio di broadcast, ma non sono utilizzate, rimuoverle dal dominio di broadcast esistente prima di aggiungerle al nuovo dominio.
- L'MTU (Maximum Transmission Unit) delle porte aggiunte a un dominio di broadcast viene aggiornato al valore MTU impostato nel dominio di broadcast.

- Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete Layer 2, ad eccezione del traffico di gestione della porta e0M.
- Se non si specifica un nome IPspace, il dominio di trasmissione viene creato nell'IPspace "predefinito".

Per semplificare la configurazione del sistema, viene creato automaticamente un gruppo di failover con lo stesso nome che contiene le stesse porte.

## System Manager

### Fasi

1. Selezionare **rete > Panoramica > Broadcast domain**.
2. Fare clic su **+ Add**
3. Assegnare un nome al dominio di trasmissione.
4. Impostare la MTU.
5. Selezionare IPspace.
6. Salvare il dominio di trasmissione.

È possibile modificare o eliminare un dominio di trasmissione dopo averlo aggiunto.

### CLI

In ONTAP 9.7 o versioni precedenti, è possibile creare manualmente un dominio di broadcast.

Se si utilizza ONTAP 9,8 e versioni successive, i domini di broadcast vengono creati automaticamente in base alla raggiungibilità del livello 2. Per ulteriori informazioni, vedere ["Riparare la raggiungibilità delle porte"](#).

### Fasi

1. Visualizzare le porte non attualmente assegnate a un dominio di trasmissione:

```
network port show
```

Se il display è grande, utilizzare `network port show -broadcast-domain` per visualizzare solo le porte non assegnate.

2. Creare un dominio di broadcast:

```
network port broadcast-domain create -broadcast-domain  
broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports  
ports_list]
```

a. `broadcast_domain_name` è il nome del dominio di trasmissione che si desidera creare.

b. `mtu_value` È la dimensione MTU per i pacchetti IP; 1500 e 9000 sono valori tipici.

Questo valore viene applicato a tutte le porte aggiunte a questo dominio di trasmissione.

c. `ipspace_name` È il nome dell'IPspace a cui verrà aggiunto questo dominio di trasmissione.

L'IPspace "predefinito" viene utilizzato a meno che non si specifichi un valore per questo parametro.

d. `ports_list` è l'elenco delle porte che verranno aggiunte al dominio di trasmissione.

Le porte vengono aggiunte nel formato `node_name:port_number`, ad esempio, `node1:e0c`.

3. Verificare che il dominio di trasmissione sia stato creato come desiderato:

```
network port show -instance -broadcast-domain new_domain
```

### Esempio

Il seguente comando crea il dominio di trasmissione bcast1 nell'IPSpace predefinito, imposta la MTU su 1500 e aggiunge quattro porte:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports  
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

### Al termine

È possibile definire il pool di indirizzi IP che saranno disponibili nel dominio di trasmissione creando una subnet oppure assegnare SVM e interfacce a IPSpace in questo momento. Per ulteriori informazioni, vedere ["Peering di cluster e SVM"](#).

Se è necessario modificare il nome di un dominio di trasmissione esistente, utilizzare `network port broadcast-domain rename` comando.

### Aggiunta o rimozione di porte da un dominio di broadcast (ONTAP 9,8 e versioni successive)

I domini di broadcast vengono creati automaticamente durante l'operazione di creazione o Unione del cluster. Non è necessario rimuovere manualmente le porte dai domini di broadcast.

Se la raggiungibilità della porta di rete è cambiata, tramite la connettività fisica della rete o la configurazione dello switch, e una porta di rete appartiene a un dominio di trasmissione diverso, consultare il seguente argomento:


["Riparare la raggiungibilità delle porte"](#)

## System Manager

A partire da ONTAP 9.14.1, è possibile utilizzare System Manager per riassegnare le porte Ethernet nei domini di broadcast. Si consiglia di assegnare ogni porta Ethernet a un dominio di broadcast. Pertanto, se si annulla l'assegnazione di una porta Ethernet a un dominio di broadcast, è necessario riassegnarla a un dominio di broadcast diverso.

### Fasi

Per riassegnare le porte Ethernet, attenersi alla seguente procedura:

1. Selezionare **rete > Panoramica**.
2. Nella sezione **Domini di trasmissione**, selezionare  accanto al nome di dominio.
3. Nel menu a discesa, selezionare **Modifica**.
4. Nella pagina **Modifica dominio di trasmissione**, deselezionare le porte Ethernet che si desidera riassegnare a un altro dominio.
5. Per ogni porta deselezionata viene visualizzata la finestra **Riassegna porta Ethernet**. Selezionare il dominio di notifica a cui si desidera riassegnare la porta, quindi selezionare **Riassegna**.
6. Selezionare tutte le porte che si desidera assegnare al dominio di broadcast corrente e salvare le modifiche.

### CLI

Se la raggiungibilità della porta di rete è cambiata, tramite la connettività fisica della rete o la configurazione dello switch, e una porta di rete appartiene a un dominio di trasmissione diverso, consultare il seguente argomento:

#### "Riparare la raggiungibilità delle porte"

In alternativa, è possibile aggiungere o rimuovere manualmente le porte dai domini di broadcast utilizzando `network port broadcast-domain add-ports` o il `network port broadcast-domain remove-ports` comando.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Le porte che si intende aggiungere a un dominio di trasmissione non devono appartenere a un altro dominio di trasmissione.
- Le porte che già appartengono a un gruppo di interfacce non possono essere aggiunte singolarmente a un dominio di trasmissione.

### A proposito di questa attività

Quando si aggiungono e rimuovono le porte di rete, si applicano le seguenti regole:

Quando si aggiungono porte...	Durante la rimozione delle porte...
Le porte possono essere porte di rete, VLAN o gruppi di interfacce (ifgrps).	N/A.
Le porte vengono aggiunte al gruppo di failover definito dal sistema del dominio di trasmissione.	Le porte vengono rimosse da tutti i gruppi di failover nel dominio di trasmissione.
La MTU delle porte viene aggiornata al valore MTU impostato nel dominio di trasmissione.	L'MTU delle porte non cambia.



L'IPSpace delle porte viene aggiornato al valore IPspace del dominio di trasmissione.

Le porte vengono spostate in IPspace predefinito senza attributi di dominio di trasmissione.



Se si rimuove l'ultima porta membro di un gruppo di interfacce utilizzando `network port ifgrp remove-port` determina la rimozione della porta del gruppo di interfacce dal dominio di trasmissione, in quanto non è consentita una porta vuota del gruppo di interfacce in un dominio di trasmissione.

## Fasi

1. Consente di visualizzare le porte attualmente assegnate o non assegnate a un dominio di trasmissione utilizzando `network port show` comando.
2. Aggiungere o rimuovere le porte di rete dal dominio di trasmissione:

Se si desidera...	Utilizzare...
Aggiungere porte a un dominio di broadcast	<code>network port broadcast-domain add-ports</code>
Rimuovere le porte da un dominio di broadcast	<code>network port broadcast-domain remove-ports</code>

3. Verificare che le porte siano state aggiunte o rimosse dal dominio di trasmissione:

```
network port show
```

Per ulteriori informazioni su questi comandi, vedere ["Comandi di ONTAP 9"](#).

## Esempi di aggiunta e rimozione di porte

Il seguente comando aggiunge la porta e0g sul cluster di nodi 1-01 e la porta e0g sul cluster di nodi 1-02 al dominio di trasmissione bcast1 nell'IPspace predefinito:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0g,cluster1-02:e0g
```

Il seguente comando aggiunge due porte del cluster al dominio di trasmissione Cluster nell'IPspace del cluster:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster  
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

Il seguente comando rimuove la porta e0e sul cluster di nodi 1-01 dal dominio di broadcast cast1 nell'IPspace predefinito:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain  
bcast1 -ports cluster-1-01:e0e
```

## Spostamento dei domini di broadcast in IPspace (ONTAP 9,8 e versioni successive)

Spostare i domini di broadcast creati dal sistema in base alla raggiungibilità del livello 2

negli IPspaces creati.

Prima di spostare il dominio di trasmissione, è necessario verificare la raggiungibilità delle porte nei domini di trasmissione.

La scansione automatica delle porte può determinare quali porte possono raggiungere l'una con l'altra e posizionarle nello stesso dominio di trasmissione, ma questa scansione non è in grado di determinare l'IPSpace appropriato. Se il dominio di trasmissione appartiene a un IPSpace non predefinito, è necessario spostarlo manualmente seguendo la procedura descritta in questa sezione.

### Prima di iniziare

I domini di broadcast vengono configurati automaticamente come parte delle operazioni di creazione e Unione del cluster. ONTAP definisce il dominio di broadcast "predefinito" come l'insieme di porte con connettività di livello 2 alla porta home dell'interfaccia di gestione sul primo nodo creato nel cluster. Se necessario, vengono creati altri domini di broadcast denominati **Default-1**, **Default-2** e così via.

Quando un nodo si unisce a un cluster esistente, le relative porte di rete si uniscono automaticamente ai domini di broadcast esistenti in base alla raggiungibilità del livello 2. Se non sono raggiungibili in un dominio di trasmissione esistente, le porte vengono inserite in uno o più nuovi domini di trasmissione.

### A proposito di questa attività

- Le porte con LIF del cluster vengono automaticamente inserite nell'IPSpace "Cluster".
- Le porte con raggiungibilità alla porta home della LIF di gestione dei nodi vengono inserite nel dominio broadcast "Default".
- Gli altri domini di broadcast vengono creati automaticamente da ONTAP come parte dell'operazione di creazione o Unione del cluster.
- Quando si aggiungono VLAN e gruppi di interfacce, queste vengono automaticamente inserite nel dominio di trasmissione appropriato circa un minuto dopo la loro creazione.

### Fasi

1. Verificare la raggiungibilità delle porte nei domini di trasmissione. ONTAP monitora automaticamente la raggiungibilità del Layer 2. Utilizzare il seguente comando per verificare che ogni porta sia stata aggiunta a un dominio di trasmissione e che sia "ok".

```
network port reachability show -detail
```

2. Se necessario, spostare i domini di broadcast in altri spazi IP:

```
network port broadcast-domain move
```

Ad esempio, se si desidera spostare un dominio di trasmissione da "Default" a "ips1":

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default  
-to-ipspace ips1
```

### Spostamento dei domini di broadcast in IPSpace (ONTAP 9,8 e versioni successive)

Spostare i domini di broadcast creati dal sistema in base alla raggiungibilità del livello 2 negli IPspaces creati.

Prima di spostare il dominio di trasmissione, è necessario verificare la raggiungibilità delle porte nei domini di trasmissione.

La scansione automatica delle porte può determinare quali porte possono raggiungere l'una con l'altra e posizionarle nello stesso dominio di trasmissione, ma questa scansione non è in grado di determinare l'IPSpace appropriato. Se il dominio di trasmissione appartiene a un IPSpace non predefinito, è necessario spostarlo manualmente seguendo la procedura descritta in questa sezione.

### Prima di iniziare

I domini di broadcast vengono configurati automaticamente come parte delle operazioni di creazione e Unione del cluster. ONTAP definisce il dominio di broadcast "predefinito" come l'insieme di porte con connettività di livello 2 alla porta home dell'interfaccia di gestione sul primo nodo creato nel cluster. Se necessario, vengono creati altri domini di broadcast denominati **Default-1**, **Default-2** e così via.

Quando un nodo si unisce a un cluster esistente, le relative porte di rete si uniscono automaticamente ai domini di broadcast esistenti in base alla raggiungibilità del livello 2. Se non sono raggiungibili in un dominio di trasmissione esistente, le porte vengono inserite in uno o più nuovi domini di trasmissione.

### A proposito di questa attività

- Le porte con LIF del cluster vengono automaticamente inserite nell'IPSpace "Cluster".
- Le porte con raggiungibilità alla porta home della LIF di gestione dei nodi vengono inserite nel dominio broadcast "Default".
- Gli altri domini di broadcast vengono creati automaticamente da ONTAP come parte dell'operazione di creazione o Unione del cluster.
- Quando si aggiungono VLAN e gruppi di interfacce, queste vengono automaticamente inserite nel dominio di trasmissione appropriato circa un minuto dopo la loro creazione.

### Fasi

1. Verificare la raggiungibilità delle porte nei domini di trasmissione. ONTAP monitora automaticamente la raggiungibilità del Layer 2. Utilizzare il seguente comando per verificare che ogni porta sia stata aggiunta a un dominio di trasmissione e che sia "ok".

```
network port reachability show -detail
```

2. Se necessario, spostare i domini di broadcast in altri spazi IP:

```
network port broadcast-domain move
```

Ad esempio, se si desidera spostare un dominio di trasmissione da "Default" a "ips1":

```
network port broadcast-domain move -ip-space Default -broadcast-domain Default  
-to-ip-space ips1
```

### Suddivisione dei domini di broadcast (ONTAP 9,8 e versioni successive)

Se la raggiungibilità delle porte di rete è cambiata, attraverso la connettività fisica della rete o la configurazione dello switch, Inoltre, un gruppo di porte di rete precedentemente configurate in un singolo dominio di broadcast è stato suddiviso in due diversi set di raggiungibilità, è possibile suddividere un dominio di broadcast per sincronizzare la configurazione ONTAP con la topologia di rete fisica.

Per determinare se un dominio di broadcast della porta di rete è suddiviso in più set di raggiungibilità, utilizzare `network port reachability show -details` Controllare e prestare attenzione a quali porte non sono dotate di connettività l'una con l'altra ("Porte irraggiungibili"). In genere, l'elenco delle porte irraggiungibili

definisce il set di porte che devono essere suddivise in un altro dominio di trasmissione, dopo aver verificato che la configurazione fisica e quella dello switch sono accurate.

### Fase

Suddividere un dominio di broadcast in due domini di broadcast:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` è il nome dell'ipspace in cui risiede il dominio di trasmissione.
- `-broadcast-domain` è il nome del dominio di trasmissione che verrà suddiviso.
- `-new-broadcast-domain` è il nome del nuovo dominio di trasmissione che verrà creato.
- `-ports` è il nome del nodo e la porta da aggiungere al nuovo dominio di trasmissione.

### Unione di domini di broadcast (ONTAP 9,8 e versioni successive)

Se la raggiungibilità delle porte di rete è cambiata, attraverso la connettività fisica della rete o la configurazione dello switch, e due gruppi di porte di rete precedentemente configurati in più domini di broadcast ora condividono la raggiungibilità, è possibile utilizzare l'Unione di due domini di broadcast per sincronizzare la configurazione ONTAP con la topologia fisica della rete.

Per determinare se più domini di broadcast appartengono a un set di raggiungibilità, utilizzare il comando "network port reachability show -details" e prestare attenzione a quali porte configurate in un altro dominio di broadcast hanno effettivamente la connettività l'una all'altra ("porte impreviste"). In genere, l'elenco delle porte impreviste definisce il set di porte che devono essere unite nel dominio di trasmissione dopo aver verificato che la configurazione fisica e quella dello switch sono accurate.

### Fase

Unire le porte da un dominio di broadcast in un dominio di broadcast esistente:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` è il nome dell'ipspace in cui risiedono i domini di trasmissione.
- `-broadcast-domain` è il nome del dominio di trasmissione che verrà unito.
- `-into-broadcast-domain` è il nome del dominio di trasmissione che riceverà porte aggiuntive.

### Modifica del valore MTU per le porte in un dominio di broadcast (ONTAP 9,8 e versioni successive)

È possibile modificare il valore MTU per un dominio di broadcast per modificare il valore MTU per tutte le porte in tale dominio di broadcast. Questa operazione può essere eseguita per supportare le modifiche della topologia apportate alla rete.

## Prima di iniziare

Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete Layer 2, ad eccezione del traffico di gestione della porta e0M.

## A proposito di questa attività

La modifica del valore MTU causa una breve interruzione del traffico sulle porte interessate. Il sistema visualizza un prompt che richiede di rispondere con y per modificare la MTU.

## Fase

Modificare il valore MTU per tutte le porte in un dominio di broadcast:

```
network port broadcast-domain modify -broadcast-domain  
<broadcast_domain_name> -mtu <mtu_value> [-ipSPACE <ipSPACE_name>]
```

- `broadcast_domain` è il nome del dominio di trasmissione.
- `mtu` È la dimensione MTU per i pacchetti IP; 1500 e 9000 sono valori tipici.
- `ipSPACE` È il nome dell'IPSpace in cui risiede il dominio di trasmissione. L'IPSpace "predefinito" viene utilizzato a meno che non si specifichi un valore per questa opzione. Il seguente comando modifica la MTU in 9000 per tutte le porte nel dominio di trasmissione `bcast1`:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <  
9000 >  
Warning: Changing broadcast domain settings will cause a momentary data-  
serving interruption.  
Do you want to continue? {y|n}: <y>
```

## Visualizza domini di broadcast (ONTAP 9,8 e versioni successive)

È possibile visualizzare l'elenco dei domini di broadcast all'interno di ciascun IPSpace di un cluster. L'output mostra anche l'elenco delle porte e il valore MTU per ciascun dominio di broadcast.

## Fase

Visualizzare i domini di broadcast e le porte associate nel cluster:

```
network port broadcast-domain show
```

Il seguente comando visualizza tutti i domini di trasmissione e le porte associate nel cluster:

```

network port broadcast-domain show
IPspace Broadcast
Name      Domain Name  MTU   Port List
-----
Cluster Cluster      9000
          cluster-1-01:e0a    complete
          cluster-1-01:e0b    complete
          cluster-1-02:e0a    complete
          cluster-1-02:e0b    complete
Default Default      1500
          cluster-1-01:e0c    complete
          cluster-1-01:e0d    complete
          cluster-1-02:e0c    complete
          cluster-1-02:e0d    complete
          Default-1 1500
          cluster-1-01:e0e    complete
          cluster-1-01:e0f    complete
          cluster-1-01:e0g    complete
          cluster-1-02:e0e    complete
          cluster-1-02:e0f    complete
          cluster-1-02:e0g    complete

```

Il seguente comando visualizza le porte nel dominio di trasmissione Default-1 che presentano uno stato di errore di aggiornamento, che indica che la porta non può essere aggiornata correttamente:

```

network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast
Name      Domain Name  MTU   Port List
-----
Default Default-1 1500
          cluster-1-02:e0g    error

```

Per ulteriori informazioni, vedere ["Comandi di ONTAP 9"](#).

### Eliminare un dominio di trasmissione

Se non è più necessario un dominio di trasmissione, è possibile eliminarlo. In questo modo, le porte associate al dominio di trasmissione vengono spostate nello spazio IPspace "predefinito".

#### Prima di iniziare

Non devono essere presenti subnet, interfacce di rete o SVM associate al dominio di trasmissione che si desidera eliminare.

## A proposito di questa attività

- Impossibile eliminare il dominio di trasmissione "Cluster" creato dal sistema.
- Tutti i gruppi di failover correlati al dominio di trasmissione vengono rimossi quando si elimina il dominio di trasmissione.


La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

### System Manager

**A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per eliminare un dominio di trasmissione**

L'opzione di eliminazione non viene visualizzata quando il dominio di trasmissione contiene porte o è associato a una subnet.

#### Fasi

1. Selezionare **rete > Panoramica > Broadcast domain**.
2. Selezionare  > **Elimina** accanto al dominio di trasmissione che si desidera rimuovere.

### CLI

**Utilizzare la CLI per eliminare un dominio di trasmissione**

#### Fase

Eliminazione di un dominio di broadcast:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

Il seguente comando elimina il dominio di trasmissione Default-1 in IPspace ipspace1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

## Dominio di broadcast (ONTAP 9,7 e versioni precedenti)

### Panoramica del dominio di trasmissione (ONTAP 9,7 e versioni precedenti)

I domini di broadcast sono destinati a raggruppare le porte di rete che appartengono alla stessa rete Layer 2. Le porte del gruppo possono quindi essere utilizzate da una macchina virtuale di storage (SVM) per il traffico di dati o di gestione.

Un dominio di broadcast risiede in un IPspace. Durante l'inizializzazione del cluster, il sistema crea due domini di broadcast predefiniti:

- Il dominio di trasmissione predefinito contiene le porte che si trovano nello spazio IPspace predefinito. Queste porte vengono utilizzate principalmente per la gestione dei dati. Anche le porte di gestione del cluster e dei nodi si trovano in questo dominio di broadcast.
- Il dominio di broadcast del cluster contiene le porte che si trovano in Cluster IPspace. Queste porte vengono utilizzate per la comunicazione del cluster e includono tutte le porte del cluster di tutti i nodi del cluster.

Se sono stati creati IPspaces univoci per separare il traffico client, è necessario creare un dominio di broadcast in ciascuno di questi IPspaces.



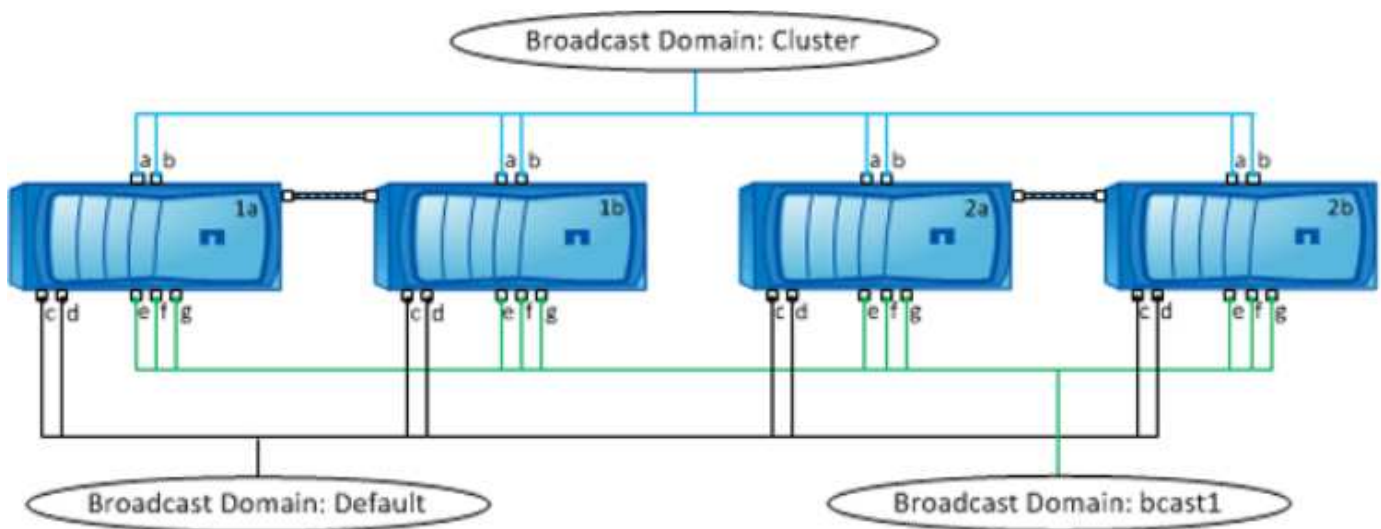
Creare un dominio di broadcast per raggruppare le porte di rete nel cluster che appartengono alla stessa rete Layer 2. Le porte possono quindi essere utilizzate dalle SVM.

#### Esempio di utilizzo di domini di broadcast

Un dominio di broadcast è un insieme di porte di rete nello stesso IPspace che ha anche la raggiungibilità di livello 2 l'una rispetto all'altra, incluse generalmente le porte di molti nodi del cluster.

L'illustrazione mostra le porte assegnate a tre domini di broadcast in un cluster a quattro nodi:

- Il dominio di broadcast del cluster viene creato automaticamente durante l'inizializzazione del cluster e contiene le porte a e b di ciascun nodo del cluster.
- Il dominio di broadcast predefinito viene creato automaticamente anche durante l'inizializzazione del cluster e contiene le porte c e d di ciascun nodo del cluster.
- Il dominio di broadcast bcast1 è stato creato manualmente e contiene le porte e, f e g di ciascun nodo del cluster. Questo dominio di broadcast è stato creato dall'amministratore di sistema specificamente per consentire a un nuovo client di accedere ai dati attraverso una nuova SVM.



Viene creato automaticamente un gruppo di failover con lo stesso nome e con le stesse porte di rete di ciascuno dei domini di trasmissione. Questo gruppo di failover viene gestito automaticamente dal sistema, il che significa che quando le porte vengono aggiunte o rimosse dal dominio di broadcast, vengono automaticamente aggiunte o rimosse da questo gruppo di failover.

#### Determinazione delle porte che possono essere utilizzate per un dominio di trasmissione (ONTAP 9,7 e versioni precedenti)

Prima di poter configurare un dominio di trasmissione da aggiungere al nuovo IPspace, è necessario determinare quali porte sono disponibili per il dominio di trasmissione.



Questa attività è pertinente per ONTAP 9.0 - 9.7, non per ONTAP 9.8.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.



## A proposito di questa attività

- Le porte possono essere porte fisiche, VLAN o gruppi di interfacce (ifgroup).
- Le porte che si desidera aggiungere al nuovo dominio di trasmissione non possono essere assegnate a un dominio di trasmissione esistente.
- Se le porte che si desidera aggiungere al dominio di trasmissione si trovano già in un altro dominio di trasmissione (ad esempio, il dominio di trasmissione predefinito in IPSpace predefinito), è necessario rimuovere le porte da tale dominio di trasmissione prima di assegnarle al nuovo dominio di trasmissione.
- Le porte a cui sono assegnati LIF non possono essere rimosse da un dominio di broadcast.
- Poiché le LIF di gestione del cluster e dei nodi sono assegnate al dominio di broadcast predefinito in IPSpace predefinito, le porte assegnate a queste LIF non possono essere rimosse dal dominio di broadcast predefinito.

## Fasi

1. Determinare le assegnazioni correnti delle porte.

```
network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
-----	----	-----	-----	-----	----	-----
node1						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000
node2						
	e0a	Cluster	Cluster	up	9000	auto/1000
	e0b	Cluster	Cluster	up	9000	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
	e0e	Default	Default	up	1500	auto/1000
	e0f	Default	Default	up	1500	auto/1000
	e0g	Default	Default	up	1500	auto/1000

In questo esempio, l'output del comando fornisce le seguenti informazioni:

- Porte e0c, e0d, e0e, e0f, e. e0g Su ciascun nodo vengono assegnati al dominio di broadcast predefinito.
  - Queste porte sono potenzialmente disponibili per l'utilizzo nel dominio di trasmissione dell'IPSpace che si desidera creare.
2. Determinare quali porte nel dominio di broadcast predefinito sono assegnate alle interfacce LIF e quindi non possono essere spostate in un nuovo dominio di broadcast.

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
Cluster						
	node1_clus1	up/up	10.0.2.40/24	node1	e0a	true
	node1_clus2	up/up	10.0.2.41/24	node1	e0b	true
	node2_clus1	up/up	10.0.2.42/24	node2	e0a	true
	node2_clus2	up/up	10.0.2.43/24	node2	e0b	true
cluster1						
	cluster_mgmt	up/up	10.0.1.41/24	node1	e0c	true
	node1_mgmt	up/up	10.0.1.42/24	node1	e0c	true
	node2_mgmt	up/up	10.0.1.43/24	node2	e0c	true

Nell'esempio seguente, l'output del comando fornisce le seguenti informazioni:

- Le porte del nodo vengono assegnate alla porta e0c. Su ciascun nodo e il nodo principale della LIF amministrativa del cluster è attivo e0c acceso node1.
- Porte e0d, e0e, e0f, e. e0g. Su ogni nodo non sono presenti LIF e possono essere rimossi dal dominio di broadcast predefinito e quindi aggiunti a un nuovo dominio di broadcast per il nuovo IPspace.

## Creare un dominio di trasmissione (ONTAP 9.7 e versioni precedenti)

In ONTAP 9.7 e versioni precedenti, si crea un dominio di broadcast per raggruppare le porte di rete del cluster che appartengono alla stessa rete Layer 2. Le porte possono quindi essere utilizzate dalle SVM. È necessario creare un dominio di trasmissione per un IPspace personalizzato. Le SVM create in IPspace utilizzano le porte nel dominio di trasmissione.



Questa attività è pertinente per ONTAP 9.0 - 9.7, non per ONTAP 9.8.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

A partire da ONTAP 9.8, i domini di broadcast vengono creati automaticamente durante l'operazione di creazione o Unione del cluster. Se si utilizza ONTAP 9.8 o versione successiva, questa procedura non è necessaria.

In ONTAP 9.7 e versioni precedenti, le porte che si intende aggiungere al dominio di trasmissione non devono appartenere a un altro dominio di trasmissione.

### A proposito di questa attività

La porta a cui si verifica il failover di LIF deve essere membro del gruppo di failover per LIF. Quando si crea un dominio di broadcast, ONTAP crea automaticamente un gruppo di failover con lo stesso nome. Il gruppo di failover contiene tutte le porte assegnate al dominio di trasmissione.

- Tutti i nomi di dominio di trasmissione devono essere univoci all'interno di un IPspace.

- Le porte aggiunte a un dominio di broadcast possono essere porte di rete fisiche, VLAN o gruppi di interfacce (ifgrps).
- Se le porte che si desidera utilizzare appartengono a un altro dominio di trasmissione, ma non sono utilizzate, utilizzare `network port broadcast-domain remove-ports` per rimuovere le porte dal dominio di trasmissione esistente.
- Le MTU delle porte aggiunte a un dominio di trasmissione vengono aggiornate al valore MTU impostato nel dominio di trasmissione.
- Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete Layer 2, ad eccezione del traffico di gestione della porta e0M.
- Se non si specifica un nome IPspace, il dominio di trasmissione viene creato nell'IPspace "predefinito".

Per semplificare la configurazione del sistema, viene creato automaticamente un gruppo di failover con lo stesso nome che contiene le stesse porte.

## Fasi

1. Visualizzare le porte non attualmente assegnate a un dominio di trasmissione:

```
network port show
```

Se il display è grande, utilizzare `network port show -broadcast-domain` per visualizzare solo le porte non assegnate.

2. Creare un dominio di broadcast:

```
network port broadcast-domain create -broadcast-domain broadcast_domain_name
-mtu mtu_value [-ipSPACE ipSPACE_name] [-ports ports_list]
```

◦ *broadcast\_domain\_name* è il nome del dominio di trasmissione che si desidera creare.

◦ *mtu\_value* È la dimensione MTU per i pacchetti IP; 1500 e 9000 sono valori tipici.

Questo valore viene applicato a tutte le porte aggiunte a questo dominio di trasmissione.

◦ *ipSPACE\_name* È il nome dell'IPspace a cui verrà aggiunto questo dominio di trasmissione.

L'IPspace "predefinito" viene utilizzato a meno che non si specifichi un valore per questo parametro.

◦ *ports\_list* è l'elenco delle porte che verranno aggiunte al dominio di trasmissione.

Le porte vengono aggiunte nel formato *node\_name:port\_number*, ad esempio, `node1:e0c`.

3. Verificare che il dominio di trasmissione sia stato creato come desiderato:

```
network port show -instance -broadcast-domain new_domain
```

## Esempio

Il seguente comando crea il dominio di trasmissione `bcast1` nell'IPspace predefinito, imposta la MTU su 1500 e aggiunge quattro porte:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

## Al termine

È possibile definire il pool di indirizzi IP che saranno disponibili nel dominio di trasmissione creando una subnet oppure assegnare SVM e interfacce a IPspace in questo momento. Per ulteriori informazioni, vedere ["Peering di cluster e SVM"](#).

Se è necessario modificare il nome di un dominio di trasmissione esistente, utilizzare `network port broadcast-domain rename` comando.

**Aggiunta o rimozione di porte da un dominio di trasmissione (ONTAP 9,7 e versioni precedenti)**

È possibile aggiungere porte di rete durante la creazione iniziale di un dominio di trasmissione oppure aggiungere o rimuovere porte da un dominio di trasmissione già esistente. Ciò consente di utilizzare in modo efficiente tutte le porte del cluster.

Se le porte che si desidera aggiungere al nuovo dominio di trasmissione si trovano già in un altro dominio di trasmissione, è necessario rimuovere le porte da tale dominio di trasmissione prima di assegnarle al nuovo dominio di trasmissione.



Questa attività è pertinente per ONTAP 9.0 - 9.7, non per ONTAP 9.8.

**Prima di iniziare**

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Le porte che si intende aggiungere a un dominio di trasmissione non devono appartenere a un altro dominio di trasmissione.
- Le porte che già appartengono a un gruppo di interfacce non possono essere aggiunte singolarmente a un dominio di trasmissione.

**A proposito di questa attività**

Quando si aggiungono e rimuovono le porte di rete, si applicano le seguenti regole:

Quando si aggiungono porte...	Durante la rimozione delle porte...
Le porte possono essere porte di rete, VLAN o gruppi di interfacce (ifgrps).	N/A.
Le porte vengono aggiunte al gruppo di failover definito dal sistema del dominio di trasmissione.	Le porte vengono rimosse da tutti i gruppi di failover nel dominio di trasmissione.
La MTU delle porte viene aggiornata al valore MTU impostato nel dominio di trasmissione.	L'MTU delle porte non cambia.
L'IPspace delle porte viene aggiornato al valore IPspace del dominio di trasmissione.	Le porte vengono spostate in IPspace predefinito senza attributi di dominio di trasmissione.



Se si rimuove l'ultima porta membro di un gruppo di interfacce utilizzando `network port ifgrp remove-port` determina la rimozione della porta del gruppo di interfacce dal dominio di trasmissione, in quanto non è consentita una porta vuota del gruppo di interfacce in un dominio di trasmissione.

**Fasi**

1. Consente di visualizzare le porte attualmente assegnate o non assegnate a un dominio di trasmissione utilizzando `network port show` comando.

## 2. Aggiungere o rimuovere le porte di rete dal dominio di trasmissione:

Se si desidera...	Utilizzare...
Aggiungere porte a un dominio di broadcast	<code>network port broadcast-domain add-ports</code>
Rimuovere le porte da un dominio di broadcast	<code>network port broadcast-domain remove-ports</code>

## 3. Verificare che le porte siano state aggiunte o rimosse dal dominio di trasmissione:

```
network port show
```

Per ulteriori informazioni su questi comandi, vedere ["Comandi di ONTAP 9"](#).

### Esempi di aggiunta e rimozione di porte

Il seguente comando aggiunge la porta e0g sul cluster di nodi 1-01 e la porta e0g sul cluster di nodi 1-02 al dominio di trasmissione bcast1 nell'IPSpace predefinito:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0g,cluster1-02:e0g
```

Il seguente comando aggiunge due porte del cluster al dominio di trasmissione Cluster nell'IPSpace del cluster:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster  
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

Il seguente comando rimuove la porta e0e sul cluster di nodi 1-01 dal dominio di broadcast cast1 nell'IPSpace predefinito:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0e
```

### Suddivisione dei domini di broadcast (ONTAP 9.7 o versioni precedenti)

È possibile modificare un dominio di broadcast esistente suddividendolo in due domini di broadcast diversi, con ciascun dominio di broadcast contenente alcune delle porte originali assegnate al dominio di broadcast originale.

#### A proposito di questa attività

- Se le porte si trovano in un gruppo di failover, è necessario suddividere tutte le porte di un gruppo di failover.
- Se alle porte sono associati LIF, i LIF non possono far parte degli intervalli di una subnet.

#### Fase

Suddividere un dominio di broadcast in due domini di broadcast:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` È il nome dell'IPSpace in cui risiede il dominio di trasmissione.
- `-broadcast-domain` è il nome del dominio di trasmissione che verrà suddiviso.
- `-new-broadcast-domain` è il nome del nuovo dominio di trasmissione che verrà creato.
- `-ports` è il nome del nodo e la porta da aggiungere al nuovo dominio di trasmissione.

### Unione di domini di broadcast (ONTAP 9,7 e versioni precedenti)

È possibile spostare tutte le porte da un dominio di broadcast a un dominio di broadcast esistente utilizzando il comando `merge`.

Questa operazione riduce i passaggi necessari per rimuovere tutte le porte da un dominio di trasmissione e aggiungerle a un dominio di trasmissione esistente.

#### Fase

Unire le porte da un dominio di broadcast in un dominio di broadcast esistente:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` È il nome dell'IPSpace in cui risiedono i domini di trasmissione.
- `-broadcast-domain` è il nome del dominio di trasmissione che verrà unito.
- `-into-broadcast-domain` è il nome del dominio di trasmissione che riceverà porte aggiuntive.

#### Esempio

Il seguente esempio unisce il dominio di trasmissione `bd-data1` al dominio di trasmissione `bd-data2`:

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-
data2
```

### Modifica del valore MTU per le porte in un dominio di broadcast (ONTAP 9,7 e versioni precedenti)

È possibile modificare il valore MTU per un dominio di broadcast per modificare il valore MTU per tutte le porte in tale dominio di broadcast. Questa operazione può essere eseguita per supportare le modifiche della topologia apportate alla rete.

#### Prima di iniziare

Il valore MTU deve corrispondere a tutti i dispositivi connessi a tale rete Layer 2, ad eccezione del traffico di gestione della porta e0M.

#### A proposito di questa attività

La modifica del valore MTU causa una breve interruzione del traffico sulle porte interessate. Il sistema visualizza un prompt che richiede di rispondere con y per modificare la MTU.

### Fase

Modificare il valore MTU per tutte le porte in un dominio di broadcast:

```
network port broadcast-domain modify -broadcast-domain  
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` è il nome del dominio di trasmissione.
- `mtu` È la dimensione MTU per i pacchetti IP; 1500 e 9000 sono valori tipici.
- `ipspace` È il nome dell'IPSpace in cui risiede il dominio di trasmissione. L'IPSpace "predefinito" viene utilizzato a meno che non si specifichi un valore per questa opzione. Il seguente comando modifica la MTU in 9000 per tutte le porte nel dominio di trasmissione `bcast1`:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <  
9000 >  
Warning: Changing broadcast domain settings will cause a momentary data-  
serving interruption.  
Do you want to continue? {y|n}: <y>
```

### Visualizzazione dei domini di broadcast (ONTAP 9,7 e versioni precedenti)

È possibile visualizzare l'elenco dei domini di broadcast all'interno di ciascun IPSpace di un cluster. L'output mostra anche l'elenco delle porte e il valore MTU per ciascun dominio di broadcast.

### Fase

Visualizzare i domini di broadcast e le porte associate nel cluster:

```
network port broadcast-domain show
```

Il seguente comando visualizza tutti i domini di trasmissione e le porte associate nel cluster:

```

network port broadcast-domain show
IPspace Broadcast
Name      Domain Name  MTU   Port List
-----
Cluster Cluster      9000
          cluster-1-01:e0a    complete
          cluster-1-01:e0b    complete
          cluster-1-02:e0a    complete
          cluster-1-02:e0b    complete
Default Default      1500
          cluster-1-01:e0c    complete
          cluster-1-01:e0d    complete
          cluster-1-02:e0c    complete
          cluster-1-02:e0d    complete
          bcast1      1500
          cluster-1-01:e0e    complete
          cluster-1-01:e0f    complete
          cluster-1-01:e0g    complete
          cluster-1-02:e0e    complete
          cluster-1-02:e0f    complete
          cluster-1-02:e0g    complete

```

Il seguente comando visualizza le porte nel dominio di trasmissione bcast1 che presentano uno stato di errore di aggiornamento, che indica che la porta non può essere aggiornata correttamente:

```

network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error

IPspace Broadcast
Name      Domain Name  MTU   Port List
-----
Default bcast1      1500
          cluster-1-02:e0g    error

```

Per ulteriori informazioni, vedere ["Comandi di ONTAP 9"](#).

### Eliminare un dominio di trasmissione

Se non è più necessario un dominio di trasmissione, è possibile eliminarlo. In questo modo, le porte associate al dominio di trasmissione vengono spostate nello spazio IPspace "predefinito".

#### Prima di iniziare

Non devono essere presenti subnet, interfacce di rete o SVM associate al dominio di trasmissione che si desidera eliminare.



### A proposito di questa attività

- Impossibile eliminare il dominio di trasmissione "Cluster" creato dal sistema.
- Tutti i gruppi di failover correlati al dominio di trasmissione vengono rimossi quando si elimina il dominio di trasmissione.


La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

#### System Manager

**A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per eliminare un dominio di trasmissione**

L'opzione di eliminazione non viene visualizzata quando il dominio di trasmissione contiene porte o è associato a una subnet.

#### Fasi

1. Selezionare **rete > Panoramica > Broadcast domain**.
2. Selezionare  > **Elimina** accanto al dominio di trasmissione che si desidera rimuovere.

#### CLI

**Utilizzare la CLI per eliminare un dominio di trasmissione**

#### Fase

Eliminazione di un dominio di broadcast:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipSPACE ipSPACE_name]
```

Il seguente comando elimina il dominio di trasmissione Default-1 in IPSPACE ipSPACE1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipSPACE
ipSPACE1
```

## Gruppi e policy di failover

### Panoramica sul failover LIF

Il failover LIF si riferisce alla migrazione automatica di una LIF a una porta di rete diversa in risposta a un errore di collegamento sulla porta corrente della LIF. Si tratta di un componente chiave per fornire alta disponibilità per le connessioni alle SVM. La configurazione del failover LIF comporta la creazione di un gruppo di failover, la modifica della LIF per l'utilizzo del gruppo di failover e la specifica di una policy di failover.

Un gruppo di failover contiene un set di porte di rete (porte fisiche, VLAN e gruppi di interfacce) da uno o più nodi in un cluster. Le porte di rete presenti nel gruppo di failover definiscono le destinazioni di failover disponibili per LIF. A un gruppo di failover possono essere assegnate le LIF di gestione del cluster, dei nodi, dell'intercluster e dei dati NAS.



Quando una LIF viene configurata senza una destinazione di failover valida, si verifica un'interruzione quando la LIF tenta di eseguire il failover. È possibile utilizzare il comando "network interface show -failover" per verificare la configurazione del failover.

Quando si crea un dominio di broadcast, viene creato automaticamente un gruppo di failover con lo stesso nome che contiene le stesse porte di rete. Questo gruppo di failover viene gestito automaticamente dal sistema, il che significa che quando le porte vengono aggiunte o rimosse dal dominio di broadcast, vengono automaticamente aggiunte o rimosse da questo gruppo di failover. Questo è un'efficienza per gli amministratori che non desiderano gestire i propri gruppi di failover.

## Creare un gruppo di failover

Si crea un gruppo di failover di porte di rete in modo che una LIF possa migrare automaticamente a una porta diversa se si verifica un errore di collegamento sulla porta corrente della LIF. Questo consente al sistema di reindirizzare il traffico di rete ad altre porte disponibili nel cluster.

### A proposito di questa attività

Si utilizza `network interface failover-groups create` per creare il gruppo e aggiungere le porte al gruppo.

- Le porte aggiunte a un gruppo di failover possono essere porte di rete, VLAN o gruppi di interfacce (ifgrps).
- Tutte le porte aggiunte al gruppo di failover devono appartenere allo stesso dominio di broadcast.
- Una singola porta può risiedere in più gruppi di failover.
- Se si dispone di LIF in diverse VLAN o domini di broadcast, è necessario configurare i gruppi di failover per ogni VLAN o dominio di broadcast.
- I gruppi di failover non si applicano negli ambienti SAN iSCSI o FC.

### Fase

Creare un gruppo di failover:

```
network interface failover-groups create -vserver vs1 -failover-group failover_group_name -targets ports_list
```

- `vs1` È il nome della SVM che può utilizzare il gruppo di failover.
- `failover_group_name` è il nome del gruppo di failover che si desidera creare.
- `ports_list` è l'elenco delle porte che verranno aggiunte al gruppo di failover. Le porte vengono aggiunte nel formato `node_name>:port_number`, ad esempio `node1:e0c`.

Il seguente comando crea il gruppo di failover fg3 per SVM vs3 e aggiunge due porte:

```
network interface failover-groups create -vserver vs3 -failover-group fg3 -targets cluster1-01:e0e,cluster1-02:e0e
```

### Al termine

- Ora che il gruppo di failover è stato creato, è necessario applicare il gruppo di failover a una LIF.

- L'applicazione di un gruppo di failover che non fornisce una destinazione di failover valida per una LIF genera un messaggio di avviso.

Se un LIF che non dispone di una destinazione di failover valida tenta di eseguire il failover, potrebbe verificarsi un'interruzione.

## Configurare le impostazioni di failover su una LIF

È possibile configurare una LIF per il failover su un gruppo specifico di porte di rete applicando una policy di failover e un gruppo di failover alla LIF. È anche possibile disattivare il failover di una LIF su un'altra porta.

### A proposito di questa attività

- Quando viene creato un LIF, il failover LIF viene attivato per impostazione predefinita e l'elenco delle porte di destinazione disponibili viene determinato dal gruppo di failover predefinito e dalla policy di failover basata sul tipo LIF e sulla policy di servizio.

A partire da 9.5, è possibile specificare una politica di servizio per la LIF che definisce quali servizi di rete possono utilizzare la LIF. Alcuni servizi di rete impongono restrizioni di failover su una LIF.



Se la policy di servizio di una LIF viene modificata in modo da limitare ulteriormente il failover, la policy di failover della LIF viene aggiornata automaticamente dal sistema.

- È possibile modificare il comportamento di failover dei LIF specificando i valori per i parametri `-failover-group` e `-failover-policy` nel comando di modifica dell'interfaccia di rete.
- La modifica di una LIF che non ha una destinazione di failover valida per la LIF genera un messaggio di avviso.

Se un LIF che non dispone di una destinazione di failover valida tenta di eseguire il failover, potrebbe verificarsi un'interruzione.

- A partire da ONTAP 9.11.1, sulle piattaforme ASA (All-Flash SAN Array), il failover LIF iSCSI viene abilitato automaticamente alle LIF iSCSI appena create sulle macchine virtuali storage appena create.

Inoltre, è possibile "[Abilitazione manuale del failover iSCSI LIF su LIF iSCSI pre-esistenti](#)", Ovvero le LIF create prima dell'aggiornamento a ONTAP 9.11.1 o versioni successive.

- L'elenco seguente descrive come l'impostazione `-failover-policy` influenza le porte di destinazione selezionate dal gruppo di failover:



Per il failover LIF iSCSI, solo le policy di failover `local-only`, `sfo-partner-only` e `disabled` sono supportati.

- `broadcast-domain-wide` Si applica a tutte le porte su tutti i nodi del gruppo di failover.
- `system-defined` Si applica solo a quelle porte sul nodo home di LIF e a un altro nodo del cluster, in genere un partner non SFO, se esistente.
- `local-only` Si applica solo a quelle porte sul nodo home di LIF.
- `sfo-partner-only` Si applica solo a quelle porte sul nodo principale della LIF e al suo partner SFO.
- `disabled` Indica che la LIF non è configurata per il failover.

Fase

Configurare le impostazioni di failover per un'interfaccia esistente:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

Esempi di configurazione delle impostazioni di failover e disattivazione del failover

Il seguente comando imposta il criterio di failover su broadcast-domain-wide e utilizza le porte del gruppo di failover fg3 come destinazioni di failover per i dati LIF 1 su SVM vs3:

```
network interface modify -vserver vs3 -lif data1 failover-policy
broadcast-domain-wide - failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif                failover-policy                failover-group
-----
vs3      data1              broadcast-domain-wide      fg3
```

Il seguente comando disattiva il failover per LIF data1 su SVM vs3:

```
network interface modify -vserver vs3 -lif data1 failover-policy disabled
```

Comandi per la gestione di policy e gruppi di failover

È possibile utilizzare network interface failover-groups comandi per gestire i gruppi di failover. Si utilizza network interface modify Comando per gestire i gruppi di failover e le policy di failover applicate a una LIF.

Se si desidera...	Utilizzare questo comando...
Aggiungere porte di rete a un gruppo di failover	network interface failover-groups add-targets
Rimuovere le porte di rete da un gruppo di failover	network interface failover-groups remove-targets
Modificare le porte di rete in un gruppo di failover	network interface failover-groups modify
Visualizza i gruppi di failover correnti	network interface failover-groups show

Configurare il failover su una LIF	<code>network interface modify -failover -group -failover-policy</code>
Visualizzare il gruppo di failover e la policy di failover utilizzati da ciascun LIF	<code>network interface show -fields failover-group, failover-policy</code>
Rinominare un gruppo di failover	<code>network interface failover-groups rename</code>
Eliminare un gruppo di failover	<code>network interface failover-groups delete</code>



La modifica di un gruppo di failover in modo che non fornisca una destinazione di failover valida per qualsiasi LIF nel cluster può causare un'interruzione quando un LIF tenta di eseguire il failover.

Per ulteriori informazioni, consultare le pagine man del `network interface failover-groups` e `network interface modify` comandi.

## Subnet (solo amministratori del cluster)

### Panoramica subnet

Le subnet consentono di allocare blocchi o pool specifici di indirizzi IP per la configurazione di rete ONTAP. In questo modo è possibile creare file LIF più facilmente specificando un nome di subnet invece di specificare i valori dell'indirizzo IP e della maschera di rete.

Una subnet viene creata all'interno di un dominio di trasmissione e contiene un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Gli indirizzi IP in una subnet vengono allocati alle porte nel dominio di trasmissione quando vengono create le LIF. Una volta rimossi i file LIF, gli indirizzi IP vengono restituiti al pool di subnet e sono disponibili per i file LIF futuri.

Si consiglia di utilizzare le subnet perché semplificano notevolmente la gestione degli indirizzi IP e semplificano la creazione di LIF. Inoltre, se si specifica un gateway durante la definizione di una subnet, una route predefinita a tale gateway viene aggiunta automaticamente alla SVM quando viene creata una LIF utilizzando tale subnet.

### Creare una subnet

È possibile creare una subnet per allocare blocchi specifici di indirizzi IPv4 o IPv6 da utilizzare in seguito quando si creano LIF per SVM.

In questo modo è possibile creare LIF più facilmente specificando un nome di subnet invece di dover specificare i valori dell'indirizzo IP e della maschera di rete per ciascun LIF.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Il dominio di trasmissione e l'IPSpace in cui si intende aggiungere la subnet devono già esistere.

#### **A proposito di questa attività**

- Tutti i nomi di subnet devono essere univoci all'interno di un IPSpace.
- Quando si aggiungono intervalli di indirizzi IP a una subnet, assicurarsi che non vi siano indirizzi IP sovrapposti nella rete in modo che sottoreti o host diversi non tentino di utilizzare lo stesso indirizzo IP.
- Se si specifica un gateway durante la definizione di una subnet, un percorso predefinito per tale gateway viene aggiunto automaticamente alla SVM quando viene creata una LIF utilizzando tale subnet. Se non si utilizzano sottoreti o se non si specifica un gateway durante la definizione di una subnet, è necessario utilizzare `route create` Comando per aggiungere manualmente un percorso alla SVM.

#### **Procedura**

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestore di sistema per creare una subnet.

### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Fare clic su **+ Add** per creare una subnet.
3. Assegnare un nome alla subnet.
4. Specificare l'indirizzo IP della subnet.
5. Impostare la subnet mask.
6. Definire l'intervallo di indirizzi IP che compongono la subnet.
7. Se utile, specificare un gateway.
8. Selezionare il dominio di trasmissione a cui appartiene la subnet.
9. Salvare le modifiche.
  - a. Se l'indirizzo IP o l'intervallo immesso è già utilizzato da un'interfaccia, viene visualizzato il seguente messaggio:  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. Facendo clic su **OK**, la LIF esistente viene associata alla subnet.

### CLI

Utilizzare la CLI per creare una subnet.

```
network subnet create -subnet-name subnet_name -broadcast-domain  
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet  
<subnet_address> [-gateway <gateway_address>] [-ip-ranges  
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` è il nome della subnet di livello 3 che si desidera creare.

Il nome può essere una stringa di testo come "Mgmt" o un valore IP di subnet specifico come 192.0.2.0/24.

- `broadcast_domain_name` è il nome del dominio di trasmissione in cui risiede la subnet.
- `ipspace_name` È il nome dell'IPSpace di cui fa parte il dominio di trasmissione.

L'IPSpace "predefinito" viene utilizzato a meno che non si specifichi un valore per questa opzione.

- `subnet_address` È l'indirizzo IP e la maschera della subnet, ad esempio 192.0.2.0/24.
- `gateway_address` è il gateway per il percorso predefinito della subnet, ad esempio 192.0.2.1.
- `ip_address_list` Indica l'elenco o l'intervallo di indirizzi IP che verranno assegnati alla subnet.

Gli indirizzi IP possono essere singoli, un intervallo di indirizzi IP o una combinazione in un elenco separato da virgole.

- Il valore `true` può essere impostato per `-force-update-lif-associations` opzione.

Questo comando non riesce se un processore di servizio o un'interfaccia di rete sta attualmente utilizzando gli indirizzi IP nell'intervallo specificato. Impostando questo valore su `true`, tutte le interfacce indirizzate manualmente vengono associate alla subnet corrente e il comando viene eseguito correttamente.

Il seguente comando crea la subnet `sub1` nel dominio di trasmissione `Default-1` nell'IPSpace predefinito. Aggiunge un indirizzo IP e una maschera della subnet IPv4, il gateway e un intervallo di indirizzi IP:

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

Il seguente comando crea la subnet `sub2` nel dominio di trasmissione predefinito in IPSpace "Default". Aggiunge una serie di indirizzi IPv6:

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

#### Al termine

È possibile assegnare le SVM e le interfacce a un IPSpace utilizzando gli indirizzi nella subnet.

Se è necessario modificare il nome di una subnet esistente, utilizzare `network subnet rename` comando.

## Aggiungere o rimuovere indirizzi IP da una subnet

È possibile aggiungere indirizzi IP durante la creazione iniziale di una subnet oppure aggiungere indirizzi IP a una subnet già esistente. È inoltre possibile rimuovere gli indirizzi IP da una subnet esistente. In questo modo è possibile allocare solo gli indirizzi IP richiesti per le SVM.


La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:



## System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per aggiungere o rimuovere indirizzi IP da o verso una subnet

### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Selezionare  > **Modifica** accanto alla subnet che si desidera modificare.
3. Aggiungere o rimuovere indirizzi IP.
4. Salvare le modifiche.
  - a. Se l'indirizzo IP o l'intervallo immesso è già utilizzato da un'interfaccia, viene visualizzato il seguente messaggio:  
`An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
  - b. Facendo clic su **OK**, la LIF esistente viene associata alla subnet.

### CLI

Utilizzare la CLI per aggiungere o rimuovere indirizzi IP da o verso una subnet

#### A proposito di questa attività

Quando si aggiungono indirizzi IP, viene visualizzato un errore se un processore di servizio o un'interfaccia di rete utilizza gli indirizzi IP dell'intervallo aggiunto. Se si desidera associare qualsiasi interfaccia indirizzata manualmente alla subnet corrente, è possibile impostare `-force-update-lif-associations` opzione a `true`.

Quando si rimuovono gli indirizzi IP, viene visualizzato un messaggio di errore se un processore di servizio o un'interfaccia di rete utilizza gli indirizzi IP da rimuovere. Se si desidera che le interfacce continuino a utilizzare gli indirizzi IP dopo che sono state rimosse dalla subnet, è possibile impostare `-force-update-lif-associations` opzione a `true`.

### Fase

Aggiungere o rimuovere indirizzi IP da una subnet:

Se si desidera...	Utilizzare questo comando...
Aggiungere indirizzi IP a una subnet	<code>subnet add-range</code> di rete
Rimuovere gli indirizzi IP da una subnet	<code>remove-ranges subnet</code> di rete

Per ulteriori informazioni su questi comandi, consulta le pagine man.

Il seguente comando aggiunge gli indirizzi IP da 192.0.2.82 a 192.0.2.85 alla subnet sub1:

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

Il seguente comando rimuove l'indirizzo IP 198.51.100.9 dalla subnet sub3:

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges  
<198.51.100.9>
```

Se l'intervallo corrente include da 1 a 10 e da 20 a 40 e si desidera aggiungere da 11 a 19 e da 41 a 50 (consentendo in pratica da 1 a 50), è possibile sovrapporre l'intervallo di indirizzi esistente utilizzando il comando seguente. Questo comando aggiunge solo i nuovi indirizzi e non influisce sugli indirizzi esistenti:

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-  
198.51.10.50>
```

## Modificare le proprietà della subnet

È possibile modificare l'indirizzo di sottorete e il valore della maschera, l'indirizzo del gateway o l'intervallo di indirizzi IP in una subnet esistente.

### A proposito di questa attività

- Quando si modificano gli indirizzi IP, è necessario assicurarsi che non vi siano indirizzi IP sovrapposti nella rete in modo che sottoreti o host diversi non tentino di utilizzare lo stesso indirizzo IP.
- Se si aggiunge o si modifica l'indirizzo IP del gateway, il gateway modificato viene applicato alle nuove SVM quando in esse viene creata una LIF utilizzando la subnet. Se il percorso non esiste già, viene creato un percorso predefinito per il gateway SVM. Potrebbe essere necessario aggiungere manualmente un nuovo percorso alla SVM quando si modifica l'indirizzo IP del gateway.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione di sistema per modificare le proprietà della subnet

### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Selezionare **> Modifica** accanto alla subnet che si desidera modificare.
3. Apportare modifiche.
4. Salvare le modifiche.
  - a. Se l'indirizzo IP o l'intervallo immesso è già utilizzato da un'interfaccia, viene visualizzato il seguente messaggio:  
An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?
  - b. Facendo clic su **OK**, la LIF esistente viene associata alla subnet.

### CLI

#### Utilizzare la CLI per modificare le proprietà della subnet

#### Fase

Modificare le proprietà della subnet:

```
network subnet modify -subnet-name <subnet_name> [-ipSPACE  
<ipSPACE_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]  
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` è il nome della subnet che si desidera modificare.
- `ipSPACE` È il nome dell'IPSpace in cui risiede la subnet.
- `subnet` è il nuovo indirizzo e la nuova maschera della subnet, se applicabile; ad esempio, 192.0.2.0/24.
- `gateway` è il nuovo gateway della subnet, se applicabile; ad esempio, 192.0.2.1. L'immissione di "" rimuove la voce del gateway.
- `ip_ranges` È il nuovo elenco, o intervallo, di indirizzi IP che verranno allocati alla subnet, se applicabile. Gli indirizzi IP possono essere singoli indirizzi, un intervallo o indirizzi IP o una combinazione in un elenco separato da virgole. L'intervallo specificato qui sostituisce gli indirizzi IP esistenti.
- `force-update-lif-associations` È necessario quando si modifica l'intervallo di indirizzi IP. È possibile impostare il valore su **true** per questa opzione quando si modifica l'intervallo di indirizzi IP. Questo comando non riesce se un processore di servizio o un'interfaccia di rete utilizza gli indirizzi IP nell'intervallo specificato. Impostando questo valore su **true**, qualsiasi interfaccia indirizzata manualmente viene associata alla subnet corrente e il comando viene eseguito correttamente.

Il seguente comando modifica l'indirizzo IP del gateway della subnet sub3:

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

## Visualizzare le subnet

È possibile visualizzare l'elenco degli indirizzi IP allocati a ciascuna subnet all'interno di un IPspace. L'output mostra anche il numero totale di indirizzi IP disponibili in ciascuna subnet e il numero di indirizzi attualmente utilizzati.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

### System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per visualizzare le subnet

#### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Visualizzare l'elenco delle subnet.

### CLI

Utilizzare la CLI per visualizzare le subnet

#### Fase

Visualizzare l'elenco delle subnet e gli intervalli di indirizzi IP associati utilizzati in tali subnet:

```
network subnet show
```

Il seguente comando visualizza le subnet e le proprietà della subnet:

```
network subnet show

IPspace: Default
Subnet
Name      Subnet          Broadcast      Gateway      Avail/      Ranges
-----
-----
sub1      192.0.2.0/24      bcast1        192.0.2.1    5/9        192.0.2.92-
192.0.2.100
sub3      198.51.100.0/24   bcast3        198.51.100.1 3/3
198.51.100.7,198.51.100.9
```

## Eliminare una subnet

Se non è più necessaria una subnet e si desidera disallocare gli indirizzi IP assegnati alla

subnet, è possibile eliminarla.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

### System Manager

**A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per eliminare una subnet**

#### Fasi

1. Selezionare **rete > Panoramica > subnet**.
2. Selezionare **⋮ > Elimina** accanto alla subnet che si desidera rimuovere.
3. Salvare le modifiche.

### CLI

#### Utilizzare la CLI per eliminare una subnet

##### A proposito di questa attività

Se un processore di servizio o un'interfaccia di rete sta attualmente utilizzando indirizzi IP compresi negli intervalli specificati, viene visualizzato un messaggio di errore. Se si desidera che le interfacce continuino a utilizzare gli indirizzi IP anche dopo l'eliminazione della subnet, è possibile impostare l'opzione `-force-update-lif-associations` su `true` per rimuovere l'associazione della subnet con i LIF.

#### Fase

Per eliminare una subnet:

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-force-update-lif-associations true]
```

Il seguente comando elimina la subnet sub1 in IPspace ipspace1:

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

## Creare SVM

È necessario creare una SVM per fornire i dati ai client.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario conoscere lo stile di sicurezza del volume root SVM.

Se si intende implementare una soluzione Hyper-V o SQL Server su SMB su questa SVM, è necessario utilizzare lo stile di protezione NTFS per il volume root. I volumi che contengono file Hyper-V o file di database SQL devono essere impostati sulla protezione NTFS al momento della creazione. Impostando lo stile di protezione del volume root su NTFS, si garantisce di non creare inavvertitamente volumi di dati UNIX o misti di tipo sicurezza.

- A partire da ONTAP 9.13.1, è possibile impostare una capacità massima per una VM di storage. È inoltre possibile configurare gli avvisi quando SVM si avvicina a un livello di capacità di soglia. Per ulteriori informazioni, vedere [Gestire la capacità SVM](#).

## System Manager

È possibile utilizzare System Manager per creare una VM di storage.

### Fasi

1. Selezionare **Storage VM**.
2. Fare clic su **+ Add** Per creare una VM di storage.
3. Assegnare un nome alla VM di storage.
4. Selezionare il protocollo di accesso:
  - SMB/CIFS, NFS
  - iSCSI
  - FC
  - NVMe
  - i. Se si seleziona **Enable SMB/CIFS** (attiva SMB/CIFS\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Nome amministratore	Specificare il nome utente dell'amministratore per la VM di storage SMB/CIFS.
Password	Specificare la password dell'amministratore per la VM di storage SMB/CIFS.
Nome server	Specificare il nome del server per la VM di storage SMB/CIFS.
Dominio Active Directory	Specificare il dominio Active Directory per fornire l'autenticazione dell'utente per la VM di storage SMB/CIFS.
Unità organizzativa	Specificare l'unità organizzativa all'interno del dominio Active Directory associato al server SMB/CIFS. "CN=Computers" è il valore predefinito che può essere modificato.
Crittografa i dati durante l'accesso alle condivisioni nella VM di storage	Selezionare questa casella di controllo per crittografare i dati utilizzando SMB 3.0 per impedire l'accesso non autorizzato ai file sulle condivisioni nella VM di storage SMB/CIFS.
Domini	Aggiungere, rimuovere o riordinare i domini elencati per la VM di storage SMB/CIFS.
Server dei nomi	Aggiungere, rimuovere o riordinare i server dei nomi per la VM di storage SMB/CIFS.

Lingua predefinita	Specifica l'impostazione di codifica della lingua predefinita per la VM di storage e i relativi volumi. Utilizzare la CLI per modificare le impostazioni dei singoli volumi all'interno di una VM di storage.
Interfaccia di rete	Per ogni interfaccia di rete configurata per la VM di storage, selezionare una subnet esistente (se ne esiste almeno una) o specificare <b>senza subnet</b> e completare i campi <b>Indirizzo IP</b> e <b>Subnet Mask</b> . Se utile, selezionare la casella di controllo <b>Usa la stessa subnet mask e lo stesso gateway per tutte le seguenti interfacce</b> . È possibile consentire al sistema di selezionare automaticamente la porta home oppure selezionare manualmente quella che si desidera utilizzare dall'elenco.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Se si seleziona **Enable NFS** (attiva NFS), completare la seguente configurazione:

O casella di controllo	Descrizione
Allow NFS client access (Consenti accesso client NFS)	Selezionare questa casella di controllo quando tutti i volumi creati sulla VM di storage NFS devono utilizzare il percorso del volume root "/" per il montaggio e il passaggio. Aggiungere regole al criterio di esportazione "predefinito" per consentire un mount traversal ininterrotto.

Regole	<p>Fare clic su <b>+ Add</b> per creare regole.</p> <ul style="list-style-type: none"> <li>• Client Specification (specifica client): Specificare i nomi host, gli indirizzi IP, i netgroup o i domini.</li> <li>• Access Protocols (protocolli di accesso): Selezionare una combinazione delle seguenti opzioni: <ul style="list-style-type: none"> <li>◦ SMB/CIFS</li> <li>◦ FlexCache</li> <li>◦ NFS <ul style="list-style-type: none"> <li>▪ NFSv3</li> <li>▪ NFSv4</li> </ul> </li> </ul> </li> <li>• Access Details (Dettagli di accesso): Per ciascun tipo di utente, specificare il livello di accesso, di sola lettura, di lettura/scrittura o di superutente. I tipi di utente includono: <ul style="list-style-type: none"> <li>◦ Tutto</li> <li>◦ Tutti (come utente anonimo)</li> <li>◦ UNIX</li> <li>◦ Kerberos 5</li> <li>◦ Kerberos 5i</li> <li>◦ Kerberos 5p</li> <li>◦ NTLM</li> </ul> </li> </ul> <p>Salvare la regola.</p>
Lingua predefinita	<p>Specifica l'impostazione di codifica della lingua predefinita per la VM di storage e i relativi volumi. Utilizzare la CLI per modificare le impostazioni dei singoli volumi all'interno di una VM di storage.</p>
Interfaccia di rete	<p>Per ogni interfaccia di rete configurata per la VM di storage, selezionare una subnet esistente (se ne esiste almeno una) o specificare <b>senza subnet</b> e completare i campi <b>Indirizzo IP</b> e <b>Subnet Mask</b>. Se utile, selezionare la casella di controllo <b>Usa la stessa subnet mask e lo stesso gateway per tutte le seguenti interfacce</b>. È possibile consentire al sistema di selezionare automaticamente la porta home oppure selezionare manualmente quella che si desidera utilizzare dall'elenco.</p>



Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.
----------------------------------	---

1. Se si seleziona **Enable iSCSI** (attiva iSCSI\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Interfaccia di rete	Per ogni interfaccia di rete configurata per la VM di storage, selezionare una subnet esistente (se ne esiste almeno una) o specificare <b>senza subnet</b> e completare i campi <b>Indirizzo IP</b> e <b>Subnet Mask</b> . Se utile, selezionare la casella di controllo <b>Usa la stessa subnet mask e lo stesso gateway per tutte le seguenti interfacce</b> . È possibile consentire al sistema di selezionare automaticamente la porta home oppure selezionare manualmente quella che si desidera utilizzare dall'elenco.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Se si seleziona **Enable FC** (attiva FC\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Configurare le porte FC	Selezionare le interfacce di rete sui nodi che si desidera includere nella VM di storage. Si consigliano due interfacce di rete per nodo.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Se si seleziona **Enable NVMe/FC** (attiva NVMe/FC\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Configurare le porte FC	Selezionare le interfacce di rete sui nodi che si desidera includere nella VM di storage. Si consigliano due interfacce di rete per nodo.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Se si seleziona **Enable NVMe/TCP** (attiva NVMe/TCP\*), completare la seguente configurazione:

O casella di controllo	Descrizione
Interfaccia di rete	Per ogni interfaccia di rete configurata per la VM di storage, selezionare una subnet esistente (se ne esiste almeno una) o specificare <b>senza subnet</b> e completare i campi <b>Indirizzo IP</b> e <b>Subnet Mask</b> . Se utile, selezionare la casella di controllo <b>Usa la stessa subnet mask e lo stesso gateway per tutte le seguenti interfacce</b> . È possibile consentire al sistema di selezionare automaticamente la porta home oppure selezionare manualmente quella che si desidera utilizzare dall'elenco.
Gestire l'account amministratore	Selezionare questa casella di controllo se si desidera gestire l'account di amministratore della VM di storage. Quando questa opzione è selezionata, specificare il nome utente, la password, confermare la password e indicare se si desidera aggiungere un'interfaccia di rete per la gestione delle macchine virtuali dello storage.

1. Salvare le modifiche.

## CLI

Utilizzare l'interfaccia utente di ONTAP per creare una subnet.

## Fasi

1. Determinare quali aggregati sono candidati per contenere il volume root SVM.

```
storage aggregate show -has-mroot false
```

È necessario scegliere un aggregato con almeno 1 GB di spazio libero per contenere il volume root. Se si intende configurare l'auditing NAS su SVM, è necessario disporre di almeno 3 GB di spazio libero aggiuntivo sull'aggregato root, con lo spazio extra utilizzato per creare il volume di staging di

auditing quando l'auditing è attivato.



Se il controllo NAS è già abilitato su una SVM esistente, il volume di staging dell'aggregato viene creato immediatamente dopo il completamento della creazione dell'aggregato.

2. Registrare il nome dell'aggregato su cui si desidera creare il volume root SVM.
3. Se si prevede di specificare una lingua quando si crea la SVM e non si conosce il valore da utilizzare, identificare e registrare il valore della lingua che si desidera specificare:

```
vserver create -language ?
```

4. Se si prevede di specificare una policy Snapshot quando si crea la SVM e non si conosce il nome della policy, elencare le policy disponibili e identificare e registrare il nome della policy Snapshot che si desidera utilizzare:

```
volume snapshot policy show -vserver vserver_name
```

5. Se si prevede di specificare un criterio di quota quando si crea la SVM e non si conosce il nome del criterio, elencare i criteri disponibili e identificare e registrare il nome del criterio di quota che si desidera utilizzare:

```
volume quota policy show -vserver vserver_name
```

## 6. Creare una SVM:

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume  
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace  
IPspace_name] [-language <language>] [-snapshot-policy  
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root  
-rootvolume-security-style ntfs -ipspace ipspace1 -language  
en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

## 7. Verificare che la configurazione SVM sia corretta.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

In questo esempio, il comando crea la SVM denominata "vs1" in IPspace "ipspace1". Il volume root è denominato "vs1\_root" e viene creato su aggr3 con lo stile di sicurezza NTFS.



A partire da ONTAP 9.13.1, è possibile impostare un modello di gruppo di policy QoS adattivo, applicando un limite di throughput e di soffitto ai volumi nella SVM. È possibile applicare questo criterio solo dopo aver creato la SVM. Per ulteriori informazioni su questo processo, vedere [Impostare un modello di gruppo di criteri adattativi](#).

## Interfacce logiche (LIF)

### Panoramica della LIF

#### Panoramica sulla configurazione delle LIF

Una LIF (interfaccia logica) rappresenta un punto di accesso di rete a un nodo del cluster. È possibile configurare le LIF sulle porte su cui il cluster invia e riceve le comunicazioni sulla rete.

Un amministratore del cluster può creare, visualizzare, modificare, migrare, ripristinare, Oppure eliminare i LIF. Un amministratore di SVM può visualizzare solo le LIF associate a SVM.

Un LIF è un indirizzo IP o WWPN con caratteristiche associate, ad esempio una policy di servizio, una porta home, un nodo home, un elenco di porte a cui eseguire il failover e una policy firewall. È possibile configurare le LIF sulle porte su cui il cluster invia e riceve le comunicazioni sulla rete.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

Le LIF possono essere ospitate sulle seguenti porte:

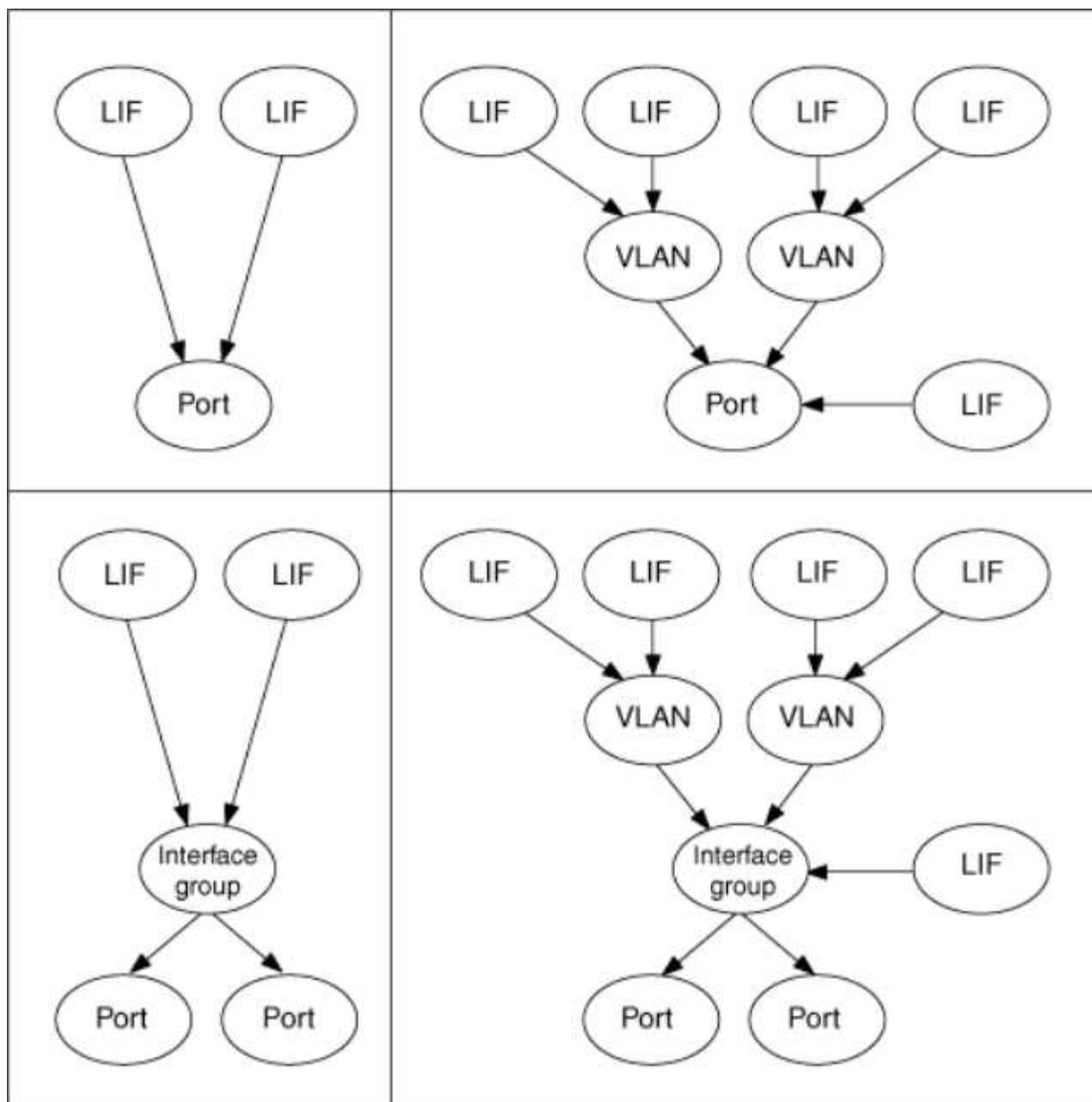
- Porte fisiche che non fanno parte di gruppi di interfacce
- Gruppi di interfacce
- VLAN
- Porte fisiche o gruppi di interfacce che ospitano VLAN
- Porte VIP (Virtual IP)

A partire da ONTAP 9.5, le LIF VIP sono supportate e sono ospitate su porte VIP.

Durante la configurazione di protocolli SAN come FC su un LIF, questo verrà associato a un WWPN.

["Amministrazione SAN"](#)

La seguente figura illustra la gerarchia di porte in un sistema ONTAP:



#### Failover e sconto della LIF

Un failover LIF si verifica quando una LIF passa dal nodo home o dalla porta al nodo partner ha o alla porta. Il failover di una LIF può essere attivato automaticamente da ONTAP o manualmente dall'amministratore del cluster per determinati eventi, come un collegamento Ethernet fisico inattivo o un nodo che abbandona il quorum del database replicato (RDB). Quando si verifica un failover della LIF, ONTAP continua a lavorare normalmente sul nodo partner fino alla risoluzione della causa del failover. Quando il nodo home o la porta torna in salute, la LIF viene riportata dal partner di ha al nodo home o alla porta. Questa inversione è chiamata sconto.

Per il failover e il giveback della LIF, le porte di ciascun nodo devono appartenere allo stesso dominio di broadcast. Per verificare che le porte rilevanti su ciascun nodo appartengano allo stesso dominio di broadcast, vedere quanto segue:

- ONTAP 9,8 e versioni successive: ["Riparare la raggiungibilità delle porte"](#)
- ONTAP 9.7 e versioni precedenti: ["Aggiungere o rimuovere porte da un dominio di broadcast"](#)

Per le LIF con failover LIF abilitato (automaticamente o manualmente) si applica quanto segue:

- Per le LIF che utilizzano una policy di servizio dati, puoi controllare le restrizioni delle policy di failover:
  - ONTAP 9,6 e versioni successive: ["LIF e policy di servizio in ONTAP 9.6 e versioni successive"](#)
  - ONTAP 9,5 e versioni precedenti: ["Ruoli LIF in ONTAP 9.5 e versioni precedenti"](#)
- L'autorevert dei LIF avviene quando l'autorevert è impostato su `true` E quando la porta home della LIF è in buone condizioni e in grado di ospitare la LIF.
- In un takeover pianificato o non pianificato del nodo, la LIF sul nodo preso in consegna, esegue il failover nel partner di ha. La porta su cui si verifica il failover di LIF è determinata da VIF Manager.
- Una volta completato il failover, la LIF funziona normalmente.
- Al momento di eseguire un giveback, la LIF torna al nodo home e alla porta, se l'opzione di indirizzamento automatico è impostata su `true`.
- Quando un collegamento ethernet si interrompe su una porta che ospita una o più LIF, VIF Manager esegue la migrazione delle LIF dalla porta inattiva a una porta diversa nello stesso dominio di trasmissione. La nuova porta potrebbe trovarsi nello stesso nodo o nel suo partner ha. Dopo il ripristino del collegamento e se l'opzione di ripristino automatico è impostata su `true`, Il VIF Manager riporta le LIF al loro nodo principale e alla loro porta principale.
- Quando un nodo abbandona il quorum del database replicato (RDB), il VIF Manager migra le LIF dal nodo fuori quorum al partner ha. Dopo che il nodo torna al quorum e se l'opzione di revert automatico è impostata su `true`, Il VIF Manager riporta le LIF al loro nodo principale e alla loro porta principale.

### Compatibilità LIF con i tipi di porta

Le LIF possono avere caratteristiche diverse per supportare diversi tipi di porta.



Quando le LIF di intercluster e di gestione sono configurate nella stessa subnet, il traffico di gestione potrebbe essere bloccato da un firewall esterno e le connessioni AutoSupport e NTP potrebbero non funzionare. È possibile ripristinare il sistema eseguendo `network interface modify -vserver vservice name -lif intercluster LIF -status-admin up|down` Comando per attivare/disattivare la LIF dell'intercluster. Tuttavia, è necessario impostare la LIF di intercluster e la LIF di gestione in diverse subnet per evitare questo problema.

LIF	Descrizione
LIF dati	LIF associata a una macchina virtuale di storage (SVM) e utilizzata per comunicare con i client. Su una porta è possibile disporre di più LIF di dati. Queste interfacce possono migrare o eseguire il failover in tutto il cluster. È possibile modificare una LIF dei dati per fungere da LIF di gestione SVM modificando la relativa policy firewall in mgmt. Le sessioni stabilite per i server NIS, LDAP, Active Directory, WINS e DNS utilizzano le LIF dei dati.

LIF del cluster	LIF utilizzata per trasportare il traffico intracluster tra i nodi di un cluster. Le LIF del cluster devono sempre essere create sulle porte del cluster. Le LIF del cluster possono eseguire il failover tra le porte del cluster sullo stesso nodo, ma non possono essere migrate o sottoposte a failover su un nodo remoto. Quando un nuovo nodo si unisce a un cluster, gli indirizzi IP vengono generati automaticamente. Tuttavia, se si desidera assegnare manualmente gli indirizzi IP alle LIF del cluster, è necessario assicurarsi che i nuovi indirizzi IP si trovino nello stesso intervallo di subnet delle LIF del cluster esistenti.
LIF gestione cluster	LIF che fornisce un'unica interfaccia di gestione per l'intero cluster. Una LIF di gestione del cluster può eseguire il failover su qualsiasi nodo del cluster. Non è possibile eseguire il failover sulle porte del cluster o dell'intercluster
LIF intercluster	Una LIF utilizzata per la comunicazione tra cluster, il backup e la replica. È necessario creare una LIF intercluster su ciascun nodo del cluster prima di stabilire una relazione di peering del cluster. Queste LIF possono eseguire il failover solo sulle porte dello stesso nodo. Non è possibile eseguire la migrazione o il failover su un altro nodo del cluster.
LIF di gestione dei nodi	LIF che fornisce un indirizzo IP dedicato per la gestione di un nodo specifico in un cluster. Le LIF di gestione dei nodi vengono create al momento della creazione o dell'adesione al cluster. Queste LIF vengono utilizzate per la manutenzione del sistema, ad esempio quando un nodo diventa inaccessibile dal cluster.
LIF. VIP	Per LIF VIP si intende qualsiasi LIF di dati creata su una porta VIP. Per ulteriori informazioni, vedere <a href="#">"Configurare i LIF VIP (Virtual IP)"</a> .

### LIF e policy di servizio (ONTAP 9,6 e versioni successive)

È possibile assegnare policy di servizio (invece di ruoli LIF o policy firewall) alle LIF che determinano il tipo di traffico supportato per le LIF. Le policy di servizio definiscono una raccolta di servizi di rete supportati da una LIF. ONTAP offre una serie di policy di servizio integrate che possono essere associate a una LIF.

È possibile visualizzare le policy di servizio e i relativi dettagli utilizzando il seguente comando:

```
network interface service-policy show
```

Le funzioni non associate a un servizio specifico utilizzeranno un comportamento definito dal sistema per selezionare le LIF per le connessioni in uscita.

### Policy di servizio per SVM di sistema

La SVM amministrativa e qualsiasi SVM di sistema contengono policy di servizio che possono essere utilizzate per le LIF in tale SVM, incluse le LIF di gestione e intercluster. Questi criteri vengono creati automaticamente dal sistema quando viene creato un IPspace.

Nella tabella seguente sono elencati i criteri integrati per i LIF nelle SVM di sistema a partire da ONTAP 9.12.1. Per le altre release, visualizzare le policy di servizio e i relativi dettagli utilizzando il seguente comando:

```
network interface service-policy show
```

Policy	Servizi inclusi	Ruolo equivalente	Descrizione
--------	-----------------	-------------------	-------------



intercluster predefinito	intercluster-core, management-https	intercluster	Utilizzato da LIF che trasportano traffico intercluster. Nota: Service Intercluster-core è disponibile da ONTAP 9.5 con il nome net-intercluster service policy.
default-route-announce	gestione-bgp	-	Utilizzato da LIF con connessioni peer BGP. Nota: Disponibile da ONTAP 9.5 con il nome net-route-announce service policy.
gestione predefinita	management-core, management-https, management-http, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client, management-ntp-client, management-log-forwarding	node-mgmt, o cluster-mgmt	Utilizzare questa policy di gestione con ambito di sistema per creare LIF di gestione con ambito di nodo e cluster di proprietà di una SVM di sistema. Queste LIF possono essere utilizzate per le connessioni in uscita verso server DNS, ad, LDAP o NIS, nonché per alcune connessioni aggiuntive per supportare le applicazioni eseguite per conto dell'intero sistema. A partire da ONTAP 9.12.1, è possibile utilizzare <code>management-log-forwarding</code> Servizio per controllare quali LIF vengono utilizzati per inoltrare i registri di audit a un server syslog remoto.

La seguente tabella elenca i servizi che i file LIF possono utilizzare su un SVM di sistema a partire da ONTAP 9.11.1:

Servizio	Limiti di failover	Descrizione
core intercluster	solo nodo principale	Servizi di intercluster principali
core di gestione	-	Servizi di gestione principali
gestione-ssh	-	Servizi per l'accesso alla gestione SSH
gestione-http	-	Servizi per l'accesso alla gestione HTTP
gestione-https	-	Servizi per l'accesso alla gestione HTTPS
gestione: autosupport	-	Servizi relativi alla pubblicazione dei payload AutoSupport
gestione-bgp	solo porta home	Servizi correlati alle interazioni peer BGP
backup-ndmp-control	-	Servizi per i controlli di backup NDMP

gestione-ems	-	Servizi per l'accesso alla messaggistica di gestione
client ntp di gestione	-	Introdotta in ONTAP 9.10.1. Servizi per l'accesso al client NTP.
management-ntp-server	-	Introdotta in ONTAP 9.11.1. Servizi per l'accesso alla gestione del server NTP
gestione-portmap	-	Servizi per la gestione di portmap
management-rsh-server	-	Servizi per la gestione dei server rsh
server-snmp-di-gestione	-	Servizi per la gestione del server SNMP
management-telnet-server	-	Servizi per la gestione dei server telnet
management-log-forwarding	-	Introdotta in ONTAP 9.12.1. Servizi per l'inoltro dei log di controllo

#### Policy di servizio per SVM di dati

Tutti i dati SVM contengono policy di servizio che possono essere utilizzate dai LIF in tale SVM.

Nella tabella seguente sono elencati i criteri integrati per le LIF nelle SVM di dati a partire da ONTAP 9.11.1. Per le altre release, visualizzare le policy di servizio e i relativi dettagli utilizzando il seguente comando:

```
network interface service-policy show
```

Policy	Servizi inclusi	Protocollo dati equivalente	Descrizione
gestione predefinita	management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nessuno	Utilizza questa policy di gestione con ambito SVM per creare LIF di gestione SVM di proprietà di una SVM di dati. Queste LIF possono essere utilizzate per fornire l'accesso SSH o HTTPS agli amministratori di SVM. Se necessario, questi LIF possono essere utilizzati per le connessioni in uscita a server DNS, ad, LDAP o NIS esterni.
blocchi-di-dati-predefiniti	data-core, data-iscsi	iscsi	Utilizzato da LIF che trasportano traffico dati SAN orientato a blocchi. A partire da ONTAP 9.10.1, la policy "default-data-block" è obsoleta. Utilizzare invece la policy di servizio "default-data-iscsi".

default-data-files	data-fpolicy-client, data-dns-server, data-flexcache, data-cifs, data-nfs, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	nfs, cifs, fcache	Utilizzare il criterio default-data-files per creare LIF NAS che supportino protocolli di dati basati su file. A volte è presente un solo LIF nella SVM, pertanto questo criterio consente di utilizzare la LIF per le connessioni in uscita a un server DNS, ad, LDAP o NIS esterno. È possibile rimuovere questi servizi da questa policy se si preferisce che queste connessioni utilizzino solo LIF di gestione.
default-data-iscsi	data-core, data-iscsi	iscsi	Utilizzato da LIF che trasportano traffico dati iSCSI.
default-data-nvme-tcp	data-core, data-nvme-tcp	nvme-tcp	Utilizzato da LIF che trasportano traffico dati NVMe/TCP.

La tabella seguente elenca i servizi che possono essere utilizzati su una SVM di dati insieme alle eventuali restrizioni imposte da ciascun servizio alla policy di failover di una LIF a partire da ONTAP 9.11.1:

Servizio	Restrizioni di failover	Descrizione
gestione-ssh	-	Servizi per l'accesso alla gestione SSH
gestione-http	-	Introdotta nei servizi ONTAP 9.10.1 per l'accesso alla gestione HTTP
gestione-https	-	Servizi per l'accesso alla gestione HTTPS
gestione-portmap	-	Servizi per l'accesso alla gestione di portmap
server-snmp-di-gestione	-	Introdotta nei servizi ONTAP 9.10.1 per l'accesso alla gestione del server SNMP
core di dati	-	Servizi dati principali
nfs dati	-	Servizio dati NFS
cifs dei dati	-	Servizio dati CIFS
data-flexcache	-	Servizio dati FlexCache
iscsi dati	solo porta home	Servizio dati iSCSI
backup-ndmp-control	-	Introdotta in ONTAP 9.10.1 Backup NDMP controlla il servizio dati

server-dns-dati	-	Introdotta nel servizio dati del server DNS di ONTAP 9.10.1
data-fpolicy-client	-	Servizio dati delle policy di screening dei file
data-nvme-tcp	solo porta home	Introdotta nel servizio dati TCP NVMe di ONTAP 9.10.1
data-s3-server	-	Servizio dati server Simple Storage Service (S3)

È necessario conoscere il modo in cui le policy di servizio vengono assegnate alle LIF nelle SVM di dati:

- Se viene creata una SVM dati con un elenco di servizi dati, le policy di servizio "default-data-files" e "default-data-block" incorporate in tale SVM vengono create utilizzando i servizi specificati.
- Se viene creata una SVM dati senza specificare un elenco di servizi dati, le policy di servizio "default-data-files" e "default-data-block" incorporate in tale SVM vengono create utilizzando un elenco predefinito di servizi dati.

L'elenco dei servizi dati predefiniti include i servizi iSCSI, NFS, NVMe, SMB e FlexCache.

- Quando si crea una LIF con un elenco di protocolli dati, una politica di servizio equivalente ai protocolli dati specificati viene assegnata alla LIF.
- Se non esiste una politica di servizio equivalente, viene creata una politica di servizio personalizzata.
- Quando si crea una LIF senza una policy di servizio o un elenco di protocolli dati, la policy di servizio default-data-files viene assegnata alla LIF per impostazione predefinita.

### Servizio data-core

Il servizio data-core consente ai componenti che in precedenza utilizzavano le LIF con il ruolo dati di funzionare come previsto sui cluster che sono stati aggiornati per gestire le LIF utilizzando le policy di servizio invece dei ruoli LIF (che sono deprecati in ONTAP 9.6).

La specifica del data-core come servizio non apre alcuna porta nel firewall, ma il servizio deve essere incluso in qualsiasi politica di servizio in una SVM dati. Ad esempio, per impostazione predefinita, la politica di servizio file di dati predefiniti contiene i seguenti servizi:

- core di dati
- nfs dati
- cifs dei dati
- data-flexcache

Il servizio data-core deve essere incluso nella policy per garantire che tutte le applicazioni che utilizzano LIF funzionino come previsto, ma gli altri tre servizi possono essere rimossi, se lo si desidera.

### Servizio LIF lato client

A partire da ONTAP 9.10.1, ONTAP offre servizi LIF lato client per più applicazioni. Questi servizi consentono di controllare quali LIF vengono utilizzati per le connessioni in uscita per conto di ciascuna applicazione.

I seguenti nuovi servizi consentono agli amministratori di controllare quali LIF vengono utilizzati come indirizzi

di origine per determinate applicazioni.

Servizio	Restrizioni SVM	Descrizione
management-ad-client	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client Active Directory per le connessioni in uscita a un server ad esterno.
client-dns-di-gestione	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client DNS per le connessioni in uscita a un server DNS esterno.
management-ldap-client	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client LDAP per le connessioni in uscita a un server LDAP esterno.
management-nis-client	-	A partire da ONTAP 9.11.1, ONTAP fornisce il servizio client NIS per le connessioni in uscita a un server NIS esterno.
client ntp di gestione	solo sistema	A partire da ONTAP 9.10.1, ONTAP fornisce il servizio client NTP per le connessioni in uscita a un server NTP esterno.
data-fpolicy-client	solo dati	A partire da ONTAP 9.8, ONTAP fornisce il servizio client per le connessioni FPolicy in uscita.

Ciascuno dei nuovi servizi viene incluso automaticamente in alcune policy di servizio integrate, ma gli amministratori possono rimuoverli dalle policy integrate o aggiungerli a policy personalizzate per controllare quali LIF vengono utilizzate per le connessioni in uscita per conto di ciascuna applicazione.

### **Ruoli LIF (ONTAP 9,5 e versioni precedenti)**

Le LIF con ruoli diversi hanno caratteristiche diverse. Un ruolo LIF determina il tipo di traffico supportato dall'interfaccia, insieme alle regole di failover applicabili, alle restrizioni firewall in vigore, alla sicurezza, al bilanciamento del carico e al comportamento di routing per ogni LIF. Una LIF può avere uno dei seguenti ruoli: Cluster, gestione del cluster, dati, intercluster, gestione dei nodi, e undef (non definito). Il ruolo undef viene utilizzato per i LIF BGP.

A partire da ONTAP 9.6, i ruoli LIF sono deprecati. È necessario specificare le policy di servizio per le LIF anziché un ruolo. Non è necessario specificare un ruolo LIF quando si crea una LIF con una politica di servizio.

### **Sicurezza LIF**

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster

Richiedere una subnet IP privata?	No	Sì	No	No	No
Hai bisogno di una rete sicura?	No	Sì	No	No	Sì
Policy firewall predefinita	Molto restrittivo	Aprire completamente	Medio	Medio	Molto restrittivo
Il firewall è personalizzabile?	Sì	No	Sì	Sì	Sì

#### Failover LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster
Comportamento predefinito	Solo le porte dello stesso gruppo di failover che si trovano sul nodo principale della LIF e su un nodo partner non SFO	Solo le porte dello stesso gruppo di failover che si trovano sul nodo principale della LIF	Solo le porte dello stesso gruppo di failover che si trovano sul nodo principale della LIF	Qualsiasi porta dello stesso gruppo di failover	Solo le porte dello stesso gruppo di failover che si trovano sul nodo principale della LIF
È personalizzabile?	Sì	No	Sì	Sì	Sì

#### Routing LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster
Quando è necessario un percorso predefinito?	Quando i client o i controller di dominio si trovano su una subnet IP diversa	Mai	Quando uno dei tipi di traffico primari richiede l'accesso a una subnet IP diversa	Quando l'amministratore si connette da un'altra subnet IP	Quando altre LIF intercluster si trovano su una subnet IP diversa
Quando è necessario un instradamento statico a una specifica subnet IP?	Raro	Mai	Raro	Raro	Quando i nodi di un altro cluster hanno le proprie LIF di intercluster in sottoreti IP diverse

Quando è necessario un percorso host statico verso un server specifico?	Per fare in modo che uno dei tipi di traffico sia elencato nella LIF di gestione dei nodi, eseguire una LIF di dati piuttosto che una LIF di gestione dei nodi. Ciò richiede una modifica del firewall corrispondente.	Mai	Raro	Raro	Raro
---	--	-----	------	------	------

#### Ribilanciamento LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster
DNS: Utilizzare come server DNS?	Sì	No	No	No	No
DNS: Esportare come zona?	Sì	No	No	No	No

#### Tipi di traffico primari LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF gestione cluster	LIF intercluster
Tipi di traffico primari	Server NFS, server CIFS, client NIS, Active Directory, LDAP, WINS, client e server DNS, iSCSI e server FC	Intracluster	Server SSH, server HTTPS, client NTP, SNMP, client AutoSupport, Client DNS, caricamento aggiornamenti software	Server SSH, server HTTPS	Replica tra cluster

## Gestire le LIF

### Configurare le policy di servizio LIF

È possibile configurare le policy di servizio LIF per identificare un singolo servizio o un elenco di servizi che utilizzeranno una LIF.

#### Creare una politica di servizio per le LIF

È possibile creare una politica di servizio per le LIF. È possibile assegnare una policy di servizio a una o più

LIF, consentendo così al LIF di trasportare il traffico per un singolo servizio o un elenco di servizi.

Per eseguire, sono necessari privilegi avanzati `network interface service-policy create` comando.

### A proposito di questa attività

I servizi integrati e le policy di servizio sono disponibili per la gestione del traffico di dati e di gestione su SVM di dati e di sistema. La maggior parte dei casi di utilizzo è soddisfatta utilizzando una politica di servizio integrata piuttosto che creare una politica di servizio personalizzata.

Se necessario, è possibile modificare queste policy di servizio incorporate.

### Fasi

1. Visualizzare i servizi disponibili nel cluster:

```
network interface service show
```

I servizi rappresentano le applicazioni a cui si accede da una LIF e le applicazioni servite dal cluster. Ogni servizio include zero o più porte TCP e UDP su cui l'applicazione è in ascolto.

Sono disponibili i seguenti servizi di gestione e dati aggiuntivi:

```
cluster1::> network interface service show

Service                                Protocol:Ports
-----                                -
cluster-core                           -
data-cifs                              -
data-core                              -
data-flexcache                         -
data-iscsi                             -
data-nfs                               -
intercluster-core                      tcp:11104-11105
management-autosupport                 -
management-bgp                        tcp:179
management-core                        -
management-https                      tcp:443
management-ssh                        tcp:22
12 entries were displayed.
```

2. Visualizzare le policy di servizio esistenti nel cluster:



```
cluster1::> network interface service-policy show
```

Vserver	Policy	Service: Allowed Addresses
-----		
-----		
cluster1		
	default-intercluster	intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-management	management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-route-announce	management-bgp: 0.0.0.0/0
Cluster		
	default-cluster	cluster-core: 0.0.0.0/0
vs0		
	default-data-blocks	data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0
	default-data-files	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0
	default-management	data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0

```
7 entries were displayed.
```

### 3. Creare una politica di servizio:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by technical support.
```

```
Do you wish to continue? (y or n): y
```

```
cluster1::> network interface service-policy create -vserver <svm_name>  
-policy <service_policy_name> -services <service_name> -allowed  
-addresses <IP_address/mask,...>
```

- "nome\_servizio" specifica un elenco di servizi da includere nella policy.
- "IP\_address/mask" specifica l'elenco di subnet mask per gli indirizzi ai quali è consentito l'accesso ai servizi nella politica di servizio. Per impostazione predefinita, tutti i servizi specificati vengono aggiunti con un elenco di indirizzi consentiti predefinito di 0.0.0.0/0, che consente il traffico da tutte le subnet. Quando viene fornito un elenco di indirizzi non predefinito, i file LIF che utilizzano il criterio sono configurati per bloccare tutte le richieste con un indirizzo di origine che non corrisponde a nessuna delle maschere specificate.

Nell'esempio seguente viene illustrato come creare una policy del servizio dati, *svm1\_data\_policy*, per una SVM che include i servizi *NFS* e *SMB*:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

Nell'esempio seguente viene illustrato come creare una policy di servizio tra cluster:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

#### 4. Verificare che la politica di servizio sia stata creata.

```
cluster1::> network interface service-policy show
```

Il seguente output mostra le policy di servizio disponibili:

```
cluster1::> network interface service-policy show
```

Vserver	Policy	Service: Allowed Addresses
-----		
-----		
cluster1		
	default-intercluster	intercluster-core: 0.0.0.0/0 management-https: 0.0.0.0/0
	intercluster1	intercluster-core: 0.0.0.0/0
	default-management	management-core: 0.0.0.0/0 management-autosupport: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	default-route-announce	management-bgp: 0.0.0.0/0
Cluster		
	default-cluster	cluster-core: 0.0.0.0/0
vs0		
	default-data-blocks	data-core: 0.0.0.0/0 data-iscsi: 0.0.0.0/0
	default-data-files	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0 data-flexcache: 0.0.0.0/0
	default-management	data-core: 0.0.0.0/0 management-ssh: 0.0.0.0/0 management-https: 0.0.0.0/0
	svm1_data_policy	data-core: 0.0.0.0/0 data-nfs: 0.0.0.0/0 data-cifs: 0.0.0.0/0

```
9 entries were displayed.
```

### Al termine

Assegnare la politica di servizio a una LIF al momento della creazione o modificando una LIF esistente.

## Assegnare una politica di servizio a una LIF

È possibile assegnare una politica di servizio a una LIF al momento della creazione della LIF o modificando la LIF. Una politica di servizio definisce l'elenco dei servizi che possono essere utilizzati con LIF.

### A proposito di questa attività

È possibile assegnare le policy di servizio per le LIF nelle SVM di amministrazione e dati.

### Fase

A seconda del momento in cui si desidera assegnare la politica di servizio a una LIF, eseguire una delle seguenti operazioni:

Se sei...	Assegnare la politica di servizio...
Creazione di una LIF	Interfaccia di rete create -vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> {(-address <IP_address> -netmask <IP_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
Modifica di una LIF	modifica interfaccia di rete -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

Quando si specifica una politica di servizio per una LIF, non è necessario specificare il protocollo dati e il ruolo per la LIF. È supportata anche la creazione di LIF specificando il ruolo e i protocolli dati.



Una politica di servizio può essere utilizzata solo dalle LIF nella stessa SVM specificata durante la creazione della politica di servizio.

### Esempi

Nell'esempio seguente viene illustrato come modificare la politica di servizio di una LIF per utilizzare la politica di servizio di gestione predefinita:

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service  
-policy default-management
```

### Comandi per la gestione delle policy di servizio LIF

Utilizzare `network interface service-policy` Comandi per gestire le policy di servizio LIF.

### Prima di iniziare

La modifica della policy di servizio di una LIF in una relazione di SnapMirror attiva interrompe il programma di replica. Se si converte una LIF da intercluster a non intercluster (o viceversa), le modifiche non verranno replicate nel cluster sottoposto a peering. Per aggiornare il cluster peer dopo aver modificato la policy di servizio LIF, eseguire prima l' `snapmirror abort` operazione quindi [risincronizzazione della relazione di replica](#).

Se si desidera...	Utilizzare questo comando...
Creazione di una politica di servizio (sono richiesti privilegi avanzati)	<code>network interface service-policy create</code>

Se si desidera...	Utilizzare questo comando...
Aggiunta di una voce di servizio aggiuntiva a una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy add-service</code>
Clonare una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy clone</code>
Modifica di una voce di servizio in una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy modify-service</code>
Rimozione di una voce di servizio da una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy remove-service</code>
Rinominare una policy di servizio esistente (sono richiesti privilegi avanzati)	<code>network interface service-policy rename</code>
Eliminazione di una policy di servizio esistente (privilegi avanzati richiesti)	<code>network interface service-policy delete</code>
Ripristinare una policy di servizio integrata al suo stato originale (sono richiesti privilegi avanzati)	<code>network interface service-policy restore-defaults</code>
Visualizzare le policy di servizio esistenti	<code>network interface service-policy show</code>

### Creazione di una LIF (interfaccia di rete)

Una SVM fornisce i dati ai client attraverso una o più interfacce logiche di rete (LIF). Per accedere ai dati, è necessario creare LIF sulle porte che si desidera utilizzare. Una LIF (interfaccia di rete) è un indirizzo IP associato a una porta fisica o logica. In caso di guasto di un componente, una LIF può eseguire il failover o essere migrata su una porta fisica diversa, continuando così a comunicare con la rete.

#### Best practice

Le porte dello switch connesse a ONTAP devono essere configurate come porte edge spanning-tree per ridurre i ritardi durante la migrazione LIF.

#### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- La porta di rete fisica o logica sottostante deve essere stata configurata con lo stato di attivazione amministrativa.
- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando System Manager o `network subnet create` comando.

- Il meccanismo per specificare il tipo di traffico gestito da una LIF è stato modificato. Per ONTAP 9.5 e versioni precedenti, i LIF utilizzavano i ruoli per specificare il tipo di traffico che gestirebbe. A partire da ONTAP 9.6, le LIF utilizzano le policy di servizio per specificare il tipo di traffico che gestirebbe.

### A proposito di questa attività

- Non è possibile assegnare protocolli NAS e SAN allo stesso LIF.

I protocolli supportati sono SMB, NFS, FlexCache, iSCSI e FC; iSCSI e FC non possono essere combinati con altri protocolli. Tuttavia, i protocolli SAN basati su NAS ed Ethernet possono essere presenti sulla stessa porta fisica.

- Non si consiglia di configurare le LIF che trasportano il traffico SMB in modo da ripristinare automaticamente i propri nodi domestici. Questo suggerimento è obbligatorio se il server SMB deve ospitare una soluzione per operazioni senza interruzioni con Hyper-V o SQL Server su SMB.
- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Tutti i servizi di mappatura dei nomi e risoluzione dei nomi host utilizzati da una SVM, come DNS, NIS, LDAP e Active Directory, Deve essere raggiungibile da almeno un LIF che gestisce il traffico dati della SVM.
- Una LIF che gestisce il traffico intracluster tra i nodi non deve trovarsi sulla stessa subnet di una LIF che gestisce il traffico di gestione o di una LIF che gestisce il traffico di dati.
- La creazione di una LIF che non dispone di una destinazione di failover valida genera un messaggio di avviso.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster:
  - System Manager: A partire da ONTAP 9.12.0, visualizzare il throughput nella griglia dell'interfaccia di rete.
  - CLI: Utilizzare `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).
- A partire da ONTAP 9.7, se sono già presenti altre LIF per la SVM nella stessa sottorete, non è necessario specificare la porta home della LIF. ONTAP sceglie automaticamente una porta casuale sul nodo principale specificato nello stesso dominio di trasmissione delle altre LIF già configurate nella stessa sottorete.

A partire da ONTAP 9.4, FC-NVMe è supportato. Se si sta creando una LIF FC-NVMe, tenere presente quanto segue:

- Il protocollo NVMe deve essere supportato dall'adattatore FC su cui viene creato il LIF.
- FC-NVMe può essere l'unico protocollo dati sulle LIF dei dati.
- È necessario configurare un LIF che gestisca il traffico di gestione per ogni macchina virtuale di storage (SVM) che supporti LA SAN.
- Le LIF e gli spazi dei nomi NVMe devono essere ospitati sullo stesso nodo.
- È possibile configurare un solo NVMe LIF che gestisce il traffico dati per SVM.
- Quando si crea un'interfaccia di rete con una subnet, ONTAP seleziona automaticamente un indirizzo IP disponibile dalla subnet selezionata e lo assegna all'interfaccia di rete. È possibile modificare la subnet se sono presenti più subnet, ma non è possibile modificare l'indirizzo IP.
- Quando si crea (aggiunge) una SVM per un'interfaccia di rete, non è possibile specificare un indirizzo IP compreso nell'intervallo di una subnet esistente. Viene visualizzato un errore di conflitto di subnet. Questo problema si verifica in altri flussi di lavoro per un'interfaccia di rete, come la creazione o la modifica di interfacce di rete tra cluster nelle impostazioni SVM o nelle impostazioni del cluster.

- A partire da ONTAP 9.10.1, la `network interface` I comandi CLI includono un `-rdma-protocols` Parametro per configurazioni NFS su RDMA. La creazione di interfacce di rete per configurazioni NFS su RDMA è supportata in Gestione sistemi a partire da ONTAP 9.12.1. Per ulteriori informazioni, vedere [Configurare LIFS per NFS su RDMA](#).
- A partire da ONTAP 9.11.1, il failover automatico iSCSI LIF è disponibile nelle piattaforme ASA (All-Flash SAN Array).

Il failover LIF iSCSI viene attivato automaticamente (il criterio di failover è impostato su `sfo-partner-only` e il valore di autorevert è impostato su `true`) Sulle LIF iSCSI appena create se non esistono LIF iSCSI nella SVM specificata o se tutte le LIF iSCSI esistenti nella SVM specificata sono già abilitate con il failover LIF iSCSI.

Se dopo aver eseguito l'aggiornamento a ONTAP 9.11.1 o versioni successive si dispone di LIF iSCSI esistenti in una SVM che non sono state abilitate con la funzione di failover LIF iSCSI e si creano nuove LIF iSCSI nella stessa SVM, le nuove LIF iSCSI assumono la stessa policy di failover (`disabled`) Delle LIF iSCSI esistenti in SVM.

#### ["Failover LIF iSCSI per piattaforme ASA"](#)

A partire da ONTAP 9.7, ONTAP sceglie automaticamente la porta home di un LIF, purché almeno un LIF esista già nella stessa sottorete di tale LIF. ONTAP sceglie una porta home nello stesso dominio di broadcast delle altre LIF della subnet. È comunque possibile specificare una porta home, ma non è più necessaria (a meno che non esistano file LIF in tale subnet nell'IPSpace specificato).

A partire da ONTAP 9.12.0, la procedura da seguire dipende dall'interfaccia in uso: Gestore di sistema o CLI:

## System Manager

### Utilizzare System Manager per aggiungere un'interfaccia di rete

#### Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare **+ Add**.
3. Selezionare uno dei seguenti ruoli di interfaccia:
  - a. Dati
  - b. Intercluster
  - c. Gestione SVM
4. Selezionare il protocollo:
  - a. SMB/CIFS E NFS
  - b. ISCSI
  - c. FC
  - d. NVMe/FC
  - e. NVMe/TCP
5. Assegnare un nome al LIF o accettare il nome generato dalle selezioni precedenti.
6. Accettare il nodo home o utilizzare il menu a discesa per selezionarlo.
7. Se almeno una subnet è configurata nell'IPSpace dell'SVM selezionato, viene visualizzato il menu a discesa Subnet (sottorete).
  - a. Se si seleziona una subnet, selezionarla dall'elenco a discesa.
  - b. Se si procede senza una subnet, viene visualizzato il menu a discesa del dominio di trasmissione:
    - i. Specificare l'indirizzo IP. Se l'indirizzo IP è in uso, viene visualizzato un messaggio di avviso.
    - ii. Specificare una subnet mask.
8. Selezionare la porta home dal dominio di trasmissione, automaticamente (scelta consigliata) o selezionandola dal menu a discesa. Il controllo della porta Home viene visualizzato in base al dominio di trasmissione o alla selezione della subnet.
9. Salvare l'interfaccia di rete.

#### CLI

### Utilizzare la CLI per creare una LIF

#### Fasi

1. Determinare quali porte del dominio di trasmissione si desidera utilizzare per la LIF.

```
network port broadcast-domain show -ipspace ipspace1
```



IPspace Name	Broadcast Domain name	MTU	Port List	Update Status	Details
ipspace1	default	1500	node1:e0d node1:e0e node2:e0d node2:e0e	complete complete complete complete	

2. Verificare che la subnet che si desidera utilizzare per i file LIF contenga un numero sufficiente di indirizzi IP inutilizzati.

```
network subnet show -ipspace ipspace1
```

3. Creare una o più LIF sulle porte che si desidera utilizzare per accedere ai dati.

```
network interface create -vserver _SVM_name_ -lif _lif_name_  
-service-policy _service_policy_name_ -home-node _node_name_ -home  
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |  
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert  
{true|false}
```

- -home-node È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

Puoi anche specificare se LIF deve ripristinare automaticamente il nodo home e la porta home con l'opzione -auto-revert.

- -home-port È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
- È possibile specificare un indirizzo IP con -address e. -netmask oppure attivare l'allocazione da una subnet con -subnet\_name opzione.
- Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene automaticamente aggiunto un percorso predefinito a tale gateway.
- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- -auto-revert Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `true` in base alle policy di gestione della rete nel proprio ambiente.
- -service-policy A partire da ONTAP 9.5, è possibile assegnare una politica di servizio per la LIF con -service-policy opzione. Quando viene specificata una policy di servizio per una LIF, questa viene utilizzata per creare un ruolo predefinito, una policy di failover e un elenco di

protocolli dati per la LIF. In ONTAP 9.5, le policy di servizio sono supportate solo per i servizi peer di intercluster e BGP. In ONTAP 9.6, è possibile creare policy di servizio per diversi servizi di gestione e dati.

- ° `-data-protocol` Consente di creare una LIF che supporti i protocolli FCP o NVMe/FC. Questa opzione non è necessaria quando si crea un LIF IP.

#### 4. **Opzionale:** Assegnare un indirizzo IPv6 nell'opzione `-address`:

- Utilizzare il comando `network ndp prefix show` per visualizzare l'elenco dei prefissi RA appresi sulle varie interfacce.

Il comando `network ndp prefix show` è disponibile a livello di privilegio avanzato.

- Utilizzare il formato `prefix::id` Per costruire manualmente l'indirizzo IPv6.

`prefix` è il prefisso appreso sulle varie interfacce.

Per derivare il `id`, scegliere un numero esadecimale casuale a 64 bit.

#### 5. Verificare che la configurazione dell'interfaccia LIF sia corretta.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
vs1	lif1	up/up	10.0.0.128/24	node1	e0d
true					

#### 6. Verificare che la configurazione del gruppo di failover sia quella desiderata.

```
network interface show -failover -vserver vs1
```

Vserver	Logical interface	Home Node:Port	Failover Policy	Failover Group
vs1	lif1	node1:e0d	system-defined	ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e				

#### 7. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	ping di rete

## Esempi

Il seguente comando crea una LIF e specifica i valori dell'indirizzo IP e della maschera di rete utilizzando `-address` e `-netmask` parametri:

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

Il seguente comando crea una LIF e assegna i valori dell'indirizzo IP e della maschera di rete dalla subnet specificata (denominata `client1_sub`):

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

Il seguente comando crea una LIF NVMe/FC e specifica `nvme-fc` protocollo dati:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

## Modificare una LIF

È possibile modificare una LIF modificando gli attributi, ad esempio il nodo principale o il nodo corrente, lo stato amministrativo, l'indirizzo IP, la netmask, la policy di failover, policy firewall e policy di servizio. È inoltre possibile modificare la famiglia di indirizzi di una LIF da IPv4 a IPv6.

### A proposito di questa attività

- Quando si modifica lo stato amministrativo di una LIF su inattivo, i blocchi NFSv4 in sospeso vengono mantenuti fino a quando lo stato amministrativo della LIF non viene riportato su UP.

Per evitare conflitti di blocco che possono verificarsi quando altri LIF tentano di accedere ai file bloccati, è necessario spostare i client NFSv4 su un LIF diverso prima di impostare lo stato amministrativo su inattivo.

- Non è possibile modificare i protocolli dati utilizzati da un FC LIF. Tuttavia, è possibile modificare i servizi assegnati a una politica di servizio o la politica di servizio assegnata a una LIF IP.

Per modificare i protocolli dati utilizzati da un LIF FC, è necessario eliminare e ricreare il LIF. Per apportare modifiche alla politica di servizio di un LIF IP, si verifica una breve interruzione durante l'esecuzione degli aggiornamenti.

- Non è possibile modificare il nodo principale o il nodo corrente di una LIF di gestione con ambito di nodo.

- Quando si utilizza una subnet per modificare l'indirizzo IP e il valore della maschera di rete per una LIF, viene assegnato un indirizzo IP dalla subnet specificata; se l'indirizzo IP precedente della LIF proviene da una subnet diversa, l'indirizzo IP viene restituito a tale subnet.
- Per modificare la famiglia di indirizzi di una LIF da IPv4 a IPv6, è necessario utilizzare la notazione con i due punti per l'indirizzo IPv6 e aggiungere un nuovo valore per `-netmask-length` parametro.
- Non è possibile modificare gli indirizzi IPv6 link-local configurati automaticamente.
- La modifica di una LIF che non ha una destinazione di failover valida per la LIF genera un messaggio di avviso.

Se un LIF che non dispone di una destinazione di failover valida tenta di eseguire il failover, potrebbe verificarsi un'interruzione.

- A partire da ONTAP 9.5, è possibile modificare la politica di servizio associata a una LIF.

In ONTAP 9.5, le policy di servizio sono supportate solo per i servizi peer di intercluster e BGP. In ONTAP 9.6, è possibile creare policy di servizio per diversi servizi di gestione e dati.

- A partire da ONTAP 9.11.1, il failover automatico di LIF iSCSI è disponibile sulle piattaforme ASA (All-Flash SAN Array).


Per le LIF iSCSI pre-esistenti, ovvero le LIF create prima dell'upgrade alla versione 9.11.1 o successiva, è possibile modificare il criterio di failover in ["Attiva il failover automatico della LIF iSCSI"](#).

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

A partire da ONTAP 9.12.0, è possibile utilizzare Gestione sistema per modificare un'interfaccia di rete

### Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare  > **Modifica** accanto all'interfaccia di rete che si desidera modificare.
3. Modificare una o più impostazioni dell'interfaccia di rete. Per ulteriori informazioni, vedere ["Creare una LIF"](#).
4. Salvare le modifiche.

### CLI

#### Utilizzare la CLI per modificare una LIF

### Fasi

1. Modificare gli attributi di una LIF utilizzando `network interface modify` comando.

Nell'esempio seguente viene illustrato come modificare l'indirizzo IP e la maschera di rete dei dati LIF 2 utilizzando un indirizzo IP e il valore della maschera di rete della subnet client1\_sub:

```
network interface modify -vserver vs1 -lif datalif2 -subnet-name
client1_sub
```

Nell'esempio seguente viene illustrato come modificare la politica di servizio di una LIF.

```
network interface modify -vserver siteA -lif node1_inter1 -service
-policy example
```

2. Verificare che gli indirizzi IP siano raggiungibili.

Se si utilizza...	Quindi utilizzare...
Indirizzi IPv4	<code>network ping</code>
Indirizzi IPv6	<code>network ping6</code>

## Migrare una LIF

Potrebbe essere necessario migrare un LIF a una porta diversa sullo stesso nodo o su un nodo diverso all'interno del cluster, se la porta è guasta o richiede manutenzione. La migrazione di un LIF è simile al failover LIF, ma la migrazione LIF è un'operazione manuale, mentre il failover LIF è la migrazione automatica di un LIF in risposta a un errore di collegamento sulla porta di rete corrente del LIF.

## Prima di iniziare

- È necessario che sia stato configurato un gruppo di failover per le LIF.
- Il nodo di destinazione e le porte devono essere operativi e devono poter accedere alla stessa rete della porta di origine.

## A proposito di questa attività

- I LIF BGP risiedono sulla porta home e non possono essere migrati su altri nodi o porte.
- Prima di rimuovere la scheda NIC dal nodo, è necessario migrare i file LIF ospitati sulle porte appartenenti a una scheda NIC in altre porte del cluster.
- È necessario eseguire il comando per la migrazione di un LIF del cluster dal nodo in cui è ospitato il LIF del cluster.
- Una LIF con ambito di nodo, come LIF di gestione con ambito di nodo, LIF di cluster, LIF di intercluster, non può essere migrata a un nodo remoto.
- Quando si esegue la migrazione di un LIF NFSv4 tra nodi, si verifica un ritardo fino a 45 secondi prima che il LIF sia disponibile su una nuova porta.

Per risolvere questo problema, utilizzare NFSv4.1 dove non si verificano ritardi.

- Puoi migrare LIF iSCSI su piattaforme ASA (All-Flash SAN Array) che eseguono ONTAP 9.11.1 o versioni successive.

La migrazione delle LIF iSCSI è limitata alle porte sul nodo principale o sul partner ha.

- Se la tua piattaforma non è una piattaforma ASA (All-Flash SAN Array) che esegue ONTAP versione 9.11.1 o successiva, non puoi migrare le LIF iSCSI da un nodo a un altro nodo.

Per aggirare questa restrizione, è necessario creare una LIF iSCSI sul nodo di destinazione. Scopri di più ["Creazione di LIF iSCSI"](#).

- Se si desidera migrare una LIF (interfaccia di rete) per NFS su RDMA, assicurarsi che la porta di destinazione sia compatibile con RoCE. È necessario eseguire ONTAP 9.10.1 o versione successiva per migrare un file LIF con l'interfaccia CLI o ONTAP 9.12.1 per eseguire la migrazione utilizzando Gestione sistema. In System Manager, una volta selezionata la porta di destinazione compatibile con RoCE, selezionare la casella di controllo accanto a **Usa porte RoCE** per completare correttamente la migrazione. Scopri di più ["Configurazione di LIF per NFS su RDMA"](#).
- Le operazioni di offload delle copie VMware VAAI non vengono eseguite quando si esegue la migrazione della LIF di origine o di destinazione. Informazioni sulla funzione di off-load delle copie:
  - ["Ambienti NFS"](#)
  - ["Ambienti SAN"](#)

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

### Utilizzare System Manager per migrare un'interfaccia di rete

#### Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare **⋮ > Migrate** accanto all'interfaccia di rete che si desidera modificare.



Per una LIF iSCSI, nella finestra di dialogo **Migrate Interface**, selezionare il nodo di destinazione e la porta del partner ha.

Se vuoi migrare la LIF iSCSI in modo permanente, seleziona la casella di controllo. La LIF iSCSI deve essere offline prima di poter essere migrata in modo permanente. Inoltre, una volta migrata in modo permanente, una LIF iSCSI non può essere annullata. Non esiste alcuna opzione di revert.

3. Fare clic su **Migra**.
4. Salvare le modifiche.

#### CLI

### Utilizzare la CLI per migrare una LIF

#### Fase

A seconda che si desideri migrare una LIF specifica o tutte le LIF, eseguire l'azione appropriata:

Se si desidera eseguire la migrazione...	Immettere il seguente comando...
Una LIF specifica	<code>network interface migrate</code>
Tutte le LIF di gestione dei dati e dei cluster su un nodo	<code>network interface migrate-all</code>
Tutte le LIF di una porta	<code>network interface migrate-all -node &lt;node&gt; -port &lt;port&gt;</code>

Nell'esempio seguente viene illustrato come migrare un LIF denominato `datalif1` Su SVM `vs0` alla porta `e0d` acceso `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b  
-dest-port e0d
```

Nell'esempio seguente viene illustrato come migrare tutti i dati e le LIF di gestione del cluster dal nodo (locale) corrente:

```
network interface migrate-all -node local
```

Ripristinare la porta home di un LIF

È possibile ripristinare la porta home di un LIF dopo il failover o la migrazione a una porta diversa manualmente o automaticamente. Se la porta home di un LIF specifico non è disponibile, LIF rimane sulla porta corrente e non viene ripristinata.

A proposito di questa attività


- Se si porta la porta home di un LIF in stato attivo prima di impostare l'opzione di revert automatico, il LIF non viene restituito alla porta home.
- Il LIF non viene ripristinato automaticamente a meno che il valore dell'opzione "auto-revert" non sia impostato su true.
- È necessario assicurarsi che l'opzione "auto-revert" (indirizzamento automatico) sia attivata per ripristinare le porte home dei file LIF.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

System Manager

Utilizzare System Manager per ripristinare un'interfaccia di rete alla porta home

Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare  > **Ripristina** accanto all'interfaccia di rete che si desidera modificare.
3. Selezionare **Ripristina** per ripristinare un'interfaccia di rete alla porta home.

CLI

Utilizzare l'interfaccia CLI per ripristinare la porta LIF home

Fase

Ripristinare manualmente o automaticamente la porta home di un LIF:

Se si desidera ripristinare la porta home di un LIF...	Quindi immettere il seguente comando...
Manualmente	<code>network interface revert -vserver vservice_name -lif lif_name</code>
Automaticamente	<code>network interface modify -vserver vservice_name -lif lif_name -auto-revert true</code>

ONTAP 9.8 e versioni successive: Ripristino da una LIF del cluster configurata in modo errato

Non è possibile creare un cluster quando la rete del cluster è cablata a uno switch, ma non tutte le porte configurate in Cluster IPspace possono raggiungere le altre porte configurate in Cluster IPspace.

A proposito di questa attività

In un cluster con switch, se un'interfaccia di rete del cluster (LIF) è configurata sulla porta errata o se una porta del cluster è collegata alla rete errata, il `cluster create` il comando può non riuscire e visualizzare il seguente errore:



Not all local cluster ports have reachability to one another.  
Use the "network port reachability show -detail" command for more details.

I risultati di `network port show` Il comando potrebbe indicare che diverse porte vengono aggiunte a Cluster IPspace perché sono connesse a una porta configurata con una LIF del cluster. Tuttavia, i risultati di `network port reachability show -detail` il comando rivela quali porte non dispongono di connettività l'una con l'altra.

Per eseguire il ripristino da una LIF del cluster configurata su una porta non raggiungibile con le altre porte configurate con le LIF del cluster, attenersi alla seguente procedura:

#### Fasi

1. Ripristinare la porta home del LIF del cluster alla porta corretta:

```
network port modify -home-port
```

2. Rimuovere dal dominio di trasmissione del cluster le porte che non hanno LIF del cluster configurate:

```
network port broadcast-domain remove-ports
```

3. Creare il cluster:

```
cluster create
```

#### Risultato

Una volta completata la creazione del cluster, il sistema rileva la configurazione corretta e inserisce le porte nei domini di trasmissione corretti.

#### Eliminare una LIF

È possibile eliminare un'interfaccia di rete (LIF) non più richiesta.

#### Prima di iniziare

I LIF da eliminare non devono essere in uso.

#### Fasi

1. Contrassegnare i file LIF che si desidera eliminare come amministrativamente bassi utilizzando il seguente comando:

```
network interface modify -vserver vservice_name -lif lif_name -status  
-admin down
```

2. Utilizzare `network interface delete` Comando per eliminare una o tutte le LIF:

Se si desidera eliminare...	Immettere il comando ...
Una LIF specifica	<code>network interface delete -vserver vs1 -lif lif_name</code>
Tutte le LIF	<code>network interface delete -vserver vs1 -lif *</code>

Il seguente comando elimina LIF mgmtlif2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Utilizzare `network interface show` Comando per confermare che la LIF è stata eliminata.

## Bilanciamento dei carichi di rete

### Panoramica della rete Balance

È possibile configurare il cluster per soddisfare le richieste dei client da LIF caricate in modo appropriato. Ciò comporta un utilizzo più bilanciato di LIF e porte, che a sua volta consente migliori performance del cluster.

Il bilanciamento del carico DNS consente di selezionare una LIF di dati opportunamente caricata e di bilanciare il traffico di rete dell'utente su tutte le porte disponibili (fisiche, gruppi di interfacce e VLAN).

Con il bilanciamento del carico DNS, i LIF sono associati alla zona di bilanciamento del carico di una SVM. Un server DNS a livello di sito è configurato per inoltrare tutte le richieste DNS e restituire il LIF meno caricato in base al traffico di rete e alla disponibilità delle risorse delle porte (utilizzo della CPU, throughput, connessioni aperte e così via). Il bilanciamento del carico DNS offre i seguenti vantaggi:

- Nuove connessioni client bilanciate tra le risorse disponibili.
- Non è richiesto alcun intervento manuale per decidere quali LIF utilizzare durante il montaggio di una specifica SVM.
- Il bilanciamento del carico DNS supporta NFSv3, NFSv4, NFSv4.1, SMB 2.0, SMB 2.1, SMB 3.0 e S3.

### Come funziona il bilanciamento del carico DNS

I client montano una SVM specificando un indirizzo IP (associato a una LIF) o un nome host (associato a più indirizzi IP). Per impostazione predefinita, i LIF vengono selezionati dal server DNS a livello di sito in modo round-robin, che bilancia il carico di lavoro in tutte le LIF.

Il bilanciamento del carico round-robin può comportare l'overload di alcune LIF, pertanto è possibile utilizzare una zona di bilanciamento del carico DNS che gestisce la risoluzione del nome host in una SVM. L'utilizzo di una zona di bilanciamento del carico DNS garantisce un migliore bilanciamento delle nuove connessioni client tra le risorse disponibili, migliorando le performance del cluster.

Una zona di bilanciamento del carico DNS è un server DNS all'interno del cluster che valuta dinamicamente il

carico su tutte le LIF e restituisce una LIF caricata correttamente. In una zona di bilanciamento del carico, DNS assegna un peso (metrico), in base al carico, a ciascun LIF.

A ogni LIF viene assegnato un peso in base al carico della porta e all'utilizzo della CPU del nodo principale. Le LIF che si trovano su porte meno caricate hanno una maggiore probabilità di essere restituite in una query DNS. I pesi possono anche essere assegnati manualmente.

## Creare una zona di bilanciamento del carico DNS

È possibile creare una zona di bilanciamento del carico DNS per facilitare la selezione dinamica di una LIF in base al carico, ovvero al numero di client montati su una LIF. È possibile creare una zona di bilanciamento del carico durante la creazione di una LIF dati.

### Prima di iniziare

Il server di inoltro DNS sul server DNS del sito deve essere configurato per inoltrare tutte le richieste per la zona di bilanciamento del carico ai file LIF configurati.

L'articolo della Knowledge base ["Come impostare il bilanciamento del carico DNS in Cluster-Mode"](#) Sul sito del supporto NetApp sono disponibili ulteriori informazioni sulla configurazione del bilanciamento del carico DNS mediante l'inoltro condizionale.

### A proposito di questa attività

- Qualsiasi LIF di dati può rispondere alle query DNS per un nome di zona per il bilanciamento del carico DNS.
- Una zona di bilanciamento del carico DNS deve avere un nome univoco nel cluster e il nome della zona deve soddisfare i seguenti requisiti:
  - Non deve superare i 256 caratteri.
  - Deve includere almeno un periodo.
  - Il primo e l'ultimo carattere non devono essere un punto o altri caratteri speciali.
  - Non può includere spazi tra caratteri.
  - Ogni etichetta nel nome DNS non deve superare i 63 caratteri.

Un'etichetta è il testo che compare prima o dopo il periodo. Ad esempio, la zona DNS denominata `storage.company.com` ha tre etichette.

### Fase

Utilizzare `network interface create` con il `dns-zone` Opzione per creare una zona di bilanciamento del carico DNS.

Se la zona di bilanciamento del carico esiste già, la LIF viene aggiunta ad essa. Per ulteriori informazioni sul comando, vedere ["Comandi di ONTAP 9"](#).

Nell'esempio riportato di seguito viene illustrato come creare una zona di bilanciamento del carico DNS denominata `storage.company.com` durante la creazione della LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

## Aggiungere o rimuovere una LIF da una zona di bilanciamento del carico

È possibile aggiungere o rimuovere una LIF dalla zona di bilanciamento del carico DNS di una macchina virtuale (SVM). È inoltre possibile rimuovere tutti i file LIF contemporaneamente da una zona di bilanciamento del carico.

### Prima di iniziare

- Tutte le LIF in una zona di bilanciamento del carico devono appartenere alla stessa SVM.
- Una LIF può far parte di una sola zona di bilanciamento del carico DNS.
- Se le LIF appartengono a sottoreti diverse, devono essere stati impostati gruppi di failover per ciascuna sottorete.

### A proposito di questa attività

Una LIF che si trova nello stato di inattività amministrativa viene temporaneamente rimossa dalla zona di bilanciamento del carico DNS. Quando la LIF ritorna allo stato di amministrazione attiva, la LIF viene aggiunta automaticamente alla zona di bilanciamento del carico DNS.

### Fase

Aggiungere o rimuovere una LIF da una zona di bilanciamento del carico:

Se si desidera...	Inserisci...
Aggiungere una LIF	<code>network interface modify -vserver vs1 -lif lif1 -dns-zone zone1</code> Esempio: <code>`network interface modify -vserver vs1 -lif data1 -dns-zone cifs.company.com`</code>
Rimuovere una singola LIF	<code>network interface modify -vserver vs1 -lif lif1 -dns-zone none</code> Esempio: <code>`network interface modify -vserver vs1 -lif data1 -dns-zone none`</code>
Rimuovere tutti i LIF	<code>`network interface modify -vserver vs1 -lif * -dns-zone none`</code> Esempio: <code>`network interface modify -vserver vs0 -lif * -dns-zone none`</code> È possibile rimuovere una SVM da una zona di bilanciamento del carico rimuovendo tutte le LIF presenti nella SVM da tale zona.

## Configurazione dei servizi DNS (ONTAP 9,8 e versioni successive)

È necessario configurare i servizi DNS per SVM prima di creare un server NFS o SMB. In genere, i server dei nomi DNS sono i server DNS integrati in Active Directory per il dominio a cui si aggiungerà il server NFS o SMB.

## A proposito di questa attività

I server DNS integrati in Active Directory contengono i record di posizione del servizio (SRV) per i server LDAP e dei controller di dominio. Se SVM non riesce a trovare i server LDAP e i controller di dominio di Active Directory, la configurazione del server NFS o SMB non riesce.

Le SVM utilizzano il database ns-switch dei servizi dei nomi host per determinare i servizi dei nomi da utilizzare e in quale ordine quando si cercano informazioni sugli host. I due name service supportati per il database host sono file e dns.

Prima di creare il server SMB, è necessario assicurarsi che il dns sia una delle origini.



Per visualizzare le statistiche per i servizi dei nomi DNS per il processo mgwd e il processo SecD, utilizzare l'interfaccia utente Statistics.

## Fasi

1. Determinare la configurazione corrente per il database dei servizi di nomi host. In questo esempio, il database del servizio nomi host utilizza le impostazioni predefinite.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Eseguire le seguenti operazioni, se necessario.

- a. Aggiungere il servizio nome DNS al database del servizio nome host nell'ordine desiderato oppure riordinare le origini.

In questo esempio, il database degli host è configurato per l'utilizzo di DNS e file locali in tale ordine.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- b. Verificare che la configurazione dei name service sia corretta.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. Configurare i servizi DNS.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



Il comando di creazione dns dei servizi vserver esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non è in grado di contattare il server dei nomi.

4. Verificare che la configurazione DNS sia corretta e che il servizio sia attivato.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Convalidare lo stato dei server dei nomi.

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

## Configurare il DNS dinamico sulla SVM

Se si desidera che il server DNS integrato in Active Directory registri dinamicamente i record DNS di un server NFS o SMB in DNS, è necessario configurare il DNS dinamico (DDNS) su SVM.

### Prima di iniziare

I name service DNS devono essere configurati su SVM. Se si utilizza un DDNS sicuro, è necessario utilizzare i server dei nomi DNS integrati in Active Directory e creare un server NFS o SMB o un account Active Directory per SVM.

### A proposito di questa attività

Il nome di dominio completo (FQDN) specificato deve essere univoco:

Il nome di dominio completo (FQDN) specificato deve essere univoco:

- Per NFS, il valore specificato in `-vserver-fqdn` come parte di `vserver services name-service dns dynamic-update` Command diventa il nome FQDN registrato per i LIF.
- Per SMB, i valori specificati come nome NetBIOS del server CIFS e nome di dominio completo del server CIFS diventano FQDN registrato per i LIF. Non è configurabile in ONTAP. Nel seguente scenario, l'FQDN LIF è "CIFS\_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1
```

```

Vserver: vs1
CIFS Server NetBIOS Name: CIFS_VS1
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
Workgroup Name: -
Kerberos Realm: -
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```



Per evitare un errore di configurazione di un FQDN SVM non conforme alle regole RFC per gli aggiornamenti DDNS, utilizzare un nome FQDN compatibile con RFC. Per ulteriori informazioni, vedere ["RFC 1123"](#).

## Fasi

### 1. Configurare DDNS su SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is-enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Gli asterischi non possono essere utilizzati come parte del FQDN personalizzato. Ad esempio, \*.netapp.com non è valido.

### 2. Verificare che la configurazione DDNS sia corretta:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

## Configurazione dei servizi DNS (ONTAP 9,7 e versioni precedenti)

È necessario configurare i servizi DNS per SVM prima di creare un server NFS o SMB. In genere, i server dei nomi DNS sono i server DNS integrati in Active Directory per il dominio a cui si aggiungerà il server NFS o SMB.

## A proposito di questa attività

I server DNS integrati in Active Directory contengono i record di posizione del servizio (SRV) per i server LDAP e dei controller di dominio. Se SVM non riesce a trovare i server LDAP e i controller di dominio di Active Directory, la configurazione del server NFS o SMB non riesce.

Le SVM utilizzano il database ns-switch dei servizi dei nomi host per determinare i servizi dei nomi da utilizzare e in quale ordine quando si cercano informazioni sugli host. I due name service supportati per il database host sono `files` e `dns`.

È necessario assicurarsi che `dns` È una delle origini prima di creare il server SMB.



Per visualizzare le statistiche per i servizi dei nomi DNS per il processo `mgwd` e il processo `SecD`, utilizzare l'interfaccia utente `Statistics`.

## Fasi

1. Determinare la configurazione corrente per `hosts` database name services.

In questo esempio, il database del servizio nomi host utilizza le impostazioni predefinite.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Eseguire le seguenti operazioni, se necessario.

- a. Aggiungere il servizio nome DNS al database del servizio nome host nell'ordine desiderato oppure riordinare le origini.

In questo esempio, il database degli host è configurato per l'utilizzo di DNS e file locali in tale ordine.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- a. Verificare che la configurazione dei name service sia corretta.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

3. Configurare i servizi DNS.

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



I servizi `vserver name-service dns create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non è in grado di contattare il server dei nomi.

4. Verificare che la configurazione DNS sia corretta e che il servizio sia attivato.



```
Vserver: vs1
Domains: example.com, example2.com Name
Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

##### 5. Convalidare lo stato dei server dei nomi.

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

## Configurare il DNS dinamico sulla SVM

Se si desidera che il server DNS integrato in Active Directory registri dinamicamente i record DNS di un server NFS o SMB in DNS, è necessario configurare il DNS dinamico (DDNS) su SVM.

### Prima di iniziare

I name service DNS devono essere configurati su SVM. Se si utilizza un DDNS sicuro, è necessario utilizzare i server dei nomi DNS integrati in Active Directory e creare un server NFS o SMB o un account Active Directory per SVM.

### A proposito di questa attività

Il nome di dominio completo (FQDN) specificato deve essere univoco:

- Per NFS, il valore specificato in `-vserver-fqdn` come parte di `vserver services name-service dns dynamic-update` Command diventa il nome FQDN registrato per i LIF.
- Per SMB, i valori specificati come nome NetBIOS del server CIFS e nome di dominio completo del server CIFS diventano FQDN registrato per i LIF. Non è configurabile in ONTAP. Nel seguente scenario, l'FQDN LIF è "CIFS\_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1
```

```

                                Vserver: vs1
                                CIFS Server NetBIOS Name: CIFS_VS1
                                NetBIOS Domain/Workgroup Name: EXAMPLE
                                Fully Qualified Domain Name: EXAMPLE.COM
                                Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                Workgroup Name: -
                                Kerberos Realm: -
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
                                CIFS Server Description:
                                List of NetBIOS Aliases: -
```



Per evitare un errore di configurazione di un FQDN SVM non conforme alle regole RFC per gli aggiornamenti DDNS, utilizzare un nome FQDN compatibile con RFC. Per ulteriori informazioni, vedere ["RFC 1123"](#).

## Fasi

### 1. Configurare DDNS su SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Gli asterischi non possono essere utilizzati come parte del FQDN personalizzato. Ad esempio, \*.netapp.com non è valido.

### 2. Verificare che la configurazione DDNS sia corretta:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

## Configurare i servizi DNS dinamici

Se si desidera che il server DNS integrato in Active Directory registri dinamicamente i record DNS di un server NFS o SMB in DNS, è necessario configurare il DNS dinamico (DDNS) su SVM.

## Prima di iniziare

I name service DNS devono essere configurati su SVM. Se si utilizza un DDNS sicuro, è necessario utilizzare i server dei nomi DNS integrati in Active Directory e creare un server NFS o SMB o un account Active Directory per SVM.

## A proposito di questa attività

L'FQDN specificato deve essere univoco.



Per evitare un errore di configurazione di un FQDN SVM non conforme alle regole RFC per gli aggiornamenti DDNS, utilizzare un nome FQDN compatibile con RFC.

## Fasi

1. Configurare DDNS su SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name  
-is-enabled true [-use-secure {true|false}] -vserver-fqdn  
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is-  
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Gli asterischi non possono essere utilizzati come parte del FQDN personalizzato. Ad esempio, \*.netapp.com non è valido.

2. Verificare che la configurazione DDNS sia corretta:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

# Risoluzione del nome host

## Panoramica sulla risoluzione dei nomi host

ONTAP deve essere in grado di convertire i nomi host in indirizzi IP numerici per fornire l'accesso ai client e ai servizi di accesso. È necessario configurare le macchine virtuali di storage (SVM) in modo che utilizzino i name service locali o esterni per risolvere le informazioni sugli host. ONTAP supporta la configurazione di un server DNS esterno o la configurazione del file host locale per la risoluzione dei nomi host.

Quando si utilizza un server DNS esterno, è possibile configurare il DNS dinamico (DDNS), che invia automaticamente informazioni DNS nuove o modificate dal sistema di storage al server DNS. Senza aggiornamenti DNS dinamici, è necessario aggiungere manualmente le informazioni DNS (nome DNS e indirizzo IP) ai server DNS identificati quando un nuovo sistema viene messo in linea o quando le informazioni DNS esistenti cambiano. Questo processo è lento e soggetto a errori. Durante il disaster recovery, la configurazione manuale può causare un lungo downtime.

## Configurare il DNS per la risoluzione del nome host

Il DNS viene utilizzato per accedere a fonti locali o remote per ottenere informazioni sull'host. È necessario configurare il DNS per accedere a una o a entrambe queste origini.

ONTAP deve essere in grado di cercare le informazioni dell'host per fornire un accesso appropriato ai client. È necessario configurare i name service per consentire a ONTAP di accedere ai servizi DNS locali o esterni per ottenere le informazioni sull'host.

ONTAP memorizza le informazioni di configurazione del name service in una tabella equivalente a `/etc/nsswitch.conf` File su sistemi UNIX.

### Configurazione di una SVM e di una LIF di dati per la risoluzione del nome host utilizzando un server DNS esterno

È possibile utilizzare `vserver services name-service dns` Per abilitare il DNS su una SVM e configurarlo per l'utilizzo del DNS per la risoluzione dei nomi host. I nomi host vengono risolti utilizzando server DNS esterni.

#### Prima di iniziare

Per la ricerca dei nomi host, è necessario che sia disponibile un server DNS a livello di sito.

È necessario configurare più server DNS per evitare un singolo punto di errore. Il `vserver services name-service dns create` Viene visualizzato un messaggio di avviso se si immette un solo nome server DNS.

#### A proposito di questa attività

Vedere [Configurare i servizi DNS dinamici](#) Per ulteriori informazioni sulla configurazione del DNS dinamico su SVM.

#### Fasi

1. Abilitare il DNS sulla SVM:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

Il seguente comando abilita i server DNS esterni su SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



Il `vserver services name-service dns create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non riesce a contattare il server dei nomi.

2. Convalidare lo stato dei server dei nomi utilizzando `vserver services name-service dns check`

comando.

```
vserver services name-service dns check -vserver vs1.example.com
```

Name Server			
Vserver	Name Server	Status	Status Details
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

Per informazioni sulle politiche di servizio relative al DNS, vedere ["LIF e policy di servizio in ONTAP 9.6 e versioni successive"](#).

## Configurare la tabella Name Service Switch per la risoluzione dei nomi host

Per consentire a ONTAP di consultare il servizio di nomi locale o esterno per recuperare le informazioni sull'host, è necessario configurare correttamente la tabella degli switch del servizio di nomi.

### Prima di iniziare

È necessario decidere quale name service utilizzare per il mapping degli host nel proprio ambiente.

### Fasi

1. Aggiungere le voci necessarie alla tabella dei name service switch:

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. Verificare che la tabella name service switch contenga le voci previste nell'ordine desiderato:

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

### Esempio

Nell'esempio seguente viene modificata una voce nella tabella degli switch del servizio nomi per SVM VS1 in modo da utilizzare prima il file hosts locale e poi un server DNS esterno per risolvere i nomi host:

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

## Gestire la tabella degli host (solo amministratori del cluster)

Un amministratore del cluster può aggiungere, modificare, eliminare e visualizzare le voci del nome host nella tabella hosts della macchina virtuale di storage amministrativa (SVM). Un amministratore SVM può configurare le voci del nome host solo per la SVM

assegnata.

## Comandi per la gestione delle voci dei nomi host locali

È possibile utilizzare `vserver services name-service dns hosts` Per creare, modificare o eliminare le voci della tabella host DNS.

Quando si creano o modificano le voci del nome host DNS, è possibile specificare più indirizzi alias separati da virgole.

Se si desidera...	Utilizzare questo comando...
Creare un nome host DNS	<code>vserver services name-service dns hosts create</code>
Modificare una voce del nome host DNS	<code>vserver services name-service dns hosts modify</code>
Eliminare una voce del nome host DNS	<code>vserver services name-service dns hosts delete</code>

Per ulteriori informazioni, consultare ["Comandi di ONTAP 9"](#) per `vserver services name-service dns hosts` comandi.

## Proteggere la rete

### Configurare la sicurezza di rete utilizzando gli standard FIPS (Federal Information Processing Standards)

ONTAP è conforme agli standard federali sull'elaborazione delle informazioni (FIPS) 140-2 per tutte le connessioni SSL. È possibile attivare e disattivare la modalità SSL FIPS, impostare i protocolli SSL a livello globale e disattivare le crittografie deboli, ad esempio RC4, in ONTAP.

Per impostazione predefinita, SSL su ONTAP è impostato con la compliance FIPS disattivata e il protocollo SSL attivato con quanto segue:

- TLSv1.3 (a partire da ONTAP 9.11.1)
- TLSv1.2
- TLSv1.1
- TLSv1

Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP a componenti client o server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.

Se si desidera che gli account amministratore accedano alle SVM con una chiave pubblica SSH, assicurarsi che l'algoritmo della chiave host sia supportato prima di attivare la modalità SSL FIPS.

**Nota:** il supporto dell'algoritmo della chiave host è stato modificato in ONTAP 9.11.1 e versioni successive.

Release di ONTAP	Tipi di chiave supportati	Tipi di chiave non supportati
9.11.1 e versioni successive	ecdsa-sha2-nistp256	rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 e versioni precedenti	ecdsa-sha2-nistp256 + ssh-ed25519	ssh-dss + ssh-rsa

Gli account di chiave pubblica SSH esistenti senza gli algoritmi di chiave supportati devono essere riconfigurati con un tipo di chiave supportato prima di attivare FIPS, altrimenti l'autenticazione dell'amministratore non avrà esito positivo.

Per ulteriori informazioni, vedere ["Abilitare gli account a chiave pubblica SSH"](#).

Per ulteriori informazioni sulla configurazione della modalità SSL FIPS, consultare `security config modify` pagina man.

## Abilitare FIPS

Si consiglia a tutti gli utenti sicuri di modificare la propria configurazione di sicurezza subito dopo l'installazione o l'aggiornamento del sistema. Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP a componenti client o server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.



Quando FIPS è attivato, non è possibile installare o creare un certificato con una chiave RSA di lunghezza pari a 4096.

## Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Attiva FIPS:

```
security config modify -interface SSL -is-fips-enabled true
```

3. Quando viene richiesto di continuare, immettere `y`
4. Se si utilizza ONTAP 9.8 o versioni precedenti, riavviare manualmente uno ad uno ogni nodo del cluster. A partire da ONTAP 9.9.1, non è necessario riavviare.

## Esempio

Se si utilizza ONTAP 9.9.1 o versione successiva, il messaggio di avviso non viene visualizzato.

```
security config modify -interface SSL -is-fips-enabled true
```

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components to fail. MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

## Disattiva FIPS

Se si esegue ancora una configurazione di sistema precedente e si desidera configurare ONTAP con compatibilità con le versioni precedenti, è possibile attivare SSLv3 solo quando FIPS è disattivato.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Disattivare FIPS digitando:

```
security config modify -interface SSL -is-fips-enabled false
```

3. Quando viene richiesto di continuare, immettere y.
4. Se si utilizza ONTAP 9.8 o versioni precedenti, riavviare manualmente ciascun nodo del cluster. A partire da ONTAP 9.9.1, non è necessario riavviare.

### Esempio

Se si utilizza ONTAP 9.9.1 o versione successiva, il messaggio di avviso non viene visualizzato.



```
security config modify -interface SSL -supported-protocols SSLv3
```

Warning: Enabling the SSLv3 protocol may reduce the security of the interface, and is not recommended.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

## Visualizza lo stato di conformità FIPS

È possibile verificare se l'intero cluster esegue le impostazioni di configurazione della protezione corrente.

### Fasi

1. Riavviare uno alla volta ciascun nodo del cluster.

Non riavviare tutti i nodi del cluster contemporaneamente. È necessario riavviare il sistema per assicurarsi che tutte le applicazioni del cluster eseguano la nuova configurazione di sicurezza e per tutte le modifiche apportate alla modalità FIPS on/off, ai protocolli e ai cifrari.

2. Visualizza lo stato di conformità corrente:

```
security config show
```

```
security config show
```

Cluster				Cluster
Security	Interface	FIPS Mode	Supported Protocols	Supported Ciphers Config
Ready				
-----	-----	-----	-----	-----
-----				
SSL	false	TLsv1_2, TLsv1_1, TLsv1	ALL:!LOW:!aNULL: !EXP:!eNULL	yes

## Configurare la crittografia IP Security (IPsec) over wire

ONTAP utilizza IPsec (Internet Protocol Security) in modalità di trasporto per garantire che i dati siano costantemente protetti e crittografati, anche durante il transito. IPsec offre la crittografia dei dati per tutto il traffico IP, inclusi i protocolli NFS, iSCSI e SMB.

A partire da ONTAP 9.12.1, il supporto IPsec del protocollo host front-end è disponibile nelle configurazioni MetroCluster IP e MetroCluster fabric-attached.

Il supporto di IPsec nei cluster MetroCluster è limitato al traffico host front-end e non è supportato dalle LIF intercluster MetroCluster.

A partire da ONTAP 9.10.1, è possibile utilizzare chiavi precondivise (PSK) o certificati per l'autenticazione con IPsec. In precedenza, solo gli PSK erano supportati con IPsec.

A partire da ONTAP 9.9.1, gli algoritmi di crittografia utilizzati da IPsec sono validati in FIPS 140-2. Gli algoritmi vengono generati dal modulo crittografico NetApp in ONTAP che riporta la convalida FIPS 140-2.

A partire da ONTAP 9.8, ONTAP supporta IPsec in modalità di trasporto.

Una volta configurato IPsec, il traffico di rete tra il client e ONTAP viene protetto con misure preventive per combattere gli attacchi di tipo play e man-in-the-middle (MITM).

Per NetApp SnapMirror e la crittografia del traffico di peering del cluster, la crittografia di peering del cluster (CPE) e la protezione TLS (Transport Layer Security) sono ancora consigliate su IPsec per garantire la sicurezza in transito via cavo. Questo perché TLS offre performance migliori rispetto a IPsec.

Mentre la funzionalità IPsec è attivata sul cluster, la rete richiede una voce del database dei criteri di protezione (SPD) che corrisponda al traffico da proteggere e che specifichi i dettagli di protezione (come la suite di crittografia e il metodo di autenticazione) prima che il traffico possa fluire. Su ciascun client è necessaria anche una voce SPD corrispondente.

## **Abilitare IPsec sul cluster**

È possibile attivare IPsec sul cluster per garantire che i dati siano costantemente protetti e crittografati, anche durante il transito.

### **Fasi**

1. Scopri se IPsec è già attivato:

```
security ipsec config show
```

Se il risultato include `IPsec Enabled: false`, passare alla fase successiva.

2. Attiva IPsec:

```
security ipsec config modify -is-enabled true
```

3. Eseguire nuovamente il comando di rilevamento:

```
security ipsec config show
```

Il risultato ora include `IPsec Enabled: true`.

## **Preparare la creazione del criterio IPsec con l'autenticazione del certificato**

È possibile saltare questo passaggio se si utilizzano solo chiavi pre-condivise (PSK) per l'autenticazione e non si utilizza l'autenticazione del certificato.

Prima di creare un criterio IPsec che utilizza i certificati per l'autenticazione, è necessario verificare che siano soddisfatti i seguenti prerequisiti:

- Sia ONTAP che il client devono avere installato il certificato CA dell'altra parte in modo che i certificati dell'entità finale (ONTAP o client) siano verificabili da entrambe le parti
- Viene installato un certificato per il LIF ONTAP che partecipa al criterio



Le LIF ONTAP possono condividere i certificati. Non è richiesta una mappatura uno-a-uno tra certificati e LIF.

## Fasi

1. Installare tutti i certificati CA utilizzati durante l'autenticazione reciproca, incluse le CA lato ONTAP e lato client, nella gestione dei certificati ONTAP, a meno che non sia già installato (come nel caso di una CA root autofirmata di ONTAP).

### Comando di esempio

```
cluster::> security certificate install -vserver svm_name -type server-ca
-cert-name my_ca_cert
```

2. Per assicurarsi che la CA installata rientri nel percorso di ricerca della CA IPsec durante l'autenticazione, aggiungere le CA di gestione dei certificati ONTAP al modulo IPsec utilizzando `security ipsec ca-certificate add` comando.

### Comando di esempio

```
cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
my_ca_cert
```

3. Creare e installare un certificato per l'utilizzo da parte della LIF ONTAP. La CA emittente di questo certificato deve essere già installata in ONTAP e aggiunta a IPsec.

### Comando di esempio

```
cluster::> security certificate install -vserver svm_name -type server -cert
-name my_nfs_server_cert
```

Per ulteriori informazioni sui certificati in ONTAP, vedere i comandi dei certificati di protezione nella documentazione di ONTAP 9 .

## Definizione del database dei criteri di protezione (SPD)

IPsec richiede una voce SPD prima di consentire il flusso del traffico sulla rete. Ciò vale sia che si utilizzi un PSK o un certificato per l'autenticazione.

## Fasi

1. Utilizzare `security ipsec policy create` comando a:
  - a. Selezionare l'indirizzo IP ONTAP o la subnet degli indirizzi IP per partecipare al trasporto IPsec.
  - b. Selezionare gli indirizzi IP del client che si connetteranno agli indirizzi IP ONTAP.



Il client deve supportare Internet Key Exchange versione 2 (IKEv2) con una chiave precondivisa (PSK).

- c. Opzionale. Selezionare i parametri di traffico a grana fine, ad esempio i protocolli di livello superiore (UDP, TCP, ICMP, ecc.) , i numeri delle porte locali e i numeri delle porte remote per proteggere il traffico. I parametri corrispondenti sono `protocols`, `local-ports` e `remote-ports`

rispettivamente.

Ignorare questo passaggio per proteggere tutto il traffico tra l'indirizzo IP ONTAP e l'indirizzo IP del client. La protezione di tutto il traffico è l'impostazione predefinita.

- d. Immettere PSK o Public-Key Infrastructure (PKI) per `auth-method` parametro per il metodo di autenticazione desiderato.
  - i. Se si immette una PSK, includere i parametri, quindi premere <enter> per visualizzare la richiesta di immissione e verifica della chiave precondivisa.



`local-identity` e `remote-identity` I parametri sono facoltativi se sia l'host che il client utilizzano il metodo `strongSwan` e non è stato selezionato alcun criterio con caratteri jolly per l'host o il client.

- ii. Se si inserisce un'infrastruttura PKI, è necessario immettere anche il `cert-name`, `local-identity`, `remote-identity` parametri. Se l'identità del certificato lato remoto non è nota o se sono previste più identità client, inserire l'identità speciale `ANYTHING`.

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

Il traffico IP non può passare tra il client e il server finché ONTAP e il client non hanno impostato i criteri IPSec corrispondenti e le credenziali di autenticazione (PSK o certificato) non sono installate su entrambi i lati. Per ulteriori informazioni, vedere la configurazione IPSec lato client.

## Utilizzare le identità IPsec

Per il metodo di autenticazione con chiave pre-condivisa, le identità locali e remote sono facoltative se host e client utilizzano il metodo di autenticazione con chiave `strongSwan` e non è stato selezionato alcun criterio con caratteri jolly per l'host o il client.

Per il metodo di autenticazione PKI/certificato, le identità locali e remote sono obbligatorie. Le identità specificano l'identità certificata all'interno del certificato di ciascun lato e vengono utilizzate nel processo di verifica. Se l'identità remota è sconosciuta o se può essere costituita da diverse identità, utilizzare l'identità speciale `ANYTHING`.

## A proposito di questa attività

All'interno di ONTAP, le identità vengono specificate modificando la voce SPD o durante la creazione del criterio SPD. Il nome SPD può essere un indirizzo IP o un nome di identità in formato stringa.

## Fase

Per modificare un'impostazione di identità SPD esistente, utilizzare il seguente comando:

```
security ipsec policy modify
```

### Comando di esempio

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity  
192.168.134.34 -remote-identity client.fooboo.com
```

### Configurazione di più client IPSec

Quando un numero limitato di client deve sfruttare IPSec, è sufficiente utilizzare una singola voce SPD per ciascun client. Tuttavia, quando centinaia o addirittura migliaia di client devono sfruttare IPSec, NetApp consiglia di utilizzare una configurazione con più client IPSec.

#### A proposito di questa attività

ONTAP supporta la connessione di più client su molte reti a un singolo indirizzo IP SVM con IPSec attivato. È possibile eseguire questa operazione utilizzando uno dei seguenti metodi:

- **Configurazione subnet**

Per consentire a tutti i client di una determinata subnet (ad esempio 192.168.134.0/24) di connettersi a un singolo indirizzo IP SVM utilizzando una singola voce di policy SPD, è necessario specificare `remote-ip-subnets` sotto forma di subnet. Inoltre, è necessario specificare `remote-identity` campo con l'identità lato client corretta.



Quando si utilizza una singola voce di criterio in una configurazione di subnet, i client IPSec in tale subnet condividono l'identità IPSec e la chiave precondivisa (PSK). Tuttavia, questo non è vero con l'autenticazione del certificato. Quando si utilizzano i certificati, ciascun client può utilizzare il proprio certificato univoco o un certificato condiviso per l'autenticazione. IPSec ONTAP verifica la validità del certificato in base alle CA installate nel relativo archivio di attendibilità locale. ONTAP supporta anche il controllo dell'elenco di revocche di certificati (CRL).

- **Consenti configurazione di tutti i client**

Per consentire a qualsiasi client, indipendentemente dall'indirizzo IP di origine, di connettersi all'indirizzo IP SVM abilitato a IPSec, utilizzare `0.0.0.0/0` carattere jolly quando si specifica `remote-ip-subnets` campo.

Inoltre, è necessario specificare `remote-identity` campo con l'identità lato client corretta. Per l'autenticazione del certificato, è possibile immettere `ANYTHING`.

Inoltre, quando `0.0.0.0/0` se si utilizza il carattere jolly, è necessario configurare un numero di porta locale o remota specifico da utilizzare. Ad esempio, `NFS port 2049`.

#### Fasi

a. Utilizzare uno dei seguenti comandi per configurare IPSec per più client.

i. Se si utilizza la **configurazione della subnet** per supportare più client IPSec:

```
security ipsec policy create -vserver vserver_name -name policy_name  
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets  
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

### Comando di esempio

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

- i. Se si utilizza l'opzione **Allow all clients Configuration** (Consenti configurazione di tutti i client) per supportare più client IPsec:

```
security ipsec policy create -vserver vserver_name -name policy_name
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
-ports port_number -local-identity local_id -remote-identity remote_id
```

### Comando di esempio

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

## Statistiche IPsec

Attraverso la negoziazione, è possibile stabilire un canale di sicurezza denominato SA (IKE Security Association) tra l'indirizzo IP di ONTAP SVM e l'indirizzo IP del client. I SAS IPsec vengono installati su entrambi gli endpoint per eseguire le operazioni di crittografia e decrittografia dei dati.

È possibile utilizzare i comandi delle statistiche per controllare lo stato di IPsec SAS e IKE SAS.

### Comandi di esempio

Comando di esempio IKE SA:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Comando e output di esempio SA IPsec:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
```

Vserver	Policy Name	Local Address	Remote Address	Initiator-SPI	State
vs1	test34	192.168.134.34	192.168.134.44	c764f9ee020cec69	ESTABLISHED

Comando e output di esempio SA IPsec:

```
security ipsec show-ipseca -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipseca -node cluster1-node1
      Policy  Local          Remote          Inbound  Outbound
Vserver  Name    Address          Address          SPI      SPI
State
-----
-----
vs1      test34
          192.168.134.34  192.168.134.44  c4c5b3d6  c2515559
INSTALLED
```

## Configurare le policy firewall per le LIF

La configurazione di un firewall migliora la sicurezza del cluster e impedisce l'accesso non autorizzato al sistema di storage. Per impostazione predefinita, il firewall integrato è configurato in modo da consentire l'accesso remoto a un set specifico di servizi IP per le LIF di dati, gestione e intercluster.

A partire da ONTAP 9.10.1:

- Le policy firewall sono obsolete e vengono sostituite dalle policy di servizio LIF. In precedenza, il firewall integrato era gestito tramite policy firewall. Questa funzionalità viene ora eseguita utilizzando una policy di servizio LIF.
- Tutti i criteri firewall sono vuoti e non aprono porte nel firewall sottostante. Tutte le porte devono invece essere aperte utilizzando una policy di servizio LIF.
- Non è richiesta alcuna azione dopo un aggiornamento alla versione 9.10.1 o successiva per passare dalle policy firewall alle policy di servizio LIF. Il sistema crea automaticamente policy di servizio LIF coerenti con le policy firewall in uso nella release precedente di ONTAP. Se si utilizzano script o altri strumenti che creano e gestiscono policy firewall personalizzate, potrebbe essere necessario aggiornare tali script per creare policy di servizio personalizzate.

Per ulteriori informazioni, vedere ["LIF e policy di servizio in ONTAP 9.6 e versioni successive"](#).

Le policy firewall possono essere utilizzate per controllare l'accesso ai protocolli dei servizi di gestione come SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPs, RSH, DNS o SNMP. Non è possibile impostare policy firewall per protocolli dati come NFS o SMB.

È possibile gestire il servizio firewall e le policy nei seguenti modi:

- Attivazione o disattivazione del servizio firewall
- Visualizzazione della configurazione corrente del servizio firewall
- Creazione di un nuovo criterio firewall con il nome del criterio e i servizi di rete specificati
- Applicazione di un criterio firewall a un'interfaccia logica
- Creazione di una nuova policy firewall che sia una copia esatta di una policy esistente

È possibile utilizzare questa opzione per creare una policy con caratteristiche simili all'interno della stessa

SVM o per copiare la policy su una SVM diversa.

- Visualizzazione di informazioni sui criteri firewall
- Modifica degli indirizzi IP e delle netmask utilizzati da una policy firewall
- Eliminazione di una policy firewall non utilizzata da una LIF

## Policy firewall e LIF

I criteri firewall LIF vengono utilizzati per limitare l'accesso al cluster su ogni LIF. È necessario comprendere in che modo la policy firewall predefinita influenza l'accesso al sistema su ciascun tipo di LIF e come è possibile personalizzare una policy firewall per aumentare o ridurre la sicurezza su una LIF.

Durante la configurazione di un LIF utilizzando `network interface create` oppure `network interface modify` il valore specificato per `-firewall-policy` Il parametro determina i protocolli di servizio e gli indirizzi IP ai quali è consentito l'accesso a LIF.

In molti casi è possibile accettare il valore predefinito del criterio firewall. In altri casi, potrebbe essere necessario limitare l'accesso a determinati indirizzi IP e a determinati protocolli dei servizi di gestione. I protocolli dei servizi di gestione disponibili includono SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS E SNMP.

Per impostazione predefinita, il criterio firewall per tutte le LIF del cluster è "" e non possono essere modificati.

La tabella seguente descrive i criteri firewall predefiniti assegnati a ciascun LIF, in base al ruolo (ONTAP 9.5 e versioni precedenti) o ai criteri di servizio (ONTAP 9.6 e versioni successive), quando si crea il LIF:

Policy del firewall	Protocolli di servizio predefiniti	Accesso predefinito	LIF applicati a.
gestione	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Qualsiasi indirizzo (0.0.0.0/0)	Gestione del cluster, gestione SVM e LIF di gestione dei nodi
mgmt-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Qualsiasi indirizzo (0.0.0.0/0)	Le LIF dei dati che supportano anche l'accesso alla gestione SVM
intercluster	https, ndmp, ndmps	Qualsiasi indirizzo (0.0.0.0/0)	Tutti i LIF intercluster
dati	dns, ndmp, ndmps, portmap	Qualsiasi indirizzo (0.0.0.0/0)	Tutti i dati LIF

## Configurazione del servizio portmap

Il servizio portmap associa i servizi RPC alle porte su cui sono in ascolto.

Il servizio portmap era sempre accessibile in ONTAP 9.3 e versioni precedenti, è diventato configurabile in ONTAP 9.4 fino a ONTAP 9.6 e viene gestito automaticamente a partire da ONTAP 9.7.



- In ONTAP 9.3 e versioni precedenti, il servizio portmap (rpcbind) era sempre accessibile sulla porta 111 nelle configurazioni di rete che si basavano sul firewall ONTAP integrato anziché su un firewall di terze parti.
- Da ONTAP 9.4 a ONTAP 9.6, è possibile modificare i criteri del firewall per controllare se il servizio portmap è accessibile su specifiche LIF.
- A partire da ONTAP 9.7, il servizio firewall portmap viene eliminato. La porta portmap viene invece aperta automaticamente per tutti i LIF che supportano il servizio NFS.

## **Il servizio Portmap è configurabile nel firewall in ONTAP 9.4 fino a ONTAP 9.6.**

Il resto di questo argomento illustra come configurare il servizio firewall portmap per le versioni da ONTAP 9.4 a ONTAP 9.6.

A seconda della configurazione, potrebbe essere possibile non consentire l'accesso al servizio su specifici tipi di LIF, in genere LIF di gestione e di intercluster. In alcuni casi, potresti persino essere in grado di impedire l'accesso alle LIF dei dati.

### **Quale comportamento ci si può aspettare**

Il comportamento da ONTAP 9.4 a ONTAP 9.6 è progettato per fornire una transizione perfetta all'aggiornamento. Se si accede già al servizio portmap su specifici tipi di LIF, questo continuerà ad essere accessibile attraverso questi tipi di LIF. Come in ONTAP 9.3 e versioni precedenti, nella policy di firewall per il tipo di LIF è possibile specificare i servizi a cui accedere.

Tutti i nodi del cluster devono eseguire ONTAP 9.4 fino a ONTAP 9.6 per rendere effettivo il comportamento. Viene influenzato solo il traffico in entrata.

Le nuove regole sono le seguenti:

- All'aggiornamento alla versione 9.4 fino alla 9.6, ONTAP aggiunge il servizio portmap a tutte le policy firewall esistenti, predefinite o personalizzate.
- Quando si crea un nuovo cluster o un nuovo IPspace, ONTAP aggiunge il servizio portmap solo al criterio dati predefinito, non ai criteri di gestione predefiniti o di intercluster.
- È possibile aggiungere il servizio portmap alle policy predefinite o personalizzate in base alle necessità e rimuovere il servizio in base alle necessità.

### **Come aggiungere o rimuovere il servizio portmap**

Per aggiungere il servizio portmap a una policy SVM o del firewall del cluster (renderlo accessibile all'interno del firewall), immettere:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Per rimuovere il servizio portmap da una policy SVM o del firewall del cluster (rendendolo inaccessibile all'interno del firewall), immettere:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

È possibile utilizzare il comando di modifica dell'interfaccia di rete per applicare il criterio firewall a una LIF esistente. Per la sintassi completa dei comandi, vedere ["Comandi di ONTAP 9"](#).

## Creare una policy firewall e assegnarla a una LIF

I criteri firewall predefiniti vengono assegnati a ciascun LIF quando si crea il LIF. In molti casi, le impostazioni predefinite del firewall funzionano correttamente e non è necessario modificarle. Se si desidera modificare i servizi di rete o gli indirizzi IP che possono accedere a una LIF, è possibile creare una policy firewall personalizzata e assegnarla alla LIF.

### A proposito di questa attività

- Non è possibile creare un criterio firewall con `policy` nome `data`, `intercluster`, `cluster`, o `mgmt`.

Questi valori sono riservati ai criteri firewall definiti dal sistema.

- Non è possibile impostare o modificare un criterio firewall per le LIF del cluster.

Il criterio del firewall per le LIF del cluster è impostato su 0.0.0.0/0 per tutti i tipi di servizi.

- Se è necessario rimuovere un servizio da un criterio, è necessario eliminare il criterio firewall esistente e crearne uno nuovo.
- Se IPv6 è attivato nel cluster, è possibile creare policy firewall con indirizzi IPv6.

Dopo aver attivato IPv6, `data`, `intercluster`, e `mgmt` I criteri firewall includono `::/0`, il carattere jolly IPv6, nell'elenco degli indirizzi accettati.

- Quando si utilizza System Manager per configurare la funzionalità di protezione dei dati tra cluster, è necessario assicurarsi che gli indirizzi IP LIF tra cluster siano inclusi nell'elenco consentito e che il servizio HTTPS sia consentito sia per le LIF tra cluster che per i firewall di proprietà dell'azienda.

Per impostazione predefinita, il `intercluster` La policy firewall consente l'accesso da tutti gli indirizzi IP (0.0.0.0/0, o `::/0` per IPv6) e abilita i servizi HTTPS, NDMP e NDMPs. Se si modifica questo criterio predefinito o si crea un criterio firewall personalizzato per le LIF tra cluster, è necessario aggiungere ciascun indirizzo IP LIF tra cluster all'elenco consentito e attivare il servizio HTTPS.

- A partire da ONTAP 9.6, i servizi firewall HTTPS e SSH non sono supportati.

In ONTAP 9.6, il `management-https` e `management-ssh` I servizi LIF sono disponibili per l'accesso alla gestione HTTPS e SSH.

### Fasi

1. Creare una policy firewall che sarà disponibile per i LIF su una SVM specifica:

```
system services firewall policy create -vserver vservice_name -policy
policy_name -service network_service -allow-list ip_address/mask
```

È possibile utilizzare questo comando più volte per aggiungere più di un servizio di rete e un elenco di indirizzi IP consentiti per ciascun servizio nella policy del firewall.

2. Verificare che il criterio sia stato aggiunto correttamente utilizzando `system services firewall policy show` comando.
3. Applicare il criterio firewall a una LIF:

```
network interface modify -vserver vservice_name -lif lif_name -firewall-policy
policy_name
```

4. Verificare che il criterio sia stato aggiunto correttamente alla LIF utilizzando `network interface show -fields firewall-policy` comando.

#### **Esempio di creazione e applicazione di un criterio firewall a una LIF**

Il seguente comando crea una policy firewall denominata `data_http` che abilita l'accesso ai protocolli HTTP e HTTPS dagli indirizzi IP sulla subnet 10.10, applica tale policy alla LIF denominata `data1` su SVM `vs1`, quindi mostra tutte le policy firewall sul cluster:

```
system services firewall policy create -vserver vs1 -policy data_http  
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show
```

Vserver	Policy	Service	Allowed
-----	-----	-----	-----
cluster-1			
	data		
		dns	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1			
	intercluster		
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
cluster-1			
	mgmt		
		dns	0.0.0.0/0
		http	0.0.0.0/0
		https	0.0.0.0/0
		ndmp	0.0.0.0/0
		ndmps	0.0.0.0/0
		ntp	0.0.0.0/0
		snmp	0.0.0.0/0
		ssh	0.0.0.0/0
vs1			
	data_http		
		http	10.10.0.0/16
		https	10.10.0.0/16

```
network interface modify -vserver vs1 -lif data1 -firewall-policy  
data_http
```

```
network interface show -fields firewall-policy
```

vserver	lif	firewall-policy
-----	-----	-----
Cluster	node1_clus_1	
Cluster	node1_clus_2	
Cluster	node2_clus_1	
Cluster	node2_clus_2	
cluster-1	cluster_mgmt	mgmt
cluster-1	node1_mgmt1	mgmt
cluster-1	node2_mgmt1	mgmt
vs1	data1	data_http
vs3	data2	data

## Comandi per la gestione del servizio firewall e delle policy

È possibile utilizzare `system services firewall` comandi per la gestione del servizio firewall, il `system services firewall policy` comandi per la gestione delle policy firewall e di `network interface modify` Comando per gestire le impostazioni del firewall per le LIF.

Se si desidera...	Utilizzare questo comando...
Attiva o disattiva il servizio firewall	<code>system services firewall modify</code>
Visualizza la configurazione corrente per il servizio firewall	<code>system services firewall show</code>
Creare una policy firewall o aggiungere un servizio a una policy firewall esistente	<code>system services firewall policy create</code>
Applicare un criterio firewall a una LIF	<code>network interface modify -lif lifname -firewall-policy</code>
Modificare gli indirizzi IP e le netmask associate a un criterio firewall	<code>system services firewall policy modify</code>
Visualizza informazioni sui criteri firewall	<code>system services firewall policy show</code>
Creare una nuova policy firewall che sia una copia esatta di una policy esistente	<code>system services firewall policy clone</code>
Eliminare una policy firewall non utilizzata da una LIF	<code>system services firewall policy delete</code>

Per ulteriori informazioni, consultare le pagine man del `system services firewall`, `system services firewall policy`, e `network interface modify` comandi in ["Comandi di ONTAP 9"](#).

## Contrassegno QoS (solo amministratori del cluster)

### Panoramica sulla QoS

Il contrassegno della qualità del servizio (QoS) di rete consente di assegnare priorità a diversi tipi di traffico in base alle condizioni della rete per utilizzare in modo efficace le risorse di rete. È possibile impostare il valore DSCP (differenziate Services code point) dei pacchetti IP in uscita per i tipi di traffico supportati per IPspace.

### Marcatura DSCP per la conformità UC

È possibile attivare il contrassegno DSCP (differenziate Services code point) sul traffico dei pacchetti IP in uscita (in uscita) per un determinato protocollo con un codice DSCP predefinito o fornito dall'utente. Il contrassegno DSCP è un meccanismo per la classificazione e la gestione del traffico di rete ed è un

componente della conformità UC (Unified Capability).

La marcatura DSCP (nota anche come *marcatura QoS* o *marcatura della qualità del servizio*) viene attivata fornendo un valore IPspace, protocollo e DSCP. I protocolli su cui è possibile applicare il contrassegno DSCP sono NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet e SNMP.

Se non si fornisce un valore DSCP quando si attiva la marcatura DSCP per un determinato protocollo, viene utilizzato un valore predefinito:

- Il valore predefinito per il traffico/protocolli dati è 0x0A (10).
- Il valore predefinito per i protocolli di controllo/traffico è 0x30 (48).

## Modificare i valori di marcatura QoS

È possibile modificare i valori di marcatura della qualità del servizio (QoS) per diversi protocolli, per ciascun IPspace.

### Prima di iniziare

Tutti i nodi del cluster devono eseguire la stessa versione di ONTAP.

### Fase

Modificare i valori di marcatura QoS utilizzando `network qos-marking modify` comando.

- Il `-ipSpace` Parameter (parametro) specifica l'IPspace per cui la voce di marcatura QoS deve essere modificata.
- Il `-protocol` Parametro specifica il protocollo per cui la voce di marcatura QoS deve essere modificata. Il `network qos-marking modify` la pagina man descrive i possibili valori del protocollo.
- Il `-dscp` Il parametro specifica il valore DSCP (Differentiated Services Code Point). I valori possibili vanno da 0 a 63.
- Il `-is-enabled` Il parametro viene utilizzato per attivare o disattivare il contrassegno QoS per il protocollo specificato nell'IPspace fornito da `-ipSpace` parametro.

Il seguente comando attiva il contrassegno QoS per il protocollo NFS nell'IPspace predefinito:

```
network qos-marking modify -ipSpace Default -protocol NFS -is-enabled true
```

Il seguente comando imposta il valore DSCP su 20 per il protocollo NFS nell'IPspace predefinito:

```
network qos-marking modify -ipSpace Default -protocol NFS -dscp 20
```

## Visualizzare i valori di marcatura QoS

È possibile visualizzare i valori di marcatura QoS per diversi protocolli, per ciascun IPspace.

### Fase

Visualizzare i valori di marcatura QoS utilizzando `network qos-marking show` comando.

Il seguente comando visualizza il contrassegno QoS per tutti i protocolli nell'IPSpace predefinito:

```
network qos-marking show -ipspace Default
IPspace          Protocol          DSCP    Enabled?
-----
Default
                CIFS              10      false
                FTP              48      false
                HTTP-admin       48      false
                HTTP-filesrv     10      false
                NDMP             10      false
                NFS              10      true
                SNMP            48      false
                SSH              48      false
                SnapMirror       10      false
                Telnet           48      false
                iSCSI            10      false

11 entries were displayed.
```

## Gestione SNMP (solo amministratori cluster)

### Panoramica SNMP

È possibile configurare SNMP per monitorare le SVM nel cluster per evitare i problemi prima che si verifichino e per rispondere ai problemi in caso di verificarsi. La gestione di SNMP implica la configurazione degli utenti SNMP e la configurazione delle destinazioni SNMP traphost (workstation di gestione) per tutti gli eventi SNMP. SNMP è disattivato per impostazione predefinita nei file LIF dei dati.

È possibile creare e gestire utenti SNMP di sola lettura nella SVM dei dati. Le LIF dei dati devono essere configurate per ricevere richieste SNMP su SVM.

Le workstation o i manager di gestione della rete SNMP possono richiedere informazioni all'agente SNMP SVM. L'agente SNMP raccoglie le informazioni e le inoltra ai gestori SNMP. L'agente SNMP genera inoltre notifiche trap ogni volta che si verificano eventi specifici. L'agente SNMP sulla SVM dispone di privilegi di sola lettura; non può essere utilizzato per operazioni impostate o per intraprendere un'azione correttiva in risposta a una trap. ONTAP fornisce un agente SNMP compatibile con le versioni SNMP v1, v2c e v3. SNMPv3 offre sicurezza avanzata utilizzando passphrase e crittografia.

Per ulteriori informazioni sul supporto SNMP nei sistemi ONTAP, vedere ["TR-4220: Supporto SNMP in Data ONTAP"](#).

### Panoramica MIB

Un MIB (Management Information base) è un file di testo che descrive oggetti e trap SNMP.

I MIB descrivono la struttura dei dati di gestione del sistema di storage e utilizzano uno spazio dei nomi gerarchico contenente OID (Object Identifier). Ogni OID identifica una variabile che può essere letta utilizzando

## SNMP.

Poiché i MIB non sono file di configurazione e ONTAP non legge questi file, la funzionalità SNMP non viene influenzata dai MIB. ONTAP fornisce il seguente file MIB:

- Una MIB personalizzata di NetApp (`netapp.mib`)

ONTAP supporta i MIB IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) e ICMP (RFC 2466), che mostrano sia i dati IPv4 che IPv6.

ONTAP fornisce inoltre un breve riferimento incrociato tra gli OID (Object Identifier) e i nomi brevi degli oggetti in `traps.dat` file.



Le versioni più recenti dei MIB e dei file `traps.dat` di ONTAP sono disponibili sul sito del supporto NetApp. Tuttavia, le versioni di questi file sul sito di supporto non corrispondono necessariamente alle funzionalità SNMP della versione di ONTAP in uso. Questi file vengono forniti per agevolare la valutazione delle funzionalità SNMP nella versione più recente di ONTAP.

## Trap SNMP

I trap SNMP acquisiscono le informazioni di monitoraggio del sistema inviate come notifica asincrona dall'agente SNMP al gestore SNMP.

Esistono tre tipi di trap SNMP: Standard, incorporato e definito dall'utente. I trap definiti dall'utente non sono supportati in ONTAP.

È possibile utilizzare una trap per controllare periodicamente le soglie operative o gli errori definiti nella MIB. Se viene raggiunta una soglia o viene rilevato un errore, l'agente SNMP invia un messaggio (trap) ai traphost che li avvisano dell'evento.



ONTAP supporta i trap SNMPv1 e, avviando ONTAP 9.1, i trap SNMPv3. ONTAP non supporta i trap SNMPv2c e informa.

## Trap SNMP standard

Questi trap sono definiti in RFC 1215. ONTAP supporta cinque trap SNMP standard: Coldstart, warmStart, linkGiù, linkup e AuthenticationFailure.



Il trap AuthenticationFailure è disattivato per impostazione predefinita. È necessario utilizzare `system snmp authtrap` per attivare il trap. Per ulteriori informazioni, consulta le pagine man: "[Comandi di ONTAP 9](#)"

## Trap SNMP integrati

I trap integrati sono predefiniti in ONTAP e vengono inviati automaticamente alle stazioni di gestione di rete presenti nell'elenco degli host trapezoidali in caso di evento. Questi trap, come `diskFailedShutdown`, `cpuTooBusy` e `volumeNearlyFull`, sono definiti nel MIB personalizzato.

Ogni trap integrato è identificato da un codice trap univoco.



## Creare una community SNMP e assegnarla a una LIF

È possibile creare una community SNMP che funga da meccanismo di autenticazione tra la stazione di gestione e la macchina virtuale di storage (SVM) quando si utilizzano SNMPv1 e SNMPv2c.

Creando community SNMP in una SVM di dati, è possibile eseguire comandi come `snmpwalk` e `snmpget` Sulle LIF dei dati.

### A proposito di questa attività

- Nelle nuove installazioni di ONTAP, SNMPv1 e SNMPv2c sono disattivati per impostazione predefinita.

SNMPv1 e SNMPv2c vengono attivati dopo la creazione di una community SNMP.

- ONTAP supporta le community di sola lettura.
- Per impostazione predefinita, il servizio SNMP è impostato su per il criterio firewall "dati" assegnato alle LIF dati `deny`.

È necessario creare un nuovo criterio firewall con il servizio SNMP impostato su `allow` Quando si crea un utente SNMP per un SVM dati.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

- È possibile creare community SNMP per gli utenti SNMPv1 e SNMPv2c sia per SVM admin che per SVM dati.
- Poiché una SVM non fa parte dello standard SNMP, le query sulle LIF dei dati devono includere l'OID root di NetApp (1.3.6.1.4.1.789), ad esempio `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

### Fasi

1. Creare una community SNMP utilizzando `system snmp community add` comando. Il seguente comando mostra come creare una community SNMP nel cluster SVM di amministrazione-1:

```
system snmp community add -type ro -community-name comty1 -vserver  
cluster-1
```

Il seguente comando mostra come creare una community SNMP nei dati SVM vs1:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Verificare che le community siano state create utilizzando il comando di visualizzazione della community `snmp` di sistema.

Il seguente comando mostra le due community create per SNMPv1 e SNMPv2c:

```

system snmp community show
cluster-1
rocomty1
vs1
rocomty2

```

3. Verificare se SNMP è consentito come servizio nella policy firewall "dati" utilizzando `system services firewall policy show` comando.

Il seguente comando indica che il servizio snmp non è consentito nella policy firewall "dati" predefinita (il servizio snmp è consentito solo nella policy firewall "mgmt"):

```

system services firewall policy show
Vserver Policy      Service      Allowed
-----
cluster-1
  data
    dns      0.0.0.0/0
    ndmp     0.0.0.0/0
    ndmps    0.0.0.0/0
cluster-1
  intercluster
    https    0.0.0.0/0
    ndmp     0.0.0.0/0
    ndmps    0.0.0.0/0
cluster-1
  mgmt
    dns      0.0.0.0/0
    http     0.0.0.0/0
    https    0.0.0.0/0
    ndmp     0.0.0.0/0
    ndmps    0.0.0.0/0
    ntp      0.0.0.0/0
    snmp     0.0.0.0/0
    ssh      0.0.0.0/0

```

4. Creare un nuovo criterio firewall che consenta l'accesso tramite snmp utilizzando `system services firewall policy create` comando.

I seguenti comandi creano una nuova policy di firewall dati denominata "data1" che consente snmp

```
system services firewall policy create -policy data1 -service snmp
-vserver vs1 -allow-list 0.0.0.0/0
```

```
cluster-1::> system services firewall policy show -service snmp
```

Vserver	Policy	Service	Allowed
-----			
cluster-1			
	mgmt		
		snmp	0.0.0.0/0
vs1			
	data1		
		snmp	0.0.0.0/0

5. Applicare il criterio firewall a una LIF dati utilizzando il comando `network interface modify` (modifica interfaccia di rete) con il parametro `-firewall-policy`.

Il seguente comando assegna il nuovo criterio firewall "data1" a "datalif1" LIF:

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

## Configurare gli utenti SNMPv3 in un cluster

SNMPv3 è un protocollo sicuro rispetto a SNMPv1 e SNMPv2c. Per utilizzare SNMPv3, è necessario configurare un utente SNMPv3 per eseguire le utility SNMP dal gestore SNMP.

### Fase

Utilizzare il "comando di creazione dell'accesso di sicurezza" per creare un utente SNMPv3.

Viene richiesto di fornire le seguenti informazioni:

- Engine ID (ID motore): Il valore predefinito e raccomandato è l'ID motore locale
- Protocollo di autenticazione
- Password di autenticazione
- Protocollo di privacy
- Password del protocollo di privacy

### Risultato

L'utente SNMPv3 può accedere dal gestore SNMP utilizzando il nome utente e la password ed eseguire i comandi dell'utility SNMP.

### Parametri di sicurezza SNMPv3

SNMPv3 include una funzionalità di autenticazione che, quando selezionata, richiede agli utenti di inserire i

propri nomi, un protocollo di autenticazione, una chiave di autenticazione e il livello di sicurezza desiderato quando si richiama un comando.

Nella tabella seguente sono elencati i parametri di protezione di SNMPv3 :

Parametro	Opzione della riga di comando	Descrizione
ID motore	-E EngineID	ID motore dell'agente SNMP. Il valore predefinito è EngineID locale (consigliato).
SecurityName	-U Nome	Il nome utente non deve superare i 32 caratteri.
AuthProtocol	-A {none	MD5
SHA	SHA-256}	Il tipo di autenticazione può essere None, MD5, SHA o SHA-256.
Chiave authkey	-UNA PASSPHRASE	Passphrase con un minimo di otto caratteri.
Livello di sicurezza	-L {authNoPriv	AuthPriv
noAuthNoPriv}	Il livello di protezione può essere autenticazione, Nessuna privacy, autenticazione, privacy o nessuna autenticazione, Nessuna privacy.	PrivProtocol
-x { none	des	aes128}
Il protocollo di privacy può essere NONE, des o aes128	PrivPassword	-X password

### Esempi di diversi livelli di sicurezza

Questo esempio mostra come un utente SNMPv3 creato con diversi livelli di sicurezza può utilizzare i comandi lato client SNMP, ad esempio `snmpwalk`, per eseguire query sugli oggetti del cluster.

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.



È necessario utilizzare `snmpwalk` 5.3.1 o versione successiva quando il protocollo di autenticazione è SHA.

### Livello di sicurezza: Authprim

Il seguente output mostra la creazione di un utente SNMPv3 con il livello di sicurezza `authprim`.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

## Modalità FIPS

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

## Test snmpwalk

Il seguente output mostra l'utente SNMPv3 che esegue il comando snmpwalk:

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## Livello di sicurezza: AuthNoPriv

Il seguente output mostra la creazione di un utente SNMPv3 con il livello di sicurezza autNoPriv.

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

## Modalità FIPS

FIPS non consente di scegliere **nessuno** per il protocollo di privacy. Di conseguenza, non è possibile configurare un utente authNoPrivat SNMPv3 in modalità FIPS.

## Test snmpwalk

Il seguente output mostra l'utente SNMPv3 che esegue il comando snmpwalk:

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1! -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## Livello di sicurezza: NoAuthNoPriv

Il seguente output mostra la creazione di un utente SNMPv3 con il livello di sicurezza noAuthNoPrimv.

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

## Modalità FIPS

FIPS non consente di scegliere **nessuno** per il protocollo di privacy.

## Test snmpwalk

Il seguente output mostra l'utente SNMPv3 che esegue il comando snmpwalk:

Per ottenere prestazioni migliori, è necessario recuperare tutti gli oggetti di una tavola anziché un singolo oggetto o pochi oggetti dalla tavola.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

## Configurare i traphost per ricevere notifiche SNMP

È possibile configurare il traphost (gestore SNMP) in modo che riceva notifiche (PDU trap SNMP) quando vengono generati trap SNMP nel cluster. È possibile specificare il nome host o l'indirizzo IP (IPv4 o IPv6) del traphost SNMP.

### Prima di iniziare

- I trap SNMP e SNMP devono essere attivati sul cluster.



I trap SNMP e SNMP sono attivati per impostazione predefinita.

- Il DNS deve essere configurato sul cluster per risolvere i nomi degli host trapezoidali.
- IPv6 deve essere attivato sul cluster per configurare i traphost SNMP utilizzando gli indirizzi IPv6.
- Per ONTAP 9.1 e versioni successive, è necessario specificare l'autenticazione di un modello di sicurezza basato sull'utente (USM) e le credenziali di privacy predefiniti durante la creazione di traphost.

### Fase

Aggiunta di un host SNMP traphost:

```
system snmp traphost add
```



I trap possono essere inviati solo quando almeno una stazione di gestione SNMP è specificata come host trapotato.

Il seguente comando aggiunge un nuovo host trapezoidale SNMPv3 denominato yyy.example.com con un utente USM noto:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

Il seguente comando aggiunge un host trapezoidale utilizzando l'indirizzo IPv6 dell'host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

## Comandi per la gestione di SNMP

È possibile utilizzare `system snmp` Comandi per gestire SNMP, trap e traphost. È possibile utilizzare `security` Comandi per gestire gli utenti SNMP per SVM. È possibile utilizzare `event` Comandi per gestire gli eventi relativi ai trap SNMP.

### Comandi per la configurazione di SNMP

Se si desidera...	Utilizzare questo comando...
Abilitare SNMP sul cluster	<code>options -option-name snmp.enable -option-value on</code>  Il servizio SNMP deve essere consentito in base alla policy firewall di gestione (mgmt). È possibile verificare se SNMP è consentito utilizzando il comando <code>show</code> del criterio firewall dei servizi di sistema.
Disattivare SNMP sul cluster	<code>options -option-name snmp.enable -option-value off</code>

### Comandi per la gestione degli utenti SNMP v1, v2c e v3

Se si desidera...	Utilizzare questo comando...
Configurare gli utenti SNMP	<code>security login create</code>
Visualizzare gli utenti SNMP	<code>security snmpusers and security login show -application snmp</code>
Eliminare gli utenti SNMP	<code>security login delete</code>
Modificare il nome del ruolo di controllo dell'accesso di un metodo di accesso per gli utenti SNMP	<code>security login modify</code>

### Comandi per fornire informazioni di contatto e posizione

Se si desidera...	Utilizzare questo comando...
Visualizzare o modificare i dettagli di contatto del cluster	<code>system snmp contact</code>
Visualizzare o modificare i dettagli della posizione del cluster	<code>system snmp location</code>



## Comandi per la gestione delle community SNMP

Se si desidera...	Utilizzare questo comando...
Aggiungere una community di sola lettura (ro) per una SVM o per tutte le SVM nel cluster	<code>system snmp community add</code>
Eliminare una community o tutte le community	<code>system snmp community delete</code>
Visualizza l'elenco di tutte le community	<code>system snmp community show</code>

Poiché le SVM non fanno parte dello standard SNMP, le query sulle LIF dei dati devono includere l'OID root di NetApp (1.3.6.1.4.1.789), ad esempio `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

## Comando per la visualizzazione dei valori delle opzioni SNMP

Se si desidera...	Utilizzare questo comando...
Visualizza i valori correnti di tutte le opzioni SNMP, inclusi il contatto del cluster, la posizione del contatto, se il cluster è configurato per l'invio di trap, l'elenco dei traphost, l'elenco delle community e il tipo di controllo degli accessi	<code>system snmp show</code>

## Comandi per la gestione di trap SNMP e traphosts

Se si desidera...	Utilizzare questo comando...
Abilitare i trap SNMP inviati dal cluster	<code>system snmp init -init 1</code>
Disattiva i trap SNMP inviati dal cluster	<code>system snmp init -init 0</code>
Aggiungere un host trapotato che riceve notifiche SNMP per eventi specifici nel cluster	<code>system snmp traphost add</code>
Eliminare un host trapezoidale	<code>system snmp traphost delete</code>
Visualizza l'elenco di traphosts	<code>system snmp traphost show</code>

## Comandi per la gestione degli eventi relativi ai trap SNMP

Se si desidera...	Utilizzare questo comando...
-------------------	------------------------------

Visualizza gli eventi per i quali vengono generati i trap SNMP (integrati)	<pre>event route show</pre> <p>Utilizzare <code>-snmp-support true</code> Parametro per visualizzare solo gli eventi relativi a SNMP.</p> <p>Utilizzare <code>instance -messagename &lt;message&gt;</code> parametro per visualizzare una descrizione dettagliata del motivo per cui si è verificato un evento e di eventuali azioni correttive.</p> <p>Il routing di singoli eventi trap SNMP a destinazioni host trapotate specifiche non è supportato. Tutti gli eventi trap SNMP vengono inviati a tutte le destinazioni dell'host trapotato.</p>
Visualizza un elenco di record della cronologia delle trap SNMP, che sono notifiche di eventi inviate alle trap SNMP	<pre>event snmphistory show</pre>
Eliminare un record di cronologia trap SNMP	<pre>event snmphistory delete</pre>

Per ulteriori informazioni su `system snmp`, `security`, e. `event` comandi, vedere le pagine man: ["Comandi di ONTAP 9"](#)

## Gestire il routing in una SVM

### Panoramica dell'instradamento delle SVM

La tabella di routing per una SVM determina il percorso di rete utilizzato dalla SVM per comunicare con una destinazione. È importante comprendere il funzionamento delle tabelle di routing in modo da prevenire i problemi di rete prima che si verifichino.

Le regole di routing sono le seguenti:

- ONTAP instrada il traffico sul percorso più specifico disponibile.
- ONTAP instrada il traffico su un percorso di gateway predefinito (con 0 bit di netmask) come ultima risorsa, quando non sono disponibili percorsi più specifici.

Nel caso di percorsi con la stessa destinazione, netmask e metrica, non vi è alcuna garanzia che il sistema utilizzi lo stesso percorso dopo un riavvio o un aggiornamento. Questo è un problema soprattutto se sono stati configurati più percorsi predefiniti.

Si consiglia di configurare un percorso predefinito solo per una SVM. Per evitare interruzioni, assicurarsi che il percorso predefinito sia in grado di raggiungere qualsiasi indirizzo di rete non raggiungibile da un percorso più specifico. Per ulteriori informazioni, consulta l'articolo della Knowledge base ["SU134: L'accesso alla rete potrebbe essere interrotto da una configurazione di routing errata in Clustered ONTAP"](#)

## Creare un percorso statico

È possibile creare percorsi statici all'interno di una macchina virtuale di storage (SVM) per controllare il modo in cui i LIF utilizzano la rete per il traffico in uscita.

Quando si crea una voce di percorso associata a una SVM, la route viene utilizzata da tutte le LIF di proprietà della SVM specificata e che si trovano sulla stessa sottorete del gateway.

### Fase

Utilizzare `network route create` per creare un percorso.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

## Abilitare il routing multipath

Se più percorsi hanno la stessa metrica per una destinazione, viene selezionato solo uno dei percorsi per il traffico in uscita. Ciò comporta la mancata utilizzo di altri percorsi per l'invio del traffico in uscita. È possibile abilitare il routing multipath per il bilanciamento del carico e utilizzare tutti i percorsi disponibili.

### Fasi

1. Accedere al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Abilita routing multipath:

```
network options multipath-routing modify -is-enabled true
```

Il routing multipath è abilitato per tutti i nodi nel cluster.

```
network options multipath-routing modify -is-enabled true
```

## Eliminare un percorso statico

È possibile eliminare un percorso statico non necessario da una SVM (Storage Virtual Machine).

### Fase

Utilizzare `network route delete` comando per eliminare un percorso statico.

Per ulteriori informazioni su questo comando, vedere `network route` pagina man: ["Comandi di ONTAP 9"](#).

Nell'esempio seguente viene eliminata una route statica associata a SVM vs0 con un gateway 10.63.0.1 e un indirizzo IP di destinazione 0.0.0.0/0:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

## Visualizzare le informazioni di routing

È possibile visualizzare informazioni sulla configurazione di routing per ogni SVM nel cluster. In questo modo è possibile diagnosticare i problemi di routing che comportano problemi di connettività tra applicazioni o servizi client e una LIF su un nodo del cluster.

### Fasi

1. Utilizzare `network route show` Comando per visualizzare i percorsi all'interno di una o più SVM. L'esempio seguente mostra un percorso configurato in SVM vs0:

```
network route show
(network route show)
Vserver          Destination      Gateway          Metric
-----
vs0
                0.0.0.0/0      172.17.178.1    20
```

2. Utilizzare `network route show-lifs` Comando per visualizzare l'associazione di route e LIF all'interno di una o più SVM.

L'esempio seguente mostra i file LIF con route di proprietà di vs0 SVM:

```
network route show-lifs
(network route show-lifs)

Vserver: vs0
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        172.17.178.1    cluster_mgmt,
                  LIF-b-01_mgmt1,
                  LIF-b-02_mgmt1
```

3. Utilizzare `network route active-entry show` Comando per visualizzare i percorsi installati su uno o più nodi, SVM, subnet o percorsi con destinazioni specifiche.

L'esempio seguente mostra tutti i percorsi installati su una SVM specifica:

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
```

Subnet Group: 0.0.0.0/0

Destination	Gateway	Interface	Metric	Flags
127.0.0.1	127.0.0.1	lo	10	UHS
127.0.10.1	127.0.20.1	losk	10	UHS
127.0.20.1	127.0.20.1	losk	10	UHS

Vserver: Data0

Node: node-1

Subnet Group: fd20:8b1e:b255:814e::/64

Destination	Gateway	Interface	Metric	Flags
default	fd20:8b1e:b255:814e::1	e0d	20	UGS
fd20:8b1e:b255:814e::/64	link#4	e0d	0	UC

Vserver: Data0

Node: node-2

Subnet Group: 0.0.0.0/0

Destination	Gateway	Interface	Metric	Flags
127.0.0.1	127.0.0.1	lo	10	UHS

Vserver: Data0

Node: node-2

Subnet Group: 0.0.0.0/0

Destination	Gateway	Interface	Metric	Flags
127.0.10.1	127.0.20.1	losk	10	UHS
127.0.20.1	127.0.20.1	losk	10	UHS

Vserver: Data0

Node: node-2

Subnet Group: fd20:8b1e:b255:814e::/64

Destination	Gateway	Interface	Metric	Flags
default	fd20:8b1e:b255:814e::1	e0d	20	UGS
fd20:8b1e:b255:814e::/64	link#4	e0d	0	UC
fd20:8b1e:b255:814e::1	link#4	e0d	0	UHL

11 entries were displayed.

## Rimuovere i percorsi dinamici dalle tabelle di routing

Quando si ricevono i reindirizzamenti ICMP per IPv4 e IPv6, i percorsi dinamici vengono aggiunti alla tabella di routing. Per impostazione predefinita, i percorsi dinamici vengono rimossi dopo 300 secondi. Se si desidera mantenere percorsi dinamici per un periodo di tempo diverso, è possibile modificare il valore di timeout.

### A proposito di questa attività

È possibile impostare il valore di timeout da 0 a 65,535 secondi. Se si imposta il valore su 0, i percorsi non scadono mai. La rimozione di percorsi dinamici impedisce la perdita di connettività causata dalla persistenza di percorsi non validi.

### Fasi

1. Visualizza il valore di timeout corrente.

◦ Per IPv4:

```
network tuning icmp show
```

◦ Per IPv6:

```
network tuning icmp6 show
```

2. Modificare il valore di timeout.

◦ Per IPv4:

```
network tuning icmp modify -node node_name -redirect-timeout  
timeout_value
```

◦ Per IPv6:

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout  
timeout_value
```

3. Verificare che il valore di timeout sia stato modificato correttamente.

◦ Per IPv4:

```
network tuning icmp show
```

◦ Per IPv6:

```
network tuning icmp6 show
```

# Visualizzare le informazioni di rete

## Visualizzare la panoramica delle informazioni di rete

Utilizzando la CLI, puoi visualizzare informazioni relative a porte, LIF, percorsi, regole di failover, gruppi di failover, regole firewall, DNS, NIS e connessioni. A partire da ONTAP 9,8, è anche possibile scaricare i dati visualizzati in Gestione sistema relativi alla rete.

Queste informazioni possono essere utili in situazioni come la riconfigurazione delle impostazioni di rete o la risoluzione dei problemi del cluster.

Gli amministratori del cluster possono visualizzare tutte le informazioni di rete disponibili. Gli amministratori di SVM possono visualizzare solo le informazioni relative alle SVM assegnate.

In System Manager, quando si visualizzano le informazioni in una vista *List*, è possibile fare clic su **Download** e l'elenco degli oggetti visualizzati viene scaricato.

- L'elenco viene scaricato in formato CSV (comma-separated values).
- Vengono scaricati solo i dati nelle colonne visibili.
- Il nome del file CSV viene formattato con il nome dell'oggetto e l'indicazione dell'ora.

## Visualizza le informazioni sulla porta di rete

È possibile visualizzare informazioni su una porta specifica o su tutte le porte di tutti i nodi del cluster.

### A proposito di questa attività

Vengono visualizzate le seguenti informazioni:

- Nome del nodo
- Nome della porta
- Nome IPspace
- Nome di dominio di trasmissione
- Stato del collegamento (verso l'alto o verso il basso)
- Impostazione MTU
- Impostazione della velocità della porta e stato operativo (1 Gigabit o 10 Gigabit al secondo)
- Impostazione della negoziazione automatica (vero o falso)
- Modalità duplex e stato operativo (metà o pieno)
- Il gruppo di interfaccia della porta, se applicabile
- Le informazioni del tag VLAN della porta, se applicabile
- Lo stato di salute della porta (stato di salute o degradato)
- Motivi per cui una porta viene contrassegnata come degradata

Se i dati di un campo non sono disponibili (ad esempio, il duplex operativo e la velocità di una porta inattiva non sarebbero disponibili), il valore del campo viene elencato come –.

Fase

Visualizzare le informazioni sulla porta di rete utilizzando `network port show` comando.

È possibile visualizzare informazioni dettagliate per ciascuna porta specificando `-instance` o ottenere informazioni specifiche specificando i nomi dei campi utilizzando `-fields` parametro.

```
network port show
Node: node1

Ignore
Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
-----
-----
e0a Cluster Cluster up 9000 auto/1000 healthy
false
e0b Cluster Cluster up 9000 auto/1000 healthy
false
e0c Default Default up 1500 auto/1000 degraded
false
e0d Default Default up 1500 auto/1000 degraded
true
Node: node2

Ignore
Speed(Mbps) Health
Health
Port IPspace Broadcast Domain Link MTU Admin/Oper Status
Status
-----
-----
e0a Cluster Cluster up 9000 auto/1000 healthy
false
e0b Cluster Cluster up 9000 auto/1000 healthy
false
e0c Default Default up 1500 auto/1000 healthy
false
e0d Default Default up 1500 auto/1000 healthy
false
8 entries were displayed.
```



## Visualizzazione delle informazioni su una VLAN (solo amministratori del cluster)

È possibile visualizzare informazioni su una VLAN specifica o su tutte le VLAN del cluster.

### A proposito di questa attività

È possibile visualizzare informazioni dettagliate per ciascuna VLAN specificando `-instance` parametro. È possibile visualizzare informazioni specifiche specificando i nomi dei campi utilizzando `-fields` parametro.

### Fase

Visualizzare le informazioni sulle VLAN utilizzando `network port vlan show` comando. Il seguente comando visualizza le informazioni su tutte le VLAN nel cluster:

```
network port vlan show
```

Node	VLAN Name	Port	Network VLAN ID	Network MAC Address
cluster-1-01				
	a0a-10	a0a	10	02:a0:98:06:10:b2
	a0a-20	a0a	20	02:a0:98:06:10:b2
	a0a-30	a0a	30	02:a0:98:06:10:b2
	a0a-40	a0a	40	02:a0:98:06:10:b2
	a0a-50	a0a	50	02:a0:98:06:10:b2
cluster-1-02				
	a0a-10	a0a	10	02:a0:98:06:10:ca
	a0a-20	a0a	20	02:a0:98:06:10:ca
	a0a-30	a0a	30	02:a0:98:06:10:ca
	a0a-40	a0a	40	02:a0:98:06:10:ca
	a0a-50	a0a	50	02:a0:98:06:10:ca

## Visualizza informazioni sul gruppo di interfacce (solo amministratori del cluster)

È possibile visualizzare informazioni su un gruppo di interfacce per determinarne la configurazione.

### A proposito di questa attività

Vengono visualizzate le seguenti informazioni:

- Nodo su cui si trova il gruppo di interfacce
- Elenco delle porte di rete incluse nel gruppo di interfacce
- Nome del gruppo di interfacce
- Funzione di distribuzione (MAC, IP, porta o sequenziale)
- Indirizzo MAC (Media Access Control) del gruppo di interfacce
- Stato di attività della porta, ovvero se tutte le porte aggregate sono attive (partecipazione completa), se alcune sono attive (partecipazione parziale) o se nessuna è attiva

## Fase

Visualizzare le informazioni sui gruppi di interfacce utilizzando `network port ifgrp show` comando.

È possibile visualizzare informazioni dettagliate per ciascun nodo specificando `-instance` parametro. È possibile visualizzare informazioni specifiche specificando i nomi dei campi utilizzando `-fields` parametro.

Il seguente comando visualizza le informazioni relative a tutti i gruppi di interfacce nel cluster:

```
network port ifgrp show
```

Node	Port IfGrp	Distribution Function	MAC Address	Active Ports	Ports
cluster-1-01	a0a	ip	02:a0:98:06:10:b2	full	e7a, e7b
cluster-1-02	a0a	sequential	02:a0:98:06:10:ca	full	e7a, e7b
cluster-1-03	a0a	port	02:a0:98:08:5b:66	full	e7a, e7b
cluster-1-04	a0a	mac	02:a0:98:08:61:4e	full	e7a, e7b

Il seguente comando visualizza informazioni dettagliate sul gruppo di interfacce per un singolo nodo:

```
network port ifgrp show -instance -node cluster-1-01
```

```
Node: cluster-1-01
Interface Group Name: a0a
Distribution Function: ip
Create Policy: multimode
MAC Address: 02:a0:98:06:10:b2
Port Participation: full
Network Ports: e7a, e7b
Up Ports: e7a, e7b
Down Ports: -
```

## Visualizzare le informazioni LIF

È possibile visualizzare informazioni dettagliate su una LIF per determinarne la configurazione.

È inoltre possibile visualizzare queste informazioni per diagnosticare i problemi LIF di base, ad esempio la ricerca di indirizzi IP duplicati o la verifica dell'appartenenza della porta di rete alla subnet corretta. Gli amministratori delle macchine virtuali di storage (SVM) possono visualizzare solo le informazioni relative alle LIF associate a SVM.

### A proposito di questa attività

Vengono visualizzate le seguenti informazioni:

- Indirizzo IP associato al LIF
- Stato amministrativo della LIF
- Stato operativo del LIF

Lo stato operativo delle LIF dei dati è determinato dallo stato delle SVM a cui sono associate le LIF dei dati. Quando la SVM viene arrestata, lo stato operativo della LIF diventa inattivo. Quando SVM viene riavviato, lo stato operativo diventa up

- E la porta su cui risiede LIF

Se i dati di un campo non sono disponibili (ad esempio, se non sono presenti informazioni estese sullo stato), il valore del campo viene elencato come –.

### **Fase**

Visualizzare le informazioni LIF utilizzando il comando show dell'interfaccia di rete.

È possibile visualizzare informazioni dettagliate per ciascun LIF specificando il parametro -instance oppure ottenere informazioni specifiche specificando i nomi dei campi utilizzando il parametro -fields.

Il seguente comando visualizza informazioni generali su tutte le LIF in un cluster:

# network interface show

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
example					
	lif1	up/up	192.0.2.129/22	node-01	e0d
false					
node	cluster_mgmt	up/up	192.0.2.3/20	node-02	e0c
false					
node-01	clus1	up/up	192.0.2.65/18	node-01	e0a
true					
	clus2	up/up	192.0.2.66/18	node-01	e0b
true					
	mgmt1	up/up	192.0.2.1/20	node-01	e0c
true					
node-02	clus1	up/up	192.0.2.67/18	node-02	e0a
true					
	clus2	up/up	192.0.2.68/18	node-02	e0b
true					
	mgmt2	up/up	192.0.2.2/20	node-02	e0d
true					
vs1	d1	up/up	192.0.2.130/21	node-01	e0d
false					
	d2	up/up	192.0.2.131/21	node-01	e0d
true					
	data3	up/up	192.0.2.132/20	node-02	e0c
true					

Il seguente comando mostra informazioni dettagliate su una singola LIF:

```
network interface show -lif data1 -instance

Vserver Name: vs1
Logical Interface Name: data1
Role: data
Data Protocol: nfs,cifs
Home Node: node-01
Home Port: e0c
Current Node: node-03
Current Port: e0c
Operational Status: up
Extended Status: -
Is Home: false
Network Address: 192.0.2.128
Netmask: 255.255.192.0
Bits in the Netmask: 18
IPv4 Link Local: -
Subnet Name: -
Administrative Status: up
Failover Policy: local-only
Firewall Policy: data
Auto Revert: false
Fully Qualified DNS Zone Name: xxx.example.com
DNS Query Listen Enable: false
Failover Group Name: Default
FCP WWPN: -
Address family: ipv4
Comment: -
IPspace of LIF: Default
```

Visualizzare le informazioni di routing

È possibile visualizzare informazioni sui percorsi all'interno di una SVM.

Fase

A seconda del tipo di informazioni di routing che si desidera visualizzare, immettere il comando appropriato:

Per visualizzare informazioni su...	Inserisci...
Percorsi statici, per SVM	network route show
LIF su ogni percorso, per SVM	network route show-lifs

È possibile visualizzare informazioni dettagliate per ciascun percorso specificando `-instance` parametro. Il seguente comando visualizza i percorsi statici all'interno delle SVM nel cluster 1:

```
network route show
Vserver          Destination      Gateway          Metric
-----
Cluster
0.0.0.0/0        10.63.0.1       10
cluster-1
0.0.0.0/0        198.51.9.1      10
vs1
0.0.0.0/0        192.0.2.1       20
vs3
0.0.0.0/0        192.0.2.1       20
```

Il seguente comando visualizza l'associazione di route statiche e interfacce logiche (LIFF) in tutte le SVM nel cluster-1:

```
network route show-lifs
Vserver: Cluster
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        10.63.0.1       -

Vserver: cluster-1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        198.51.9.1      cluster_mgmt,
cluster-1_mgmt1,

Vserver: vs1
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data1_1, data1_2

Vserver: vs3
Destination      Gateway          Logical Interfaces
-----
0.0.0.0/0        192.0.2.1       data2_1, data2_2
```

## Visualizzare le voci della tabella degli host DNS (solo amministratori del cluster)

Le voci della tabella host DNS associano i nomi host agli indirizzi IP. È possibile visualizzare i nomi host, gli alias e l'indirizzo IP a cui mappano tutte le SVM in un cluster.

## Fase

Visualizzare le voci del nome host per tutte le SVM utilizzando il comando `show` degli host dns dei servizi vserver.

Nell'esempio seguente vengono visualizzate le voci della tabella host:

```
vserver services name-service dns hosts show
Vserver      Address      Hostname      Aliases
-----
cluster-1
10.72.219.36  lnx219-36    -
vs1
10.72.219.37  lnx219-37    lnx219-37.example.com
```

È possibile utilizzare `vserver services name-service dns` Per abilitare il DNS su una SVM e configurarlo per l'utilizzo del DNS per la risoluzione dei nomi host. I nomi host vengono risolti utilizzando server DNS esterni.

## Visualizzare le configurazioni del dominio DNS

È possibile visualizzare la configurazione del dominio DNS di una o più macchine virtuali di storage (SVM) nel cluster per verificare che sia configurata correttamente.

## Fase

Visualizzazione delle configurazioni del dominio DNS mediante `vserver services name-service dns show` comando.

Il seguente comando visualizza le configurazioni DNS per tutte le SVM nel cluster:

```
vserver services name-service dns show
Vserver      State      Domains      Name
-----
cluster-1    enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs1          enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs2          enabled    xyz.company.com  192.56.0.129,
192.56.0.130
vs3          enabled    xyz.company.com  192.56.0.129,
192.56.0.130
```

Il seguente comando visualizza informazioni dettagliate sulla configurazione DNS per SVM vs1:

```
vserver services name-service dns show -vserver vs1
      Vserver: vs1
      Domains: xyz.company.com
      Name Servers: 192.56.0.129, 192.56.0.130
      Enable/Disable DNS: enabled
      Timeout (secs): 2
      Maximum Attempts: 1
```

## Visualizzare le informazioni sui gruppi di failover

È possibile visualizzare informazioni sui gruppi di failover, tra cui l'elenco di nodi e porte in ciascun gruppo di failover, se il failover è attivato o disattivato e il tipo di policy di failover che viene applicata a ciascuna LIF.

### Fasi

1. Visualizzare le porte di destinazione per ciascun gruppo di failover utilizzando `network interface failover-groups show` comando.

Il seguente comando visualizza le informazioni su tutti i gruppi di failover su un cluster a due nodi:

```
network interface failover-groups show
      Vserver      Group      Failover
      -----
      Cluster
      vs1          Cluster
                        cluster1-01:e0a, cluster1-01:e0b,
                        cluster1-02:e0a, cluster1-02:e0b
      vs1          Default
                        cluster1-01:e0c, cluster1-01:e0d,
                        cluster1-01:e0e, cluster1-02:e0c,
                        cluster1-02:e0d, cluster1-02:e0e
```

2. Visualizzare le porte di destinazione e il dominio di trasmissione per uno specifico gruppo di failover utilizzando `network interface failover-groups show` comando.

Il seguente comando visualizza informazioni dettagliate sui dati del gruppo di failover 12 per SVM vs4:



```
network interface failover-groups show -vserver vs4 -failover-group data12
```

```
Vserver Name: vs4
Failover Group Name: data12
Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                  cluster1-02:e0g
Broadcast Domain: Default
```

3. Visualizzare le impostazioni di failover utilizzate da tutti i file LIF utilizzando `network interface show` comando.

Il seguente comando visualizza il criterio di failover e il gruppo di failover utilizzati da ciascun LIF:

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver    lif                failover-policy    failover-group
-----
Cluster    cluster1-01_clus_1    local-only         Cluster
Cluster    cluster1-01_clus_2    local-only         Cluster
Cluster    cluster1-02_clus_1    local-only         Cluster
Cluster    cluster1-02_clus_2    local-only         Cluster
cluster1    cluster_mgmt          broadcast-domain-wide Default
cluster1    cluster1-01_mgmt1     local-only         Default
cluster1    cluster1-02_mgmt1     local-only         Default
vs1         data1                 disabled           Default
vs3         data2                 system-defined     group2
```

## Visualizzare le destinazioni di failover LIF

Potrebbe essere necessario controllare se i criteri di failover e i gruppi di failover di una LIF sono configurati correttamente. Per evitare una configurazione errata delle regole di failover, è possibile visualizzare le destinazioni di failover per una singola LIF o per tutte le LIF.

### A proposito di questa attività

La visualizzazione delle destinazioni di failover LIF consente di verificare quanto segue:

- Se le LIF sono configurate con il gruppo di failover e la policy di failover corretti
- Se l'elenco risultante di porte di destinazione di failover è appropriato per ogni LIF
- Se la destinazione di failover di una LIF dati non è una porta di gestione (e0M)

### Fase

Visualizzare le destinazioni di failover di una LIF utilizzando `failover` opzione di `network interface`

show comando.

Il seguente comando visualizza le informazioni sulle destinazioni di failover per tutte le LIF in un cluster a due nodi. Il Failover Targets Riga mostra l'elenco (con priorità) delle combinazioni nodo-porta per un dato LIF.

```
network interface show -failover

      Logical      Home      Failover      Failover
Vserver Interface  Node:Port      Policy      Group
-----
Cluster
      node1_clus1  node1:e0a      local-only      Cluster
                        Failover Targets: node1:e0a,
                        node1:e0b
      node1_clus2  node1:e0b      local-only      Cluster
                        Failover Targets: node1:e0b,
                        node1:e0a
      node2_clus1  node2:e0a      local-only      Cluster
                        Failover Targets: node2:e0a,
                        node2:e0b
      node2_clus2  node2:e0b      local-only      Cluster
                        Failover Targets: node2:e0b,
                        node2:e0a
cluster1
      cluster_mgmt node1:e0c      broadcast-domain-wide
                        Default
                        Failover Targets: node1:e0c,
                        node1:e0d,
                        node2:e0c,
                        node2:e0d
      node1_mgmt1  node1:e0c      local-only      Default
                        Failover Targets: node1:e0c,
                        node1:e0d
      node2_mgmt1  node2:e0c      local-only      Default
                        Failover Targets: node2:e0c,
                        node2:e0d
vs1
      data1        node1:e0e      system-defined  bcast1
                        Failover Targets: node1:e0e,
                        node1:e0f,
                        node2:e0e,
                        node2:e0f
```

## Visualizzare i LIF in una zona di bilanciamento del carico

È possibile verificare se una zona di bilanciamento del carico è configurata correttamente visualizzando tutte le LIF ad essa associate. È inoltre possibile visualizzare la zona di

bilanciamento del carico di una LIF specifica o le zone di bilanciamento del carico per tutte le LIF.

Fase

Visualizzare i LIF e i dettagli del bilanciamento del carico desiderati utilizzando uno dei seguenti comandi

Per visualizzare...	Inserisci...
LIF in una particolare zona di bilanciamento del carico	<code>network interface show -dns-zone zone_name</code>  <code>zone_name</code> specifica il nome della zona di bilanciamento del carico.
La zona di bilanciamento del carico di una LIF specifica	<code>network interface show -lif lif_name -fields dns-zone</code>
Le zone di bilanciamento del carico di tutte le LIF	<code>network interface show -fields dns-zone</code>

Esempi di visualizzazione delle zone di bilanciamento del carico per le LIF

Il seguente comando visualizza i dettagli di tutte le LIF nella zona di bilanciamento del carico `storage.company.com` per SVM `vs0`:

```
net int show -vserver vs0 -dns-zone storage.company.com
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs0	lif3	up/up	10.98.226.225/20	ndeux-11	e0c	true
	lif4	up/up	10.98.224.23/20	ndeux-21	e0c	true
	lif5	up/up	10.98.239.65/20	ndeux-11	e0c	true
	lif6	up/up	10.98.239.66/20	ndeux-11	e0c	true
	lif7	up/up	10.98.239.63/20	ndeux-21	e0c	true
	lif8	up/up	10.98.239.64/20	ndeux-21	e0c	true

Il seguente comando visualizza i dettagli della zona DNS dei dati LIF 3:

```
network interface show -lif data3 -fields dns-zone
```

Vserver	lif	dns-zone
vs0	data3	storage.company.com

Il seguente comando visualizza l'elenco di tutte le LIF del cluster e delle relative zone DNS:

```
network interface show -fields dns-zone
Vserver    lif          dns-zone
-----
cluster    cluster_mgmt none
ndeux-21   clus1        none
ndeux-21   clus2        none
ndeux-21   mgmt1        none
vs0        data1        storage.company.com
vs0        data2        storage.company.com
```

## Visualizzare le connessioni del cluster

È possibile visualizzare tutte le connessioni attive nel cluster o un numero di connessioni attive sul nodo in base al client, all'interfaccia logica, al protocollo o al servizio. È inoltre possibile visualizzare tutte le connessioni in ascolto nel cluster.

### Visualizza le connessioni attive per client (solo amministratori del cluster)

È possibile visualizzare le connessioni attive per client per verificare il nodo utilizzato da un client specifico e per visualizzare eventuali squilibri tra i conteggi dei client per nodo.

#### A proposito di questa attività

Il numero di connessioni attive per client è utile nei seguenti scenari:

- Ricerca di un nodo occupato o sovraccarico.
- Determinare il motivo per cui l'accesso di un determinato client a un volume è lento.

È possibile visualizzare i dettagli sul nodo a cui il client sta accedendo e confrontarlo con il nodo su cui risiede il volume. Se l'accesso al volume richiede l'attraversamento della rete del cluster, i client potrebbero riscontrare una riduzione delle performance a causa dell'accesso remoto al volume su un nodo remoto oversubsd.

- Verificare che tutti i nodi siano utilizzati allo stesso modo per l'accesso ai dati.
- Ricerca di client con un numero inaspettatamente elevato di connessioni.
- Verificare se alcuni client dispongono di connessioni a un nodo.

#### Fase

Visualizzare il numero delle connessioni attive per client su un nodo utilizzando `network connections active show-clients` comando.

Per ulteriori informazioni su questo comando, consulta la pagina man: ["Comandi di ONTAP 9"](#)

```

network connections active show-clients
Node      Vserver Name      Client IP Address      Count
-----
node0     vs0                192.0.2.253            1
          vs0                192.0.2.252            2
          Cluster        192.10.2.124           5
node1     vs0                192.0.2.250            1
          vs0                192.0.2.252            3
          Cluster        192.10.2.123           4
node2     vs1                customer.example.com    1
          vs1                192.0.2.245            3
          Cluster        192.10.2.122           4
node3     vs1                customer.example.org    1
          vs1                customer.example.net    3
          Cluster        192.10.2.121           4

```

### Visualizzazione delle connessioni attive in base al protocollo (solo amministratori del cluster)

È possibile visualizzare un numero di connessioni attive in base al protocollo (TCP o UDP) su un nodo per confrontare l'utilizzo dei protocolli all'interno del cluster.

#### A proposito di questa attività

Il numero di connessioni attive per protocollo è utile nei seguenti scenari:

- Individuazione dei client UDP che perdono la connessione.

Se un nodo si trova vicino al limite di connessione, i client UDP sono i primi a essere ignorati.

- Verificare che non vengano utilizzati altri protocolli.

#### Fase

Visualizzare il numero delle connessioni attive in base al protocollo su un nodo utilizzando `network connections active show-protocols` comando.

Per ulteriori informazioni su questo comando, vedere la pagina `man`.

```

network connections active show-protocols
Node      Vserver Name  Protocol  Count
-----
node0
      vs0      UDP      19
      Cluster  TCP      11
node1
      vs0      UDP      17
      Cluster  TCP      8
node2
      vs1      UDP      14
      Cluster  TCP      10
node3
      vs1      UDP      18
      Cluster  TCP      4

```

### Visualizzazione delle connessioni attive per servizio (solo amministratori del cluster)

È possibile visualizzare un numero di connessioni attive in base al tipo di servizio (ad esempio, per NFS, SMB, mount e così via) per ciascun nodo di un cluster. Ciò è utile per confrontare l'utilizzo dei servizi all'interno del cluster, che consente di determinare il carico di lavoro primario di un nodo.

#### A proposito di questa attività

Il numero di connessioni attive per servizio è utile nei seguenti scenari:

- Verifica dell'utilizzo di tutti i nodi per i servizi appropriati e del corretto funzionamento del bilanciamento del carico per tale servizio.
- Verificare che non vengano utilizzati altri servizi. Visualizzare il numero delle connessioni attive per servizio su un nodo utilizzando `network connections active show-services` comando.

Per ulteriori informazioni su questo comando, consulta la pagina man: ["Comandi di ONTAP 9"](#)

```

network connections active show-services
Node      Vserver Name      Service      Count
-----
node0
    vs0          mount          3
    vs0          nfs            14
    vs0          nlm_v4         4
    vs0          cifs_srv       3
    vs0          port_map       18
    vs0          rclopcp        27
    Cluster      ctlopcp        60
node1
    vs0          cifs_srv       3
    vs0          rclopcp        16
    Cluster      ctlopcp        60
node2
    vs1          rclopcp        13
    Cluster      ctlopcp        60
node3
    vs1          cifs_srv       1
    vs1          rclopcp        17
    Cluster      ctlopcp        60

```

## Visualizza le connessioni attive per LIF su un nodo e SVM

È possibile visualizzare un numero di connessioni attive per ciascuna LIF, per nodo e SVM (Storage Virtual Machine), per visualizzare gli squilibri di connessione tra le LIF all'interno del cluster.

### A proposito di questa attività

Il numero di connessioni attive per LIF è utile nei seguenti scenari:

- Trovare un LIF sovraccarico confrontando il numero di connessioni su ciascun LIF.
- Verifica del corretto funzionamento del bilanciamento del carico DNS per tutti i file LIF dei dati.
- Confrontando il numero di connessioni con le varie SVM per individuare le SVM più utilizzate.

### Fase

Visualizzare un numero di connessioni attive per ciascun LIF in base a SVM e nodo utilizzando `network connections active show-lifs` comando.

Per ulteriori informazioni su questo comando, consulta la pagina man: ["Comandi di ONTAP 9"](#)

```

network connections active show-lifs
Node      Vserver Name  Interface Name  Count
-----
node0
    vs0        datalif1        3
    Cluster    node0_clus_1    6
    Cluster    node0_clus_2    5
node1
    vs0        datalif2        3
    Cluster    node1_clus_1    3
    Cluster    node1_clus_2    5
node2
    vs1        datalif2        1
    Cluster    node2_clus_1    5
    Cluster    node2_clus_2    3
node3
    vs1        datalif1        1
    Cluster    node3_clus_1    2
    Cluster    node3_clus_2    2

```

## Visualizzare le connessioni attive in un cluster

È possibile visualizzare informazioni sulle connessioni attive in un cluster per visualizzare LIF, porta, host remoto, servizio, macchine virtuali di storage (SVM) e protocollo utilizzati dalle singole connessioni.

### A proposito di questa attività

La visualizzazione delle connessioni attive in un cluster è utile nei seguenti scenari:

- Verificare che i singoli client utilizzino il protocollo e il servizio corretti sul nodo corretto.
- Se un client ha problemi ad accedere ai dati utilizzando una determinata combinazione di nodo, protocollo e servizio, è possibile utilizzare questo comando per trovare un client simile per la configurazione o il confronto delle tracce dei pacchetti.

### Fase

Visualizzare le connessioni attive in un cluster utilizzando `network connections active show` comando.

Per ulteriori informazioni su questo comando, consulta la pagina man: ["Comandi di ONTAP 9"](#)

Il seguente comando mostra le connessioni attive sul nodo node1:



```
network connections active show -node node1
```

Vserver	Interface	Remote	
Name	Name:Local Port	Host:Port	Protocol/Service
-----	-----	-----	-----
Node: node1			
Cluster	node1_clus_1:50297	192.0.2.253:7700	TCP/ctlopcp
Cluster	node1_clus_1:13387	192.0.2.253:7700	TCP/ctlopcp
Cluster	node1_clus_1:8340	192.0.2.252:7700	TCP/ctlopcp
Cluster	node1_clus_1:42766	192.0.2.252:7700	TCP/ctlopcp
Cluster	node1_clus_1:36119	192.0.2.250:7700	TCP/ctlopcp
vs1	data1:111	host1.aa.com:10741	UDP/port-map
vs3	data2:111	host1.aa.com:10741	UDP/port-map
vs1	data1:111	host1.aa.com:12017	UDP/port-map
vs3	data2:111	host1.aa.com:12017	UDP/port-map

Il seguente comando mostra le connessioni attive su SVM vs1:

```
network connections active show -vserver vs1
```

Vserver	Interface	Remote	
Name	Name:Local Port	Host:Port	Protocol/Service
-----	-----	-----	-----
Node: node1			
vs1	data1:111	host1.aa.com:10741	UDP/port-map
vs1	data1:111	host1.aa.com:12017	UDP/port-map

## Visualizzare le connessioni in ascolto in un cluster

È possibile visualizzare le informazioni relative alle connessioni in ascolto in un cluster per visualizzare le LIF e le porte che accettano le connessioni per un determinato protocollo e servizio.

### A proposito di questa attività

La visualizzazione delle connessioni in ascolto in un cluster è utile nei seguenti scenari:

- Verificare che il protocollo o il servizio desiderato sia in ascolto su una LIF se le connessioni del client a tale LIF non riescono in modo coerente.
- Verifica dell'apertura di un listener UDP/rclopcp in ogni LIF del cluster in caso di errore dell'accesso remoto ai dati di un volume su un nodo tramite LIF su un altro nodo.
- Verifica dell'apertura di un listener UDP/rclopcp in ogni LIF del cluster se i trasferimenti SnapMirror tra due nodi nello stesso cluster non funzionano.
- Verifica dell'apertura di un listener TCP/ctlopcp in ogni LIF di intercluster se i trasferimenti SnapMirror tra due nodi in cluster diversi non riescono.

### Fase

Visualizzare le connessioni in ascolto per nodo utilizzando `network connections listening show` comando.

```

network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: node0
Cluster           node0_clus_1:7700              TCP/ctlopcp
vs1               data1:4049                    UDP/unknown
vs1               data1:111                     TCP/port-map
vs1               data1:111                     UDP/port-map
vs1               data1:4046                    TCP/sm
vs1               data1:4046                    UDP/sm
vs1               data1:4045                    TCP/nlm-v4
vs1               data1:4045                    UDP/nlm-v4
vs1               data1:2049                    TCP/nfs
vs1               data1:2049                    UDP/nfs
vs1               data1:635                     TCP/mount
vs1               data1:635                     UDP/mount
Cluster           node0_clus_2:7700              TCP/ctlopcp

```

## Comandi per la diagnosi dei problemi di rete

È possibile diagnosticare i problemi sulla rete utilizzando comandi come `ping`, `traceroute`, `ndp`, e `tcpdump`. È inoltre possibile utilizzare comandi come `ping6` e `traceroute6` Per diagnosticare i problemi IPv6.

Se si desidera...	Immettere questo comando...
Verificare se il nodo può raggiungere altri host sulla rete	<code>network ping</code>
Verificare se il nodo può raggiungere altri host sulla rete IPv6	<code>network ping6</code>
Tracciare il percorso che i pacchetti IPv4 portano a un nodo di rete	<code>network traceroute</code>
Tracciare il percorso che i pacchetti IPv6 portano a un nodo di rete	<code>network traceroute6</code>
Gestire il protocollo NDP (Neighbor Discovery Protocol)	<code>network ndp</code>
Visualizza le statistiche relative ai pacchetti ricevuti e inviati su un'interfaccia di rete specifica o su tutte le interfacce di rete	<code>run -node <i>node_name</i> ifstat</code> <b>Nota:</b> Questo comando è disponibile dal nodeshell.
Visualizza le informazioni sui dispositivi vicini rilevati da ciascun nodo e porta del cluster, inclusi il tipo di dispositivo remoto e la piattaforma del dispositivo	<code>network device-discovery show</code>

Visualizzare i CDP vicini al nodo (ONTAP supporta solo annunci CDPv1)	<code>run -node <i>node_name</i> cdpd show-neighbors</code> <b>Nota:</b> Questo comando è disponibile dal nodeshell.
Tracciare i pacchetti inviati e ricevuti nella rete	<code>network tcpdump start -node <i>node-name</i> -port <i>port_name</i></code> <b>Nota:</b> Questo comando è disponibile dal nodeshell.
Misurare la latenza e il throughput tra nodi intercluster o intracluster	<code>`network test -path -source-node <i>source_nodename</i> local -destination-cluster <i>destination_clustername</i> -destination-node <i>destination_nodename</i> -session -type <i>Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer</i></code> Per ulteriori informazioni, consultare <a href="#">"Gestione delle performance"</a> .

Per ulteriori informazioni su questi comandi, consulta le pagine man appropriate: ["Comandi di ONTAP 9"](#)

## Visualizzare la connettività di rete con i protocolli di rilevamento neighbor

### Visualizzare la connettività di rete con i protocolli di rilevamento neighbor

In un data center, è possibile utilizzare i protocolli neighbor Discovery per visualizzare la connettività di rete tra una coppia di sistemi fisici o virtuali e le relative interfacce di rete. ONTAP supporta due protocolli di rilevamento neighbor: Protocollo di rilevamento Cisco (CDP) e protocollo di rilevamento link Layer (LLDP).

I protocolli neighbor Discovery consentono di rilevare e visualizzare automaticamente informazioni sui dispositivi abilitati al protocollo collegati direttamente in una rete. Ogni dispositivo comunica informazioni di identificazione, funzionalità e connettività. Queste informazioni vengono trasmesse in frame Ethernet a un indirizzo MAC multicast e vengono ricevute da tutti i dispositivi abilitati per il protocollo vicini.

Affinché due dispositivi diventino vicini, ciascuno deve avere un protocollo abilitato e configurato correttamente. La funzionalità del protocollo di rilevamento è limitata alle reti direttamente connesse. I dispositivi adiacenti possono includere dispositivi abilitati al protocollo, come switch, router, bridge e così via. ONTAP supporta due protocolli di rilevamento neighbor, che possono essere utilizzati singolarmente o insieme.

### Cisco Discovery Protocol (CDP)

CDP è un protocollo di link Layer proprietario sviluppato da Cisco Systems. È attivato per impostazione predefinita in ONTAP per le porte del cluster, ma deve essere attivato esplicitamente per le porte dati.

### Link Layer Discovery Protocol (LLDP)

LLDP è un protocollo indipendente dal vendor specificato nel documento standard IEEE 802.1AB. Deve essere attivato esplicitamente per tutte le porte.

### Utilizzare CDP per rilevare la connettività di rete

L'utilizzo di CDP per rilevare la connettività di rete consiste nell'esaminare le considerazioni di implementazione, abilitarla sulle porte dati, visualizzare i dispositivi adiacenti e regolare i valori di configurazione CDP in base alle necessità. CDP è attivato per impostazione predefinita sulle porte del cluster.

Per poter visualizzare le informazioni relative ai dispositivi adiacenti, è necessario abilitare il protocollo CDP anche su switch e router.

Release di ONTAP	Descrizione
9.10.1 e versioni precedenti	Il CDP viene utilizzato anche dal monitor di stato dello switch del cluster per rilevare automaticamente gli switch del cluster e della rete di gestione.
9.11.1 e versioni successive	Il CDP viene utilizzato anche dal monitor di stato dello switch del cluster per rilevare automaticamente gli switch di cluster, storage e rete di gestione.

### Informazioni correlate

["Amministrazione del sistema"](#)

### Considerazioni sull'utilizzo di CDP

Per impostazione predefinita, i dispositivi compatibili con CDP inviano annunci CDPv2. I dispositivi conformi a CDP inviano annunci CDPv1 solo quando ricevono annunci CDPv1. ONTAP supporta solo CDPv1. Pertanto, quando un nodo ONTAP invia annunci CDPv1, i dispositivi adiacenti conformi a CDP restituiscono annunci CDPv1.

Prima di attivare CDP su un nodo, è necessario prendere in considerazione le seguenti informazioni:

- CDP è supportato per tutte le porte.
- Gli annunci CDP vengono inviati e ricevuti dalle porte in stato attivo.
- Per inviare e ricevere annunci CDP, è necessario attivare CDP sia sui dispositivi trasmittenti che su quelli riceventi.
- Gli annunci CDP vengono inviati a intervalli regolari ed è possibile configurare l'intervallo di tempo.
- Quando gli indirizzi IP vengono modificati per un LIF, il nodo invia le informazioni aggiornate nel successivo annuncio CDP.
- ONTAP 9.10.1 e versioni precedenti:
  - CDP è sempre attivato sulle porte del cluster.
  - CDP è disattivato, per impostazione predefinita, su tutte le porte non cluster.
- ONTAP 9.11.1 e versioni successive:
  - CDP è sempre abilitato sulle porte del cluster e dello storage.
  - CDP è disattivato, per impostazione predefinita, su tutte le porte non cluster e non storage.



A volte, quando i LIF vengono modificati sul nodo, le informazioni CDP non vengono aggiornate sul lato del dispositivo ricevente (ad esempio, uno switch). In caso di problemi di questo tipo, configurare l'interfaccia di rete del nodo sullo stato inattivo e quindi su.

- Solo gli indirizzi IPv4 vengono pubblicizzati negli annunci CDP.
- Per le porte di rete fisiche con VLAN, vengono annunciate tutte le LIF configurate sulle VLAN su tale porta.
- Per le porte fisiche che fanno parte di un gruppo di interfacce, tutti gli indirizzi IP configurati su quel gruppo di interfacce vengono annunciati su ciascuna porta fisica.
- Per un gruppo di interfacce che ospita VLAN, tutte le LIF configurate sul gruppo di interfacce e le VLAN vengono pubblicizzate su ciascuna porta di rete.

- Poiché i pacchetti CDP sono limitati a non più di 1500 byte, sulle porte configurate con un elevato numero di LIF è possibile che sullo switch adiacente venga riportato solo un sottoinsieme di questi indirizzi IP.

### Attiva o disattiva CDP

Per rilevare e inviare annunci pubblicitari a dispositivi adiacenti conformi a CDP, è necessario attivare CDP su ciascun nodo del cluster.

Per impostazione predefinita in ONTAP 9.10.1 e versioni precedenti, CDP è attivato su tutte le porte cluster di un nodo e disattivato su tutte le porte non cluster di un nodo.

Per impostazione predefinita, in ONTAP 9.11.1 e versioni successive, CDP viene attivato su tutte le porte di cluster e storage di un nodo e disattivato su tutte le porte non di cluster e non di storage di un nodo.

### A proposito di questa attività

Il `cdpd.enable` L'opzione controlla se CDP è attivato o disattivato sulle porte di un nodo:

- Per ONTAP 9.10.1 e versioni precedenti, ON attiva CDP su porte non cluster.
- Per ONTAP 9.11.1 e versioni successive, on attiva CDP su porte non cluster e non storage.
- Per ONTAP 9.10.1 e versioni precedenti, Off disattiva il CDP sulle porte non cluster; non è possibile disattivare il CDP sulle porte cluster.
- Per ONTAP 9.11.1 e versioni successive, Off disattiva il CDP sulle porte non cluster e non storage; non è possibile disattivare il CDP sulle porte cluster.

Quando CDP è disattivato su una porta collegata a un dispositivo conforme a CDP, il traffico di rete potrebbe non essere ottimizzato.

### Fasi

1. Visualizza l'impostazione CDP corrente per un nodo o per tutti i nodi di un cluster:

Per visualizzare l'impostazione CDP di...	Inserisci...
Un nodo	<code>run - node &lt;node_name&gt; options cdpd.enable</code>
Tutti i nodi di un cluster	<code>options cdpd.enable</code>

2. Abilitare o disabilitare CDP su tutte le porte di un nodo o su tutte le porte di tutti i nodi di un cluster:

Per attivare o disattivare CDP on...	Inserisci...
Un nodo	<code>run -node node_name options cdpd.enable {on or off}</code>
Tutti i nodi di un cluster	<code>options cdpd.enable {on or off}</code>

### Visualizzare le informazioni CDP neighbor

È possibile visualizzare informazioni sui dispositivi vicini collegati a ciascuna porta dei nodi del cluster, a

condizione che la porta sia collegata a un dispositivo conforme a CDP. È possibile utilizzare `network device-discovery show -protocol cdp` per visualizzare le informazioni sui vicini.

**A proposito di questa attività**

In ONTAP 9.10.1 e versioni precedenti, poiché CDP è sempre abilitato per le porte del cluster, le informazioni CDP neighbor vengono sempre visualizzate per tali porte. Il CDP deve essere attivato sulle porte non del cluster per visualizzare le informazioni sulle porte vicine.

In ONTAP 9.11.1 e versioni successive, poiché CDP è sempre abilitato per le porte del cluster e dello storage, le informazioni relative alle porte CDP adiacenti vengono sempre visualizzate per tali porte. Il CDP deve essere attivato sulle porte non cluster e non storage per visualizzare le informazioni sulle porte vicine.

**Fase**

Visualizza informazioni su tutti i dispositivi compatibili con CDP collegati alle porte di un nodo del cluster:

```
network device-discovery show -node node -protocol cdp
```

Il seguente comando mostra i vicini collegati alle porte sul nodo sti2650-212:

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/          Local   Discovered
Protocol       Port    Device (LLDP: ChassisID)  Interface      Platform
-----
sti2650-212/cdp
                e0M      RTP-LF810-510K37.gdl.eng.netapp.com (SAL1942R8JS)
                                Ethernet1/14    N9K-
C93120TX
                e0a      CS:RTP-CS01-510K35        0/8            CN1610
                e0b      CS:RTP-CS01-510K36        0/8            CN1610
                e0c      RTP-LF350-510K34.gdl.eng.netapp.com (FDO21521S76)
                                Ethernet1/21    N9K-
C93180YC-FX
                e0d      RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                Ethernet1/22    N9K-
C93180YC-FX
                e0e      RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                Ethernet1/23    N9K-
C93180YC-FX
                e0f      RTP-LF349-510K33.gdl.eng.netapp.com (FDO21521S4T)
                                Ethernet1/24    N9K-
C93180YC-FX
```

L'output elenca i dispositivi Cisco collegati a ciascuna porta del nodo specificato.

## Configurare il tempo di attesa per i messaggi CDP

Il tempo di attesa è il periodo di tempo durante il quale gli annunci CDP vengono memorizzati nella cache nelle periferiche compatibili con CDP adiacenti. Il tempo di attesa viene pubblicizzato in ciascun pacchetto CDPv1 e viene aggiornato ogni volta che un pacchetto CDPv1 viene ricevuto da un nodo.

- Il valore di `cdpd.holdtime` L'opzione deve essere impostata sullo stesso valore su entrambi i nodi di una coppia ha.
- Il valore predefinito del tempo di attesa è 180 secondi, ma è possibile immettere valori compresi tra 10 secondi e 255 secondi.
- Se un indirizzo IP viene rimosso prima della scadenza del tempo di attesa, le informazioni CDP vengono memorizzate nella cache fino alla scadenza del tempo di attesa.

### Fasi

1. Visualizza il tempo di attesa CDP corrente per un nodo o per tutti i nodi di un cluster:

Per visualizzare il tempo di attesa di...	Inserisci...
Un nodo	<code>run -node node_name options cdpd.holdtime</code>
Tutti i nodi di un cluster	<code>options cdpd.holdtime</code>

2. Configurare il tempo di attesa CDP su tutte le porte di un nodo o su tutte le porte di tutti i nodi di un cluster:

Per impostare il tempo di attesa su...	Inserisci...
Un nodo	<code>run -node node_name options cdpd.holdtime holdtime</code>
Tutti i nodi di un cluster	<code>options cdpd.holdtime holdtime</code>

## Impostare l'intervallo per l'invio di annunci CDP

Gli annunci CDP vengono inviati ai vicini CDP a intervalli periodici. È possibile aumentare o ridurre l'intervallo per l'invio di annunci CDP in base al traffico di rete e alle modifiche della topologia di rete.

- Il valore di `cdpd.interval` L'opzione deve essere impostata sullo stesso valore su entrambi i nodi di una coppia ha.
- L'intervallo predefinito è 60 secondi, ma è possibile immettere un valore compreso tra 5 secondi e 900 secondi.

### Fasi

1. Visualizza l'intervallo di tempo corrente per l'annuncio CDP per un nodo o per tutti i nodi di un cluster:

Per visualizzare l'intervallo per...	Inserisci...
--------------------------------------	--------------

Un nodo	<code>run -node node_name options cdpd.interval</code>
Tutti i nodi di un cluster	<code>options cdpd.interval</code>

2. Configurare l'intervallo per l'invio di annunci CDP per tutte le porte di un nodo o per tutte le porte di tutti i nodi di un cluster:

Per impostare l'intervallo per...	Inserisci...
Un nodo	<code>run -node node_name options cdpd.interval interval</code>
Tutti i nodi di un cluster	<code>options cdpd.interval interval</code>

### Visualizzare o cancellare le statistiche CDP

È possibile visualizzare le statistiche CDP per il cluster e le porte non del cluster su ciascun nodo per rilevare potenziali problemi di connettività di rete. Le statistiche CDP sono cumulative rispetto all'ultima cancellazione.

#### A proposito di questa attività

In ONTAP 9.10.1 e versioni precedenti, poiché CDP è sempre abilitato per le porte, le statistiche CDP vengono sempre visualizzate per il traffico su tali porte. Il CDP deve essere attivato sulle porte per visualizzare le statistiche relative a tali porte.

In ONTAP 9.11.1 e versioni successive, poiché CDP è sempre abilitato per le porte di cluster e storage, le statistiche CDP vengono sempre visualizzate per il traffico su tali porte. Il CDP deve essere attivato su porte non cluster o non storage per visualizzare le statistiche relative a tali porte.

#### Fase

Visualizzare o cancellare le statistiche CDP correnti per tutte le porte su un nodo:

Se si desidera...	Inserisci...
Visualizzare le statistiche CDP	<code>run -node node_name cdpd show-stats</code>
Cancellare le statistiche CDP	<code>run -node node_name cdpd zero-stats</code>

### Esempio di visualizzazione e cancellazione delle statistiche

Il comando seguente mostra le statistiche CDP prima che vengano cancellate. L'output visualizza il numero totale di pacchetti inviati e ricevuti dall'ultima cancellazione delle statistiche.



```
run -node nodel cdpd show-stats
```

#### RECEIVE

Packets:	9116	Csum Errors:	0	Unsupported Vers:	4561
Invalid length:	0	Malformed:	0	Mem alloc fails:	0
Missing TLVs:	0	Cache overflow:	0	Other errors:	0

#### TRANSMIT

Packets:	4557	Xmit fails:	0	No hostname:	0
Packet truncated:	0	Mem alloc fails:	0	Other errors:	0

#### OTHER

Init failures:	0
----------------	---

Il seguente comando cancella le statistiche CDP:

```
run -node nodel cdpd zero-stats
```

```
run -node nodel cdpd show-stats
```

#### RECEIVE

Packets:	0	Csum Errors:	0	Unsupported Vers:	0
Invalid length:	0	Malformed:	0	Mem alloc fails:	0
Missing TLVs:	0	Cache overflow:	0	Other errors:	0

#### TRANSMIT

Packets:	0	Xmit fails:	0	No hostname:	0
Packet truncated:	0	Mem alloc fails:	0	Other errors:	0

#### OTHER

Init failures:	0
----------------	---

Una volta cancellate, le statistiche iniziano ad accumularsi dopo l'invio o la ricezione del successivo annuncio CDP.

### Utilizzare LLDP per rilevare la connettività di rete

L'utilizzo di LLDP per rilevare la connettività di rete consiste nell'esaminare le considerazioni di implementazione, abilitarla su tutte le porte, visualizzare i dispositivi adiacenti e regolare i valori di configurazione LLDP in base alle necessità.

LLDP deve essere abilitato anche su qualsiasi switch e router prima di poter visualizzare le informazioni sui dispositivi vicini.

ONTAP attualmente riporta le seguenti strutture TLV (Type-length-value Structures):

- ID chassis
- ID porta
- TTL (Time-to-Live)
- Nome del sistema

Il nome di sistema TLV non viene inviato sui dispositivi CNA.

Alcuni adattatori di rete convergenti (CNA), come l'adattatore X1143 e le porte integrate UTA2, contengono il supporto di offload per LLDP:

- L'offload LLDP viene utilizzato per il Data Center Bridging (DCB).
- Le informazioni visualizzate potrebbero differire tra il cluster e lo switch.

I dati relativi all'ID dello chassis e all'ID della porta visualizzati dallo switch potrebbero essere diversi per le porte CNA e non CNA.

Ad esempio:

- Per porte non CNA:
  - L'ID dello chassis è un indirizzo MAC fisso di una delle porte sul nodo
  - Port ID (ID porta) è il nome della porta corrispondente sul nodo
- Per le porte CNA:
  - ID chassis e ID porta sono gli indirizzi MAC delle rispettive porte sul nodo.

Tuttavia, i dati visualizzati dal cluster sono coerenti per questi tipi di porte.



La specifica LLDP definisce l'accesso alle informazioni raccolte tramite un MIB SNMP. Tuttavia, ONTAP attualmente non supporta il MIB LDP.

#### **Attiva o disattiva LLDP**

Per rilevare e inviare annunci pubblicitari ai dispositivi adiacenti conformi a LLDP, è necessario attivare LLDP su ciascun nodo del cluster. A partire da ONTAP 9.7, LLDP è attivato per impostazione predefinita su tutte le porte di un nodo.

#### **A proposito di questa attività**

Per ONTAP 9.10.1 e versioni precedenti, la `lldp.enable` L'opzione controlla se LLDP è attivato o disattivato sulle porte di un nodo:

- `on` Attiva LLDP su tutte le porte.
- `off` Disattiva LLDP su tutte le porte.

Per ONTAP 9.11.1 e versioni successive, la `lldp.enable` L'opzione controlla se LLDP è attivato o disattivato sulle porte non cluster e non storage di un nodo:

- `on` Attiva LLDP su tutte le porte non cluster e non storage.

- `off` Disattiva LLDP su tutte le porte non cluster e non storage.

## Fasi

1. Visualizza l'impostazione LLDP corrente per un nodo o per tutti i nodi di un cluster:
  - **Nodo singolo:** `run -node node_name options lldp.enable`
  - **All Node (tutti i nodi):** Opzioni `lldp.enable`
2. Attivare o disattivare LLDP su tutte le porte di un nodo o su tutte le porte di tutti i nodi di un cluster:

Per attivare o disattivare LLDP on...	Inserisci...
Un nodo	<code>`run -node node_name options lldp.enable {on</code>
<code>off}`</code>	Tutti i nodi di un cluster
<code>`options lldp.enable {on</code>	<code>off}`</code>

- **Nodo singolo:**

```
run -node node_name options lldp.enable {on|off}
```

- **Tutti i nodi:**

```
options lldp.enable {on|off}
```

## Visualizzare le informazioni LLDP neighbor

È possibile visualizzare informazioni sui dispositivi vicini collegati a ciascuna porta dei nodi del cluster, a condizione che la porta sia collegata a un dispositivo compatibile con LLDP. Il comando `network device-Discovery show` consente di visualizzare le informazioni sulle periferiche vicine.

## Fase

1. Visualizza informazioni su tutti i dispositivi compatibili con LLDP collegati alle porte di un nodo del cluster:

```
network device-discovery show -node node -protocol lldp
```

Il seguente comando mostra i vicini collegati alle porte sul nodo `cluster-1_01`. L'output elenca i dispositivi abilitati LLDP collegati a ciascuna porta del nodo specificato. Se il `-protocol` Viene omessa, l'output elenca anche i dispositivi abilitati per CDP.

```

network device-discovery show -node cluster-1_01 -protocol lldp
Node/          Local   Discovered
Protocol      Port    Device                                Interface      Platform
-----
cluster-1_01/lldp
                e2a      0013.c31e.5c60                        GigabitEthernet1/36
                e2b      0013.c31e.5c60                        GigabitEthernet1/35
                e2c      0013.c31e.5c60                        GigabitEthernet1/34
                e2d      0013.c31e.5c60                        GigabitEthernet1/33

```

### Regolare l'intervallo di trasmissione degli annunci LLDP

Gli annunci LLDP vengono inviati ai vicini LLDP a intervalli periodici. È possibile aumentare o ridurre l'intervallo di invio degli annunci LLDP in base al traffico di rete e alle modifiche della topologia di rete.

#### A proposito di questa attività

L'intervallo predefinito consigliato da IEEE è 30 secondi, ma è possibile immettere un valore compreso tra 5 secondi e 300 secondi.

#### Fasi

1. Visualizza l'intervallo di tempo di annuncio LLDP corrente per un nodo o per tutti i nodi di un cluster:

- Nodo singolo:

```
run -node <node_name> options lldp.xmit.interval
```

- Tutti i nodi:

```
options lldp.xmit.interval
```

2. Regolare l'intervallo per l'invio di annunci LLDP per tutte le porte di un nodo o per tutte le porte di tutti i nodi di un cluster:

- Nodo singolo:

```
run -node <node_name> options lldp.xmit.interval <interval>
```

- Tutti i nodi:

```
options lldp.xmit.interval <interval>
```

## Regola il valore del time-to-live per gli annunci LLDP

TTL (Time-to-Live) è il periodo di tempo per il quale gli annunci LLDP vengono memorizzati nella cache nei dispositivi compatibili con LLDP vicini. Il TTL viene pubblicizzato in ciascun pacchetto LLDP e viene aggiornato ogni volta che un pacchetto LLDP viene ricevuto da un nodo. TTL può essere modificato nei frame LLDP in uscita.

### A proposito di questa attività

- TTL è un valore calcolato, il prodotto dell'intervallo di trasmissione (`lldp.xmit.interval`) e il moltiplicatore hold (`lldp.xmit.hold`) più uno.
- Il valore predefinito del moltiplicatore Hold è 4, ma è possibile immettere valori compresi tra 1 e 100.
- Il TTL predefinito è quindi di 121 secondi, come consigliato da IEEE, ma regolando l'intervallo di trasmissione e i valori del moltiplicatore di mantenimento, è possibile specificare un valore per i frame in uscita da 6 secondi a 30001 secondi.
- Se un indirizzo IP viene rimosso prima della scadenza del TTL, le informazioni LLDP vengono memorizzate nella cache fino alla scadenza del TTL.

### Fasi

1. Visualizza il valore del moltiplicatore di mantenimento corrente per un nodo o per tutti i nodi di un cluster:

- Nodo singolo:

```
run -node <node_name> options lldp.xmit.hold
```

- Tutti i nodi:

```
options lldp.xmit.hold
```

2. Regolare il valore del moltiplicatore Hold su tutte le porte di un nodo o su tutte le porte di tutti i nodi di un cluster:

- Nodo singolo:

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

- Tutti i nodi:

```
options lldp.xmit.hold <hold_value>
```

## Visualizzare o cancellare le statistiche LLDP

È possibile visualizzare le statistiche LLDP per il cluster e le porte non del cluster su ciascun nodo per rilevare potenziali problemi di connettività di rete. Le statistiche LLDP sono cumulative a partire dall'ultima cancellazione.

### A proposito di questa attività

Per ONTAP 9.10.1 e versioni precedenti, poiché LLDP è sempre abilitato per le porte del cluster, le statistiche LLDP vengono sempre visualizzate per il traffico su tali porte. LLDP deve essere attivato sulle porte non cluster per visualizzare le statistiche per tali porte.

Per ONTAP 9.11.1 e versioni successive, poiché LLDP è sempre abilitato per le porte di cluster e storage, le statistiche LLDP vengono sempre visualizzate per il traffico su tali porte. LLDP deve essere abilitato sulle porte non cluster e non storage per visualizzare le statistiche per tali porte.

**Fase**

Visualizzare o cancellare le statistiche LLDP correnti per tutte le porte su un nodo:

Se si desidera...	Inserisci...
Visualizzare le statistiche LLDP	<code>run -node node_name lldp stats</code>
Cancellare le statistiche LLDP	<code>run -node node_name lldp stats -z</code>

**Mostra e cancella esempio di statistiche**

Il comando seguente mostra le statistiche LLDP prima che vengano cancellate. L'output visualizza il numero totale di pacchetti inviati e ricevuti dall'ultima cancellazione delle statistiche.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
  Total frames:      190k | Accepted frames:   190k | Total drops:
0
TRANSMIT
  Total frames:      5195 | Total failures:      0
OTHER
  Stored entries:      64
```

Il seguente comando cancella le statistiche LLDP.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
  Total frames:      0 | Accepted frames:      0 | Total drops:
0
TRANSMIT
  Total frames:      0 | Total failures:      0
OTHER
  Stored entries:      64
```

Una volta cancellate, le statistiche iniziano ad accumularsi dopo l'invio o la ricezione del successivo annuncio LLDP.

# Gestione dello storage NAS

## Gestire i protocolli NAS con System Manager

### Panoramica sulla gestione NAS con System Manager

Gli argomenti di questa sezione mostrano come configurare e gestire gli ambienti NAS con Gestione di sistema in ONTAP 9.7 e versioni successive.

Se si utilizza Gestione di sistema classico (disponibile solo in ONTAP 9.7 e versioni precedenti), consultare i seguenti argomenti:

- ["Panoramica della configurazione di NFS"](#)
- ["Panoramica della configurazione SMB"](#)

System Manager supporta i flussi di lavoro per:

- Configurazione iniziale dei cluster che si intende utilizzare per i file service NAS.
- Provisioning di volumi aggiuntivo per esigenze di storage in continua evoluzione.
- Configurazione e manutenzione per strutture di sicurezza e autenticazione standard di settore.

Con System Manager, è possibile gestire i servizi NAS a livello di componente:

- Protocolli: NFS, SMB o entrambi (multiprotocollo NAS)
- Servizi di gestione dei nomi: DNS, LDAP e NIS
- Switch name service
- Sicurezza Kerberos
- Esportazioni e condivisioni
- Qtree
- Mappatura dei nomi di utenti e gruppi

### Provisioning dello storage NFS per gli archivi dati VMware

Prima di utilizzare la console di storage virtuale per VMware vSphere (VSC) per eseguire il provisioning dei volumi NFS su un sistema di storage basato su ONTAP per gli host ESXi, abilitare NFS utilizzando Gestione di sistema per ONTAP 9.7 o versioni successive.

Dopo aver creato un ["Storage VM abilitato per NFS"](#) In System Manager, è possibile eseguire il provisioning dei volumi NFS e gestire i datastore utilizzando VSC.

A partire da VSC 7.0, VSC fa parte di ["Strumenti ONTAP per appliance virtuali VMware vSphere"](#), Che include VSC, vStorage API for Storage Awareness (VASA) Provider e Storage Replication Adapter (SRA) per le funzionalità di VMware vSphere.

Controllare ["Matrice di interoperabilità NetApp"](#) Per confermare la compatibilità tra le versioni correnti di ONTAP e VSC.

Per impostare l'accesso NFS per gli host ESXi agli archivi dati utilizzando System Manager Classic (per



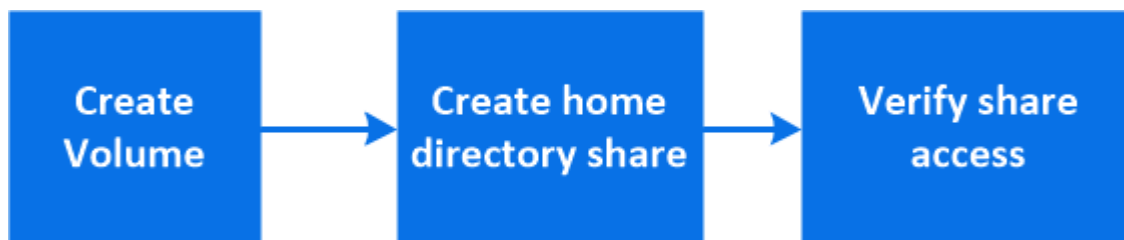
ONTAP 9.7 e versioni precedenti), vedere ["Panoramica della configurazione NFS per ESXi con VSC"](#)

Per ulteriori informazioni, vedere ["TR-4597: VMware vSphere per ONTAP"](#) E la documentazione per la release VSC.

## Provisioning dello storage NAS per le home directory

Creare volumi per fornire storage per le home directory utilizzando il protocollo SMB.

Questa procedura crea nuovi volumi per le home directory su un ["VM di storage già in uso con SMB"](#). È possibile accettare le impostazioni predefinite del sistema durante la configurazione dei volumi o specificare configurazioni personalizzate.



È possibile creare volumi FlexVol oppure, per file system di grandi dimensioni con requisiti di performance elevati, è possibile creare volumi FlexGroup. Vedere anche ["Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup"](#).

Puoi anche salvare le specifiche di questo volume in un Ansible Playbook. Per ulteriori informazioni, visitare il sito Web all'indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

### Fasi

1. Aggiungere un nuovo volume in una VM di storage abilitata per SMB.
  - a. Selezionare **Storage > Volumes** (archiviazione > volumi), quindi fare clic su **Add** (Aggiungi).
  - b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Vengono elencate solo le VM di storage configurate con il protocollo SMB. Se è disponibile una sola VM di storage configurata con il protocollo SMB, il campo **Storage VM** non viene visualizzato.

- Se si fa clic su **Salva** a questo punto, System Manager utilizza le impostazioni predefinite del sistema per creare e aggiungere un volume FlexVol.
- È possibile fare clic su **altre opzioni** per personalizzare la configurazione del volume e abilitare servizi come autorizzazione, qualità del servizio e protezione dei dati. Fare riferimento a [Personalizzare la configurazione del volume](#), quindi tornare qui per completare i seguenti passaggi.

2. [[fase 2,fase 2 nel flusso di lavoro]] fare clic su **Storage > Shares**, fare clic su **Add** e selezionare **Home Directory**.
3. Su un client Windows, effettuare le seguenti operazioni per verificare che la condivisione sia accessibile.
  - a. In Esplora risorse, mappare un disco alla condivisione nel seguente formato:  
`\\_SMB_Server_Name__Share_Name__`  
  
Se il nome della condivisione è stato creato con variabili (%w, %d o %u), verificare l'accesso con un nome risolto.
  - b. Sul disco appena creato, creare un file di prova, quindi eliminare il file.

## Personalizzare la configurazione del volume

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

### Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di qualità del servizio personalizzato o disattivare la qualità del servizio, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom, Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

- Autorizzazioni di accesso per i protocolli per i quali è configurato il volume.
- Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.
- Selezionare **Salva** per creare il volume e aggiungerlo alla VM di cluster e di storage.



Dopo aver salvato il volume, tornare a [\[step2\]](#) per completare il provisioning delle home directory.

## Provisioning dello storage NAS per i server Linux utilizzando NFS

Creare volumi per fornire storage ai server Linux utilizzando il protocollo NFS con Gestione di sistema di ONTAP (9.7 e versioni successive).

Questa procedura crea nuovi volumi su un ["VM di storage esistente abilitata per NFS"](#). È possibile accettare le impostazioni predefinite del sistema durante la configurazione dei volumi o specificare configurazioni personalizzate.

È possibile creare volumi FlexVol oppure, per file system di grandi dimensioni con requisiti di performance elevati, è possibile creare volumi FlexGroup. Vedere anche ["Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup"](#).

Puoi anche salvare le specifiche di questo volume in un Ansible Playbook. Per ulteriori informazioni, visitare il

sito Web all'indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

Per ulteriori informazioni sulla gamma di funzionalità del protocollo NFS ONTAP, consultare ["Panoramica di riferimento di NFS"](#).

## Fasi

1. Aggiungere un nuovo volume in una VM di storage abilitata per NFS.
  - a. Fare clic su **Storage > Volumes** (archiviazione > volumi), quindi su **Add** (Aggiungi).
  - b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Vengono elencate solo le VM di storage configurate con il protocollo NFS. Se è disponibile una sola VM di storage configurata con il protocollo SMB, il campo **Storage VM** non viene visualizzato.

- Se si fa clic su **Salva** a questo punto, System Manager utilizza le impostazioni predefinite del sistema per creare e aggiungere un volume FlexVol.



Il criterio di esportazione predefinito garantisce l'accesso completo a tutti gli utenti.

- È possibile fare clic su **altre opzioni** per personalizzare la configurazione del volume e abilitare servizi come autorizzazione, qualità del servizio e protezione dei dati. Fare riferimento a [Personalizzare la configurazione del volume](#), quindi tornare qui per completare i seguenti passaggi.

2. su un client Linux, procedere come segue per verificare l'accesso.
  - a. Creare e montare il volume utilizzando l'interfaccia di rete della VM di storage.
  - b. Sul volume appena montato, creare un file di test, scriverne del testo ed eliminare il file.

Dopo aver verificato l'accesso, è possibile ["limitare l'accesso del client con i criteri di esportazione del volume"](#) E impostare la proprietà e le autorizzazioni UNIX desiderate sul volume montato.

## Personalizzare la configurazione del volume

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

### Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di qualità del servizio personalizzato o disattivare la qualità del servizio, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom, Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume

FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

- Autorizzazioni di accesso per i protocolli per i quali è configurato il volume.
- Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.
- Selezionare **Salva** per creare il volume e aggiungerlo alla VM di cluster e di storage.



Dopo aver salvato il volume, tornare a [\[step2-complete-prov\]](#) Per completare il provisioning per i server Linux utilizzando NFS.

### Altri modi per farlo in ONTAP

Per eseguire questa attività con...	Fare riferimento a...
System Manager Classic (ONTAP 9.7 e versioni precedenti)	<a href="#">"Panoramica della configurazione di NFS"</a>
Interfaccia a riga di comando (CLI) di ONTAP	<a href="#">"Panoramica della configurazione di NFS con la CLI"</a>

## Gestire l'accesso utilizzando policy di esportazione

Abilitare l'accesso del client Linux ai server NFS utilizzando i criteri di esportazione.

Questa procedura crea o modifica i criteri di esportazione per un ["VM di storage esistente abilitata per NFS"](#).

### Fasi

1. In System Manager, fare clic su **Storage > Volumes**.
2. Fare clic su un volume abilitato NFS e fare clic su **More** (Altro).
3. Fare clic su **Edit Export Policy** (Modifica policy di esportazione), quindi su **Select an existing policy** (Seleziona policy esistente) o **Add a new policy** (Aggiungi nuova policy).

## Provisioning dello storage NAS per i server Windows utilizzando SMB

Creare volumi per fornire storage ai server Windows utilizzando il protocollo SMB utilizzando Gestione di sistema, disponibile con ONTAP 9.7 e versioni successive.

Questa procedura crea nuovi volumi su un ["VM di storage già in uso con SMB"](#) e crea una condivisione per la directory root (/) del volume. È possibile accettare le impostazioni predefinite del sistema durante la configurazione dei volumi o specificare configurazioni personalizzate. Dopo la configurazione SMB iniziale, è possibile creare condivisioni aggiuntive e modificarne le proprietà.

È possibile creare volumi FlexVol oppure, per file system di grandi dimensioni con requisiti di performance elevati, è possibile creare volumi FlexGroup. Vedere anche ["Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup"](#).

Puoi anche salvare le specifiche di questo volume in un Ansible Playbook. Per ulteriori informazioni, visitare il sito Web all'indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

Per ulteriori informazioni sulla gamma di funzionalità del protocollo SMB ONTAP, consultare ["Panoramica di riferimento SMB"](#).

### Prima di iniziare

- A partire da ONTAP 9.13.1, puoi attivare l'analisi della capacità e il monitoraggio delle attività per impostazione predefinita sui nuovi volumi. In System Manager, è possibile gestire le impostazioni predefinite a livello di cluster o storage VM. Per ulteriori informazioni, vedere [Abilita analisi del file system](#).

### Fasi

1. Aggiungere un nuovo volume in una VM di storage abilitata per SMB.

- a. Fare clic su **Storage > Volumes** (archiviazione > volumi), quindi su **Add** (Aggiungi).
- b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Vengono elencate solo le VM di storage configurate con il protocollo SMB. Se è disponibile una sola VM di storage configurata con il protocollo SMB, il campo **Storage VM** non viene visualizzato.

- Se si seleziona **Salva** a questo punto, System Manager utilizza le impostazioni predefinite del sistema per creare e aggiungere un volume FlexVol.
- È possibile selezionare **altre opzioni** per personalizzare la configurazione del volume in modo da abilitare servizi come autorizzazione, qualità del servizio e protezione dei dati. Fare riferimento a [Personalizzare la configurazione del volume](#), quindi tornare qui per completare i seguenti passaggi.

2. passa a un client Windows per verificare che la condivisione sia accessibile.

- a. In Esplora risorse, mappare un disco alla condivisione nel seguente formato:

\\\_SMB\_Server\_Name\_\_Share\_Name\_

- b. Sul disco appena creato, creare un file di test, scriverne del testo ed eliminare il file.

Dopo aver verificato l'accesso, è possibile limitare l'accesso client con l'ACL di condivisione e impostare le proprietà di sicurezza desiderate sull'unità mappata. Vedere ["Creare una condivisione SMB"](#) per ulteriori informazioni.

### Aggiungere o modificare le condivisioni

È possibile aggiungere ulteriori condivisioni dopo la configurazione SMB iniziale. Le condivisioni vengono create con i valori predefiniti e le proprietà selezionate. Questi possono essere modificati in un secondo momento.

Durante la configurazione di una condivisione, è possibile impostare le seguenti proprietà di condivisione:


- Autorizzazioni di accesso
- Condividere le proprietà
  - Abilita la disponibilità continua per le condivisioni che contengono dati Hyper-V e SQL Server su SMB (a partire da ONTAP 9.10.1). Vedere anche:
    - ["Requisiti di condivisione continuamente disponibili per Hyper-V su SMB"](#)
    - ["Requisiti di condivisione continuamente disponibili per SQL Server su SMB"](#)
  - Crittografare i dati con SMB 3.0 mentre si accede a questa condivisione.

Dopo la configurazione iniziale, è anche possibile modificare queste proprietà:

- Link simbolici
  - Attiva o disattiva i link simbolici e i widelink
- Condividere le proprietà
  - Consentire ai client di accedere alla directory Snapshot Copies.
  - Abilitare gli oplock, consentendo ai client di bloccare i file e memorizzare nella cache il contenuto localmente (impostazione predefinita).
  - Abilitare l'enumerazione basata sull'accesso (ABE) per visualizzare le risorse condivise in base alle autorizzazioni di accesso dell'utente.

## Procedure

Per aggiungere una nuova condivisione in un volume abilitato per SMB, fare clic su **Storage > Shares**, fare clic su **Add** e selezionare **Share**.

Per modificare una condivisione esistente, fare clic su **Storage > Shares**, quindi fare clic su  E selezionare **Modifica**.

## Personalizzare la configurazione del volume

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

## Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di QoS personalizzato o disattivare la QoS, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom, Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

**Questa opzione non è disponibile se in precedenza è stato selezionato \*posizionamento manuale in Performance Service Level.** In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita. **Autorizzazione di accesso per i protocolli per i quali è**

**configurato il volume. \*Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa. \*Fare clic su \*Save (Salva) per creare il volume e aggiungerlo alla VM del cluster e dello storage.**

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

## Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di qualità del servizio personalizzato o disattivare la qualità del servizio, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom, Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

- Autorizzazioni di accesso per i protocolli per i quali è configurato il volume.
- Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.
- Selezionare **Salva** per creare il volume e aggiungerlo alla VM di cluster e di storage.



Dopo aver salvato il volume, tornare a. [\[step2-compl-prov-win\]](#) Per completare il provisioning per i server Windows utilizzando SMB.

## Altri modi per farlo in ONTAP

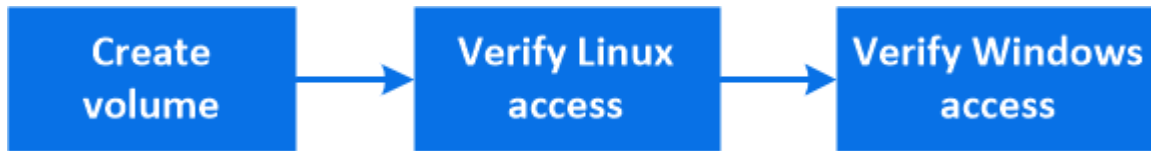
Per eseguire questa attività con...	Fare riferimento a...
System Manager Classic (ONTAP 9.7 e versioni precedenti)	<a href="#">"Panoramica della configurazione SMB"</a>
L'interfaccia della riga di comando di ONTAP	<a href="#">"Panoramica della configurazione SMB con la CLI"</a>



## Provisioning dello storage NAS per Windows e Linux utilizzando sia NFS che SMB

Creare volumi per fornire storage ai client utilizzando il protocollo NFS o SMB.

Questa procedura crea nuovi volumi su un "VM di storage esistente abilitata per protocolli NFS e SMB".



Il protocollo NFS è generalmente utilizzato in ambienti Linux. Di norma il protocollo SMB viene utilizzato in ambienti Windows. Tuttavia, sia NFS che SMB possono essere utilizzati con Linux o Windows.

È possibile creare volumi FlexVol oppure, per file system di grandi dimensioni con requisiti di performance elevati, è possibile creare volumi FlexGroup. Vedere ["Eseguire il provisioning dello storage NAS per file system di grandi dimensioni utilizzando volumi FlexGroup"](#).

Puoi anche salvare le specifiche di questo volume in un Ansible Playbook. Per ulteriori informazioni, visitare il sito Web all'indirizzo ["Utilizza i Playbook Ansible per aggiungere o modificare volumi o LUN"](#).

### Fasi

1. Aggiungere un nuovo volume in una VM di storage abilitata per NFS e SMB.

- Fare clic su **Storage > Volumes** (archiviazione > volumi), quindi su **Add** (Aggiungi).
- Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Vengono elencate solo le VM di storage configurate con i protocolli NFS e SMB. Se è disponibile una sola VM di storage configurata con i protocolli NFS e SMB, il campo **Storage VM** non viene visualizzato.

- Fare clic su **altre opzioni** e selezionare **Esporta tramite NFS**.

L'impostazione predefinita garantisce l'accesso completo a tutti gli utenti. È possibile aggiungere altre regole restrittive al criterio di esportazione in un secondo momento.

- Selezionare **Condividi tramite SMB/CIFS**.

La condivisione viene creata con un ACL (Access Control List) predefinito impostato su "controllo completo" per il gruppo **Everyone**. È possibile aggiungere restrizioni all'ACL in un secondo momento.

- Se si fa clic su **Salva** a questo punto, System Manager utilizza le impostazioni predefinite del sistema per creare e aggiungere un volume FlexVol.

In alternativa, è possibile continuare ad abilitare eventuali servizi aggiuntivi richiesti, come autorizzazione, qualità del servizio e protezione dei dati. Fare riferimento a [Personalizzare la configurazione del volume](#), quindi tornare qui per completare i seguenti passaggi.

2. su un client Linux, verificare che l'esportazione sia accessibile.

- Creare e montare il volume utilizzando l'interfaccia di rete della VM di storage.
- Sul volume appena montato, creare un file di test, scriverne del testo ed eliminare il file.



3. Su un client Windows, effettuare le seguenti operazioni per verificare che la condivisione sia accessibile.

a. In Esplora risorse, mappare un disco alla condivisione nel seguente formato:

\\\_SMB\_Server\_Name\_\_Share\_Name\_

b. Sul disco appena creato, creare un file di test, scriverne del testo ed eliminare il file.

Dopo aver verificato l'accesso, è possibile "[Limitare l'accesso del client con i criteri di esportazione del volume e limitare l'accesso del client con l'ACL di condivisione](#)" e impostare la proprietà e le autorizzazioni desiderate sul volume esportato e condiviso.

## Personalizzare la configurazione del volume

È possibile personalizzare la configurazione del volume quando si aggiungono volumi invece di accettare le impostazioni predefinite del sistema.

### Procedura

Dopo aver fatto clic su **altre opzioni**, selezionare la funzionalità desiderata e immettere i valori richiesti.

- Cache per il volume remoto.
- Performance service level (qualità del servizio, QoS).

A partire da ONTAP 9.8, è possibile specificare un criterio di qualità del servizio personalizzato o disattivare la qualità del servizio, oltre alla selezione del valore predefinito.

- Per disattivare QoS, selezionare **Custom, Existing**, quindi **None**.
- Se si seleziona **personalizzato** e si specifica un livello di servizio esistente, viene automaticamente selezionato un livello locale.
- A partire da ONTAP 9.9.1, se si sceglie di creare un livello di servizio delle performance personalizzato, è possibile utilizzare Gestione sistema per selezionare manualmente il livello locale (**posizionamento manuale**) sul quale si desidera posizionare il volume che si sta creando.

Questa opzione non è disponibile se si selezionano le opzioni della cache remota o del volume FlexGroup.

- FlexGroup Volumes (selezionare **Distribuisci i dati del volume nel cluster**).

Questa opzione non è disponibile se in precedenza è stato selezionato **posizionamento manuale** in **Performance Service Level**. In caso contrario, il volume che si sta aggiungendo diventa un volume FlexVol per impostazione predefinita.

- Autorizzazioni di accesso per i protocolli per i quali è configurato il volume.
- Protezione dei dati con SnapMirror (locale o remoto), quindi specificare il criterio di protezione e le impostazioni per il cluster di destinazione dagli elenchi a discesa.
- Selezionare **Salva** per creare il volume e aggiungerlo alla VM di cluster e di storage.

Dopo aver salvato il volume, tornare a. [\[step2-compl-prov-nfs-smb\]](#) Per completare il provisioning multiprotocollo per server Windows e Linux.

## Altri modi per farlo in ONTAP

Per eseguire queste attività con...	Guarda questo contenuto...
System Manager Classic (ONTAP 9.7 e versioni precedenti)	<a href="#">"Panoramica della configurazione multiprotocollo SMB e NFS"</a>
L'interfaccia della riga di comando di ONTAP	<a href="#">"Panoramica della configurazione SMB con la CLI"</a> <a href="#">+"Panoramica della configurazione di NFS con la CLI"</a> <a href="#">+"Quali sono gli stili di sicurezza e i loro effetti"</a> <a href="#">+"Distinzione tra maiuscole e minuscole dei nomi di file e directory in un ambiente multiprotocollo"</a>

## Accesso client sicuro con Kerberos

Abilitare Kerberos per proteggere l'accesso allo storage per i client NAS.

Questa procedura consente di configurare Kerberos su una VM di storage esistente abilitata per ["NFS"](#) oppure ["PMI"](#).

Prima di iniziare, è necessario aver configurato DNS, NTP e ["LDAP"](#) sul sistema storage.



### Fasi

1. Nella riga di comando di ONTAP, impostare le autorizzazioni UNIX per il volume root della VM di storage.
  - a. Visualizzare le autorizzazioni pertinenti sul volume root della VM di storage: `volume show -volume root_vol_name-fields user,group,unix-permissions`

Il volume root della VM di storage deve avere la seguente configurazione:

Nome...	Impostazione in corso...
UID	Root o ID 0
GID	Root o ID 0
Autorizzazioni UNIX	755

- a. Se questi valori non vengono visualizzati, utilizzare `volume modify` per aggiornarli.
2. Impostare le autorizzazioni utente per il volume root della VM di storage.
    - a. Visualizzare gli utenti UNIX locali: `vserver services name-service unix-user show -vserver vserver_name`

Per la macchina virtuale di storage devono essere configurati i seguenti utenti UNIX:

Nome utente	ID utente	ID gruppo primario
nfs	500	0
root	0	0

+

**Nota:** l'utente NFS non è richiesto se esiste una mappatura nome Kerberos-UNIX per l'SPN dell'utente client NFS; vedere il passaggio 5.

- a. Se questi valori non vengono visualizzati, utilizzare `vserver services name-service unix-user modify` per aggiornarli.

3. Impostare le autorizzazioni di gruppo per il volume root della VM di storage.

- a. Visualizzare i gruppi UNIX locali: `vserver services name-service unix-group show -vserver vserver_name`

La macchina virtuale di storage deve avere i seguenti gruppi UNIX configurati:

Nome del gruppo	ID gruppo
daemon	1
root	0

- a. Se questi valori non vengono visualizzati, utilizzare `vserver services name-service unix-group modify` per aggiornarli.

4. Passare a System Manager per configurare Kerberos

5. In System Manager, fare clic su **Storage > Storage VM** e selezionare la VM di storage.

6. Fare clic su **Impostazioni**.

7. Fare clic su ➔ In Kerberos.

8. Fare clic su **Add** (Aggiungi) sotto Kerberos Realm (Area autenticazione Kerberos) e completare le seguenti sezioni:

- Aggiungi area di autenticazione Kerberos

Inserire i dettagli di configurazione in base al vendor KDC.

- Aggiungi interfaccia di rete a Realm

Fare clic su **Aggiungi** e selezionare un'interfaccia di rete.

9. Se lo si desidera, aggiungere i mapping dai nomi principali Kerberos ai nomi utente locali.

- a. Fare clic su **Storage > Storage VM** (Storage VM) e selezionare la VM di storage.
- b. Fare clic su **Impostazioni**, quindi su ➔ Sotto **mappatura nome**.
- c. In **Kerberos to UNIX**, aggiungere modelli e sostituzioni utilizzando espressioni regolari.



## Fornire l'accesso client con i servizi di nome

Abilitare ONTAP per cercare informazioni su host, utenti, gruppi o netgroup utilizzando LDAP o NIS per autenticare i client NAS.

Questa procedura crea o modifica le configurazioni LDAP o NIS su una VM di storage esistente abilitata per "NFS" oppure "PMI".

Per le configurazioni LDAP, è necessario disporre dei dettagli di configurazione LDAP richiesti nell'ambiente e utilizzare uno schema LDAP ONTAP predefinito.

## Fasi

1. Configurare il servizio richiesto: Fare clic su **Storage > Storage VM**.
2. Selezionare la VM di storage, fare clic su **Impostazioni**, quindi fare clic su  Per LDAP o NIS.
3. Includi eventuali modifiche nel nome switch servizi: Fare clic su  Sotto Name Services Switch.

## Gestire directory e file

Espandere la visualizzazione del volume di System Manager per visualizzare ed eliminare directory e file.

A partire da ONTAP 9.9.1, le directory vengono eliminate con la funzionalità di eliminazione rapida delle directory a bassa latenza.

Per ulteriori informazioni sulla visualizzazione dei file system in ONTAP 9.9.1 e versioni successive, vedere ["Panoramica di file System Analytics"](#).

## Fase

1. Selezionare **Storage > Volumes** (Storage > volumi). Espandere un volume per visualizzarne il contenuto.

## Gestione di utenti e gruppi specifici dell'host con System Manager

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per gestire utenti e gruppi specifici di un host UNIX o Windows.

È possibile eseguire le seguenti procedure:

Windows	UNIX
<ul style="list-style-type: none"><li>• <a href="#">Visualizzare utenti e gruppi Windows</a></li><li>• <a href="#">[add-edit-delete-Windows]</a></li><li>• <a href="#">[manage-windows-users]</a></li></ul>	<ul style="list-style-type: none"><li>• <a href="#">Visualizzare utenti e gruppi UNIX</a></li><li>• <a href="#">[add-edit-delete-UNIX]</a></li><li>• <a href="#">[manage-unix-users]</a></li></ul>



## Visualizzare utenti e gruppi Windows

In System Manager, è possibile visualizzare un elenco di utenti e gruppi Windows.

## Fasi

1. In System Manager, fare clic su **Storage > Storage VM**.
2. Selezionare la VM di storage, quindi selezionare la scheda **Impostazioni**.
3. Scorrere fino all'area **host Users and Groups** (utenti e gruppi host).

La sezione **Windows** visualizza un riepilogo del numero di utenti in ciascun gruppo associato alla VM di storage selezionata.

4. Fare clic su  Nella sezione **Windows**.
5. Fare clic sulla scheda **gruppi**, quindi su  accanto al nome di un gruppo per visualizzare i dettagli relativi a tale gruppo.
6. Per visualizzare gli utenti di un gruppo, selezionare il gruppo, quindi fare clic sulla scheda **utenti**.

## Aggiungere, modificare o eliminare un gruppo Windows

In System Manager, è possibile gestire i gruppi Windows aggiungendoli, modificandoli o eliminandoli.

### Fasi

1. In Gestione sistema, visualizzare l'elenco dei gruppi Windows. Fare riferimento a [Visualizzare utenti e gruppi Windows](#).
2. Nella scheda **gruppi**, è possibile gestire i gruppi con le seguenti attività:

Per eseguire questa azione...	Eseguire questa procedura...
Aggiungere un gruppo	<ol style="list-style-type: none"><li>1. Fare clic su <b>+ Add</b>.</li><li>2. Inserire le informazioni del gruppo.</li><li>3. Specificare i privilegi.</li><li>4. Specificare i membri del gruppo (aggiungere utenti locali, utenti di dominio o gruppi di dominio).</li></ol>
Modificare un gruppo	<ol style="list-style-type: none"><li>1. Accanto al nome del gruppo, fare clic su <b>:</b>, Quindi fare clic su <b>Edit</b> (Modifica).</li><li>2. Modificare le informazioni del gruppo.</li></ol>
Eliminare un gruppo	<ol style="list-style-type: none"><li>1. Selezionare la casella accanto al gruppo o ai gruppi che si desidera eliminare.</li><li>2. Fare clic su <b>Delete</b>.</li></ol> <p><b>Nota:</b> è anche possibile eliminare un singolo gruppo facendo clic su <b>:</b> Accanto al nome del gruppo, quindi fare clic su <b>Delete</b> (Elimina).</p>






## Gestire gli utenti Windows

In System Manager, è possibile gestire gli utenti Windows aggiungendoli, modificandoli, eliminandoli, abilitandoli o disattivandoli. È inoltre possibile modificare la password di un utente Windows.

### Fasi

1. In System Manager, visualizzare l'elenco degli utenti per il gruppo. Fare riferimento a [Visualizzare utenti e gruppi Windows](#).
2. Nella scheda **utenti**, è possibile gestire gli utenti con le seguenti attività:

Per eseguire questa azione...	Eseguire questa procedura...
Aggiungere un utente	<ol style="list-style-type: none"><li>1. Fare clic su <b>+ Add</b>.</li><li>2. Inserire le informazioni dell'utente.</li></ol>
Modificare un utente	<ol style="list-style-type: none"><li>1. Accanto al nome utente, fare clic su <b>:</b>, Quindi fare clic su <b>Edit</b> (Modifica).</li><li>2. Modificare le informazioni dell'utente.</li></ol>

Eliminare un utente	<ol style="list-style-type: none"> <li>1. Selezionare la casella accanto all'utente o agli utenti che si desidera eliminare.</li> <li>2. Fare clic su  <b>Delete</b> .</li> </ol> <p><b>Nota:</b> è inoltre possibile eliminare un singolo utente facendo clic su  Accanto al nome utente, quindi fare clic su <b>Delete</b> (Elimina).</p>
Modificare la password dell'utente	<ol style="list-style-type: none"> <li>1. Accanto al nome utente, fare clic su  , Quindi fare clic su <b>Change Password</b> (Modifica password).</li> <li>2. Inserire la nuova password e confermarla.</li> </ol>
Abilitare un utente	<ol style="list-style-type: none"> <li>1. Selezionare la casella accanto a ciascun utente disattivato che si desidera attivare.</li> <li>2. Fare clic su  <b>Enable</b> .</li> </ol>
Disattivare un utente	<ol style="list-style-type: none"> <li>1. Selezionare la casella accanto a ciascun utente abilitato che si desidera disattivare.</li> <li>2. Fare clic su  <b>Disable</b> .</li> </ol>


## Visualizzare utenti e gruppi UNIX

In System Manager, è possibile visualizzare un elenco di utenti e gruppi UNIX.

### Fasi

1. In System Manager, fare clic su **Storage > Storage VM**.
2. Selezionare la VM di storage, quindi selezionare la scheda **Impostazioni**.
3. Scorrere fino all'area **host Users and Groups** (utenti e gruppi host).

La sezione **UNIX** visualizza un riepilogo del numero di utenti in ciascun gruppo associato alla VM di storage selezionata.

4. Fare clic su  Nella sezione **UNIX**.
5. Fare clic sulla scheda **Groups** (gruppi) per visualizzare i dettagli relativi al gruppo.
6. Per visualizzare gli utenti di un gruppo, selezionare il gruppo, quindi fare clic sulla scheda **utenti**.




## Aggiungere, modificare o eliminare un gruppo UNIX

In System Manager, è possibile gestire i gruppi UNIX aggiungendoli, modificandoli o eliminandoli.

### Fasi

1. In System Manager, visualizzare l'elenco dei gruppi UNIX. Fare riferimento a [Visualizzare utenti e gruppi UNIX](#).
2. Nella scheda **gruppi**, è possibile gestire i gruppi con le seguenti attività:

Per eseguire questa azione...	Eseguire questa procedura...
-------------------------------	------------------------------




Aggiungere un gruppo	<ol style="list-style-type: none"> <li>1. Fare clic su  <b>Add</b> .</li> <li>2. Inserire le informazioni del gruppo.</li> <li>3. (Facoltativo) specificare gli utenti associati.</li> </ol>
Modificare un gruppo	<ol style="list-style-type: none"> <li>1. Selezionare il gruppo.</li> <li>2. Fare clic su  <b>Edit</b> .</li> <li>3. Modificare le informazioni del gruppo.</li> <li>4. (Facoltativo) aggiungere o rimuovere utenti.</li> </ol>
Eliminare un gruppo	<ol style="list-style-type: none"> <li>1. Selezionare il gruppo o i gruppi che si desidera eliminare.</li> <li>2. Fare clic su  <b>Delete</b> .</li> </ol>

## Gestire gli utenti UNIX

In System Manager, è possibile gestire gli utenti Windows aggiungendoli, modificandoli o eliminandoli.

### Fasi

1. In System Manager, visualizzare l'elenco degli utenti per il gruppo. Fare riferimento a. [Visualizzare utenti e gruppi UNIX](#).
2. Nella scheda **utenti**, è possibile gestire gli utenti con le seguenti attività:

Per eseguire questa azione...	Eseguire questa procedura...
Aggiungere un utente	<ol style="list-style-type: none"> <li>1. Fare clic su  <b>Add</b> .</li> <li>2. Inserire le informazioni dell'utente.</li> </ol>
Modificare un utente	<ol style="list-style-type: none"> <li>1. Selezionare l'utente che si desidera modificare.</li> <li>2. Fare clic su  <b>Edit</b> .</li> <li>3. Modificare le informazioni dell'utente.</li> </ol>
Eliminare un utente	<ol style="list-style-type: none"> <li>1. Selezionare l'utente o gli utenti che si desidera eliminare.</li> <li>2. Fare clic su  <b>Delete</b> .</li> </ol>

## Monitorare i client attivi NFS

A partire da ONTAP 9.8, System Manager mostra quali connessioni client NFS sono attive quando NFS viene concesso in licenza su un cluster.

Ciò consente di verificare rapidamente quali client NFS si connettono attivamente a una VM di storage, che sono connessi ma inattivi e che sono disconnessi.

Per ogni indirizzo IP del client NFS, il display **NFS Clients** mostra: \* Ora dell'ultimo accesso \* Indirizzo IP dell'interfaccia di rete \* versione della connessione NFS \* Nome della Storage VM

Inoltre, un elenco dei client NFS attivi nelle ultime 48 ore viene visualizzato anche nella schermata **Storage>Volumes** e un numero di client NFS viene incluso nella schermata **Dashboard**.

## Fase

1. Visualizzare l'attività del client NFS: Fare clic su **hosts > NFS Clients**.

## Abilitare lo storage NAS

### Abilitare lo storage NAS per i server Linux utilizzando NFS

Creare o modificare le VM di storage per abilitare i server NFS per la distribuzione dei dati ai client Linux.



Questa procedura abilita una VM di storage nuova o esistente per il protocollo NFS. Si presuppone che i dettagli di configurazione siano disponibili per qualsiasi servizio di rete, autenticazione o sicurezza richiesto nel proprio ambiente.



## Fasi

1. Abilitare NFS su una VM di storage.
  - a. Per le nuove macchine virtuali storage: Fare clic su **Storage > Storage VMS**, fare clic su **Add** (Aggiungi), inserire il nome di una macchina virtuale storage e nella scheda **SMB/CIFS, NFS, S3**, selezionare **Enable NFS** (attiva NFS).
    - Confermare la lingua predefinita.
    - Aggiungere interfacce di rete.
    - Aggiornare le informazioni dell'account amministratore della VM di storage (opzionale).
  - b. Per le VM di storage esistenti: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings** (Impostazioni), quindi fare clic su Sotto **NFS**.
2. Aprire il criterio di esportazione del volume root della VM di storage:
  - a. Fare clic su **Storage > Volumes**, selezionare il volume root della VM di storage (che per impostazione predefinita è *volume-name \_root*), quindi fare clic sul criterio visualizzato in **Export Policy**.
  - b. Fare clic su **Aggiungi** per aggiungere una regola.
    - Specifica del client = 0.0.0.0/0
    - Access Protocol (protocolli di accesso) = NFS
    - Dettagli di accesso = UNIX di sola lettura
3. Configurare DNS for host-name resolution (Configura DNS per la risoluzione del nome host): Fare clic su **Storage > Storage VMS**, selezionare la VM di storage, fare clic su **Settings** (Impostazioni), quindi fare clic su Sotto **DNS**.
4. Configurare i name service secondo necessità.
  - a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su LDAP o NIS.

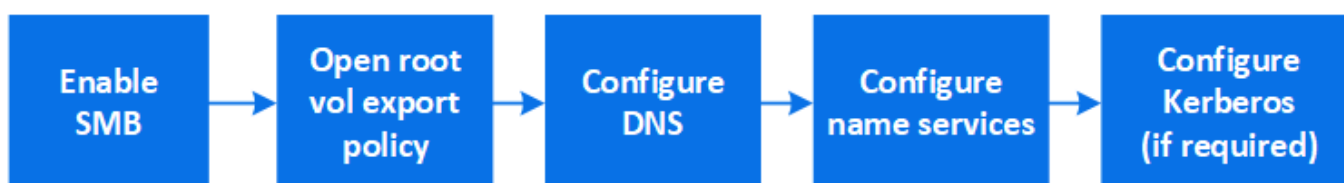


- b. Includere eventuali modifiche nel file name Services switch: Fare clic su  Nel riquadro Name Services Switch.
5. Configurare Kerberos se necessario:
  - a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, quindi fare clic su **Settings** (Impostazioni).
  - b. Fare clic su  Nel riquadro Kerberos, quindi fare clic su **Aggiungi**.


### Abilitare lo storage NAS per i server Windows utilizzando SMB

Creare o modificare le VM di storage per consentire ai server SMB di fornire dati ai client Windows.

Questa procedura consente di abilitare una VM di storage nuova o esistente per il protocollo SMB. Si presuppone che i dettagli di configurazione siano disponibili per qualsiasi servizio di rete, autenticazione o sicurezza richiesto nel proprio ambiente.




#### Fasi



1. Abilitare SMB su una VM di storage.
  - a. Per le nuove macchine virtuali storage: Fare clic su **Storage > Storage VM**, fare clic su **Add** (Aggiungi), inserire il nome di una macchina virtuale storage e nella scheda **SMB/CIFS, NFS, S3** selezionare **Enable SMB/CIFS** (attiva SMB/CIFS).
    - Inserire le seguenti informazioni:
      - Nome e password dell'amministratore
      - Nome del server
      - Dominio Active Directory
    - Confermare l'unità organizzativa.
    - Confermare i valori DNS.
    - Confermare la lingua predefinita.
    - Aggiungere interfacce di rete.
    - Aggiornare le informazioni dell'account amministratore della VM di storage (opzionale).
  - b. Per le VM di storage esistenti: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings** (Impostazioni), quindi fare clic su  Sotto **SMB**.
2. Aprire il criterio di esportazione del volume root della VM di storage:
  - a. Fare clic su **Storage > Volumes**, selezionare il volume root della VM di storage (che per impostazione predefinita è *volume-name\_root*), quindi fare clic sul criterio visualizzato in **Export Policy**.
  - b. Fare clic su **Aggiungi** per aggiungere una regola.
    - Specifica del client = 0.0.0.0/0
    - Access Protocol (protocolli di accesso) = SMB

- Dettagli di accesso = NTFS di sola lettura


### 3. Configurare il DNS per la risoluzione del nome host:

- Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su  Sotto **DNS**.
- Passare al server DNS e mappare il server SMB.
  - Creare voci di ricerca in avanti (A - record di indirizzo) e indietro (PTR - record puntatore) per mappare il nome del server SMB all'indirizzo IP dell'interfaccia di rete dati.
  - Se si utilizzano alias NetBIOS, creare una voce di ricerca alias canonical name (CNAME resource record) per associare ciascun alias all'indirizzo IP dell'interfaccia di rete dati del server SMB.

### 4. Configurare i name service secondo necessità

- Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su  Sotto **LDAP o NIS**.
- Includere eventuali modifiche nel file name Services switch: Fare clic su  Sotto **Name Services Switch**.

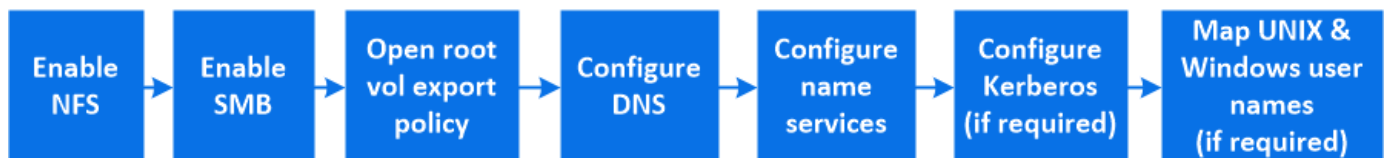
### 5. Configurare Kerberos se necessario:

- Fare clic su **Storage > Storage VM**, selezionare la VM di storage, quindi fare clic su **Settings** (Impostazioni).
- Fare clic su  In **Kerberos**, quindi fare clic su **Aggiungi**.

## Abilitare lo storage NAS per Windows e Linux utilizzando sia NFS che SMB

Creare o modificare le VM di storage per consentire ai server NFS e SMB di fornire dati ai client Linux e Windows.








Questa procedura consente a una VM di storage nuova o esistente di servire protocolli NFS e SMB. Si presuppone che i dettagli di configurazione siano disponibili per qualsiasi servizio di rete, autenticazione o sicurezza richiesto nel proprio ambiente.



### Fasi

#### 1. Abilitare NFS e SMB su una VM di storage.

- Per le nuove macchine virtuali storage: Fare clic su **Storage > Storage VMS**, fare clic su **Add** (Aggiungi), inserire il nome di una macchina virtuale storage e nella scheda **SMB/CIFS, NFS, S3**, selezionare **Enable SMB/CIFS** (attiva SMB/CIFS\*) e **Enable NFS** (attiva NFS\*).
  - Inserire le seguenti informazioni:
    - Nome e password dell'amministratore
    - Nome del server
    - Dominio Active Directory
  - Confermare l'unità organizzativa.
  - Confermare i valori DNS.

- Confermare la lingua predefinita.
  - Aggiungere interfacce di rete.
  - Aggiornare le informazioni dell'account amministratore della VM di storage (opzionale).
- b. Per le VM di storage esistenti: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, quindi fare clic su **Settings** (Impostazioni). Se NFS o SMB non sono già abilitati, completare i seguenti passaggi secondari.
- Fare clic su  Sotto **NFS**.
  - Fare clic su  Sotto **SMB**.
2. Aprire il criterio di esportazione del volume root della VM di storage:
- a. Fare clic su **Storage > Volumes**, selezionare il volume root della VM di storage (che per impostazione predefinita è *volume-name\_root*), quindi fare clic sul criterio visualizzato in **Export Policy**.
- b. Fare clic su **Aggiungi** per aggiungere una regola.
- Specifica del client = 0.0.0.0/0
  - Access Protocol (protocolli di accesso) = NFS
  - Dettagli di accesso = NFS di sola lettura
3. Configurare il DNS per la risoluzione del nome host:
- a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su  Sotto **DNS**.
- b. Una volta completata la configurazione DNS, passare al server DNS e mappare il server SMB.
- Creare voci di ricerca in avanti (A - record di indirizzo) e indietro (PTR - record puntatore) per mappare il nome del server SMB all'indirizzo IP dell'interfaccia di rete dati.
  - Se si utilizzano alias NetBIOS, creare una voce di ricerca alias canonical name (CNAME resource record) per associare ciascun alias all'indirizzo IP dell'interfaccia di rete dati del server SMB.
4. Configurare i name service secondo necessità:
- a. Fare clic su **Storage > Storage VM**, selezionare la VM di storage, fare clic su **Settings**, quindi fare clic su  Per LDAP o NIS.
- b. Includere eventuali modifiche nel file name Services switch: Fare clic su  Sotto **Name Services Switch**.
5. Configurare Kerberos se necessario: Fare clic su  Nel riquadro Kerberos, quindi fare clic su **Aggiungi**.
6. Se necessario, mappare i nomi utente UNIX e Windows: Fare clic su  In **mappatura nome** e fare clic su **Aggiungi**.

Utilizzare questa procedura solo se il sito dispone di account utente Windows e UNIX che non vengono mappati implicitamente, ovvero quando la versione minuscola di ciascun nome utente Windows corrisponde al nome utente UNIX. Questa procedura può essere eseguita utilizzando LDAP, NIS o utenti locali. Se si dispone di due set di utenti che non corrispondono, è necessario configurare la mappatura dei nomi.

## Configurare NFS con la CLI

### Panoramica della configurazione di NFS con la CLI

È possibile utilizzare i comandi CLI di ONTAP 9 per configurare l'accesso del client NFS

ai file contenuti in un nuovo volume o qtree in una macchina virtuale di storage (SVM) nuova o esistente.

Attenersi alle seguenti procedure se si desidera configurare l'accesso a un volume o a un qtree nel modo seguente:

- Si desidera utilizzare qualsiasi versione di NFS attualmente supportata da ONTAP: NFSv3, NFSv4, NFSv4.1, NFSv4.2 o NFSv4.1 con pNFS.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

Per utilizzare System Manager per configurare l'accesso multiprotocollo NAS, vedere ["Provisioning dello storage NAS per Windows e Linux utilizzando sia NFS che SMB"](#).

- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.

I dettagli sulla sintassi dei comandi sono disponibili nelle pagine guida CLI e man ONTAP.

- Per proteggere il nuovo volume verranno utilizzate le autorizzazioni per i file UNIX.
- Si dispone di privilegi di amministratore del cluster, non di amministratore SVM.

Per ulteriori informazioni sulla gamma di funzionalità del protocollo NFS ONTAP, consultare ["Panoramica di riferimento di NFS"](#).

**Altri modi per farlo in ONTAP**

Per eseguire queste attività con...	Fare riferimento a...
System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive)	<a href="#">"Provisioning dello storage NAS per i server Linux utilizzando NFS"</a>
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	<a href="#">"Panoramica della configurazione di NFS"</a>

**Workflow di configurazione NFS**

La configurazione di NFS implica la valutazione dei requisiti di storage fisico e di rete e la scelta di un workflow specifico per il tuo obiettivo: Configurare l'accesso NFS a una SVM nuova o esistente oppure aggiungere un volume o qtree a una SVM esistente già completamente configurata per l'accesso NFS.

**Preparazione**

**Valutare i requisiti di storage fisico**

Prima di eseguire il provisioning dello storage NFS per i client, è necessario assicurarsi che vi sia spazio sufficiente in un aggregato esistente per il nuovo volume. In caso contrario, è possibile aggiungere dischi a un aggregato esistente o creare un nuovo aggregato del tipo desiderato.

**Fasi**

## 1. Visualizzare lo spazio disponibile negli aggregati esistenti:

```
storage aggregate show
```

Se esiste un aggregato con spazio sufficiente, registrare il nome nel foglio di lavoro.

```
cluster::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0         239.0GB   11.13GB   95% online    1 node1  raid_dp, normal
aggr_1         239.0GB   11.13GB   95% online    1 node1  raid_dp, normal
aggr_2         239.0GB   11.13GB   95% online    1 node2  raid_dp, normal
aggr_3         239.0GB   11.13GB   95% online    1 node2  raid_dp, normal
aggr_4         239.0GB   238.9GB   95% online    5 node3  raid_dp, normal
aggr_5         239.0GB   239.0GB   95% online    4 node4  raid_dp, normal
6 entries were displayed.
```

2. Se non sono presenti aggregati con spazio sufficiente, aggiungere dischi a un aggregato esistente utilizzando `storage aggregate add-disks` oppure creare un nuovo aggregato utilizzando il comando `storage aggregate create` comando.

### Informazioni correlate

["Concetti di ONTAP"](#)

### Valutare i requisiti di rete

Prima di fornire storage NFS ai client, è necessario verificare che la rete sia configurata correttamente per soddisfare i requisiti di provisioning NFS.

### Di cosa hai bisogno

È necessario configurare i seguenti oggetti di rete del cluster:

- Porte fisiche e logiche
- Domini di broadcast
- Subnet (se richieste)
- IPspaces (come richiesto, oltre all'IPSpace predefinito)
- Gruppi di failover (secondo necessità, oltre al gruppo di failover predefinito per ciascun dominio di broadcast)
- Firewall esterni

### Fasi

1. Visualizzare le porte fisiche e virtuali disponibili:

```
network port show
```

- Quando possibile, utilizzare la porta con la velocità massima per la rete dati.
- Per ottenere le migliori prestazioni, tutti i componenti della rete dati devono avere la stessa impostazione MTU.

2. Se si intende utilizzare un nome di sottorete per assegnare l'indirizzo IP e il valore della maschera di rete per una LIF, verificare che la subnet esista e che gli indirizzi disponibili siano sufficienti: +

```
network subnet show
```

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Le subnet vengono create utilizzando `network subnet create` comando.

3. Visualizzare gli spazi IP disponibili:

```
network ipspace show
```

È possibile utilizzare l'IPSpace predefinito o un IPSpace personalizzato.

4. Se si desidera utilizzare gli indirizzi IPv6, verificare che IPv6 sia attivato sul cluster:

```
network options ipv6 show
```

Se necessario, è possibile attivare IPv6 utilizzando `network options ipv6 modify` comando.

## Decidere dove eseguire il provisioning della nuova capacità di storage NFS

Prima di creare un nuovo volume o qtree NFS, è necessario decidere se posizionarlo in una SVM nuova o esistente e la quantità di configurazione richiesta da SVM. Questa decisione determina il tuo flusso di lavoro.

### Scelte

- Se si desidera eseguire il provisioning di un volume o qtree su una nuova SVM o su una SVM esistente con NFS abilitato ma non configurato, completare la procedura descritta in "Configurazione dell'accesso NFS a una SVM" e "aggiunta dello storage NFS a una SVM abilitata per NFS".

[Configurare l'accesso NFS a una SVM](#)

[Aggiungere storage NFS a una SVM abilitata per NFS](#)

È possibile scegliere di creare una nuova SVM se si verifica una delle seguenti condizioni:

- Si sta abilitando NFS su un cluster per la prima volta.
- Esistono SVM in un cluster in cui non si desidera attivare il supporto NFS.
- Si dispone di una o più SVM abilitate NFS in un cluster e si desidera un altro server NFS in uno spazio dei nomi isolato (scenario multi-tenancy). È inoltre necessario scegliere questa opzione per eseguire il provisioning dello storage su una SVM esistente che ha NFS attivato ma non configurato. Questo potrebbe verificarsi se è stata creata la SVM per l'accesso SAN o se non sono stati attivati protocolli al momento della creazione della SVM.

Dopo aver attivato NFS su SVM, procedere con il provisioning di un volume o qtree.

- Se si desidera eseguire il provisioning di un volume o qtree su una SVM esistente completamente configurata per l'accesso NFS, completare la procedura descritta in "aggiunta dello storage NFS a una SVM abilitata per NFS".

### [Aggiunta di storage NFS a una SVM abilitata per NFS](#)

## Foglio di lavoro per la raccolta delle informazioni di configurazione NFS

Il foglio di lavoro per la configurazione di NFS consente di raccogliere le informazioni necessarie per impostare l'accesso NFS per i client.

Completare una o entrambe le sezioni del foglio di lavoro in base alla decisione presa in merito al provisioning dello storage:

Se si configura l'accesso NFS a una SVM, completare entrambe le sezioni.

- Configurazione dell'accesso NFS a una SVM
- Aggiunta di capacità di storage a una SVM abilitata per NFS

Se si aggiunge capacità di storage a una SVM abilitata per NFS, è necessario completare solo:

- Aggiunta di capacità di storage a una SVM abilitata per NFS

Per ulteriori informazioni sui parametri, consultare le pagine man dei comandi.

### Configurare l'accesso NFS a una SVM

#### Parametri per la creazione di una SVM

Questi valori vengono forniti con `vserver create` Se si sta creando una nuova SVM.


Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Un nome fornito per la nuova SVM che sia un nome di dominio completo (FQDN) o che segua un'altra convenzione che applica nomi SVM univoci in un cluster.	
<code>-aggregate</code>	Il nome di un aggregato nel cluster con spazio sufficiente per la nuova capacità di storage NFS.	
<code>-rootvolume</code>	Un nome univoco fornito per il volume root SVM.	
<code>-rootvolume-security-style</code>	Utilizzare lo stile di sicurezza UNIX per SVM.	<code>unix</code>

-language	Utilizzare l'impostazione della lingua predefinita in questo flusso di lavoro.	C.UTF-8
ipspace	Gli IPspaces sono spazi di indirizzi IP distinti in cui risiedono (macchine virtuali di storage (SVM)).	

## Parametri per la creazione di un server NFS

Questi valori vengono forniti con `vserver nfs create` Quando si crea un nuovo server NFS e si specificano le versioni NFS supportate.

Se si attiva NFSv4 o versioni successive, è necessario utilizzare LDAP per una maggiore protezione.

Campo	Descrizione	Il tuo valore
-v3, -v4.0, -v4.1, -v4.1-pnfs	<p>Abilitare le versioni NFS in base alle esigenze.</p> <div>  <p>La versione 4.2 è supportata anche in ONTAP 9.8 e versioni successive quando v4.1 è attivato.</p> </div>	
-v4-id-domain	Nome di dominio di mappatura ID.	
-v4-numeric-ids	Supporto per ID proprietari numerici (abilitati o disabilitati).	

## Parametri per la creazione di una LIF

Questi valori vengono forniti con `network interface create` Durante la creazione di LIF.

Se si utilizza Kerberos, è necessario attivare Kerberos su più LIF.

Campo	Descrizione	Il tuo valore
-lif	Un nome fornito per il nuovo LIF.	
-role	Utilizza il ruolo LIF dei dati in questo flusso di lavoro.	data
-data-protocol	Utilizzare solo il protocollo NFS in questo flusso di lavoro.	nfs



<code>-home-node</code>	Il nodo a cui la LIF restituisce quando <code>network interface revert</code> Viene eseguito sul LIF.	
<code>-home-port</code>	La porta o il gruppo di interfacce a cui LIF restituisce quando <code>network interface revert</code> Viene eseguito sul LIF.	
<code>-address</code>	L'indirizzo IPv4 o IPv6 del cluster che verrà utilizzato per l'accesso ai dati dal nuovo LIF.	
<code>-netmask</code>	La maschera di rete e il gateway per LIF.	
<code>-subnet</code>	Un pool di indirizzi IP. Utilizzato al posto di <code>-address</code> e <code>-netmask</code> per assegnare automaticamente indirizzi e netmask.	
<code>-firewall-policy</code>	Utilizzare la policy predefinita del firewall dati in questo flusso di lavoro.	data

## Parametri per la risoluzione del nome host DNS

Questi valori vengono forniti con `vserver services name-service dns create` Durante la configurazione del DNS.

Campo	Descrizione	Il tuo valore
<code>-domains</code>	Fino a cinque nomi di dominio DNS.	
<code>-name-servers</code>	Fino a tre indirizzi IP per ciascun server dei nomi DNS.	

**Indicare le informazioni sul servizio**

## Parametri per la creazione di utenti locali

Questi valori vengono forniti se si creano utenti locali utilizzando `vserver services name-service unix-user create` comando. Se si configurano utenti locali caricando un file contenente utenti UNIX da un URI (Uniform Resource Identifier), non è necessario specificare questi valori manualmente.

	Nome utente ( <code>-user</code> )	ID utente ( <code>-id</code> )	ID gruppo ( <code>-primary-gid</code> )	Nome completo ( <code>-full-name</code> )

Esempio	johnm	123	100	John Miller
1				
2				
3				
...				
n				

### Parametri per la creazione di gruppi locali

Questi valori vengono forniti se si creano gruppi locali utilizzando `vserver services name-service unix-group create` comando. Se si configurano gruppi locali caricando un file contenente gruppi UNIX da un URI, non è necessario specificare questi valori manualmente.

	Nome del gruppo (-name)	ID gruppo (-id)
Esempio	Progettazione	100
1		
2		
3		
...		
n		

### Parametri per NIS

Questi valori vengono forniti con `vserver services name-service nis-domain create` comando.



A partire da ONTAP 9.2, il campo `-nis-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server NIS.

Campo	Descrizione	Il tuo valore
<code>-domain</code>	Il dominio NIS che SVM utilizzerà per la ricerca dei nomi.	
<code>-active</code>	Il server di dominio NIS attivo.	true oppure false

<code>-servers</code>	ONTAP 9.0, 9.1: Uno o più indirizzi IP dei server NIS utilizzati dalla configurazione del dominio NIS.	
<code>-nis-servers</code>	ONTAP 9.2: Un elenco separato da virgole di indirizzi IP e nomi host per i server NIS utilizzati dalla configurazione del dominio.	

## Parametri per LDAP

Questi valori vengono forniti con `vserver services name-service ldap client create` comando.

È inoltre necessario un certificato CA principale autofirmato `.pem` file.



A partire da ONTAP 9.2, il campo `-ldap-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server LDAP.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM per la quale si desidera creare una configurazione del client LDAP.	
<code>-client-config</code>	Il nome assegnato per la nuova configurazione del client LDAP.	
<code>-servers</code>	ONTAP 9.0, 9.1: Uno o più server LDAP in base all'indirizzo IP in un elenco separato da virgole.	
<code>-ldap-servers</code>	ONTAP 9.2: Un elenco separato da virgole di indirizzi IP e nomi host per i server LDAP.	
<code>-query-timeout</code>	Utilizzare l'impostazione predefinita 3 secondi per questo flusso di lavoro.	3
<code>-min-bind-level</code>	Il livello minimo di autenticazione BIND. L'impostazione predefinita è <code>anonymous</code> . Deve essere impostato su <code>sasl</code> se la firma e il sigillo sono configurati.	
<code>-preferred-ad-servers</code>	Uno o più server Active Directory preferiti in base all'indirizzo IP in un elenco delimitato da virgole.	

Campo	Descrizione	Il tuo valore
-ad-domain	Il dominio Active Directory.	
-schema	Modello di schema da utilizzare. È possibile utilizzare uno schema predefinito o personalizzato.	
-port	Utilizzare la porta predefinita del server LDAP 389 per questo flusso di lavoro.	389
-bind-dn	Il nome distinto dell'utente Bind.	
-base-dn	Il nome distinto di base. L'impostazione predefinita è "" (root).	
-base-scope	Utilizzare l'ambito di ricerca di base predefinito subnet per questo flusso di lavoro.	subnet
-session-security	Attiva la firma o la firma LDAP e il sealing. L'impostazione predefinita è none.	
-use-start-tls	Attiva LDAP su TLS. L'impostazione predefinita è false.	

### Parametri per l'autenticazione Kerberos

Questi valori vengono forniti con `vserver nfs kerberos realm create` comando. Alcuni valori variano a seconda che si utilizzi Microsoft Active Directory come server KDC (Key Distribution Center) o MIT o altro server KDC UNIX.

Campo	Descrizione	Il tuo valore
-vserver	SVM che comunicherà con il KDC.	
-realm	L'area di autenticazione Kerberos.	
-clock-skew	Disallineamento del clock consentito tra client e server.	
-kdc-ip	Indirizzo IP KDC.	

-kdc-port	Numero della porta KDC.	
-adserver-name	Solo Microsoft KDC: Nome DEL server AD.	
-adserver-ip	Solo Microsoft KDC: Indirizzo IP DEL SERVER AD.	
-adminserver-ip	Solo KDC UNIX: Indirizzo IP del server di amministrazione.	
-adminserver-port	Solo KDC UNIX: Numero di porta del server di amministrazione.	
-passwordserver-ip	Solo KDC UNIX: Indirizzo IP del server delle password.	
-passwordserver-port	Solo KDC UNIX: Porta del server delle password.	
-kdc-vendor	Vendor KDC.	{ Microsoft
Other }	-comment	Eventuali commenti desiderati.

Questi valori vengono forniti con `vserver nfs kerberos interface enable` comando.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM per la quale si desidera creare una configurazione Kerberos.	
-lif	I dati LIF sui quali attivare Kerberos. È possibile attivare Kerberos su più LIF.	
-spn	Nome del principio di servizio (SPN)	
-permitted-enc-types	I tipi di crittografia consentiti per Kerberos su NFS; <code>aes-256</code> è consigliato, a seconda delle funzionalità del client.	

-admin-username	Le credenziali dell'amministratore KDC per recuperare la chiave segreta SPN direttamente dal KDC. È richiesta una password	
-keytab-uri	Il file keytab del KDC contenente la chiave SPN se non si dispone delle credenziali di amministratore KDC.	
-ou	L'unità organizzativa (OU) in base alla quale verrà creato l'account server Microsoft Active Directory quando si attiva Kerberos utilizzando un realm per Microsoft KDC.	

### Aggiunta di capacità di storage a una SVM abilitata per NFS

#### Parametri per la creazione di policy e regole di esportazione

Questi valori vengono forniti con `vserver export-policy create` comando.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM che ospiterà il nuovo volume.	
-policyname	Nome fornito per una nuova policy di esportazione.	

Questi valori vengono forniti per ogni regola con `vserver export-policy rule create` comando.

Campo	Descrizione	Il tuo valore
-clientmatch	Specifica di corrispondenza del client.	
-ruleindex	Posizione della regola di esportazione nell'elenco delle regole.	
-protocol	Utilizza NFS in questo flusso di lavoro.	nfs
-rorule	Metodo di autenticazione per l'accesso in sola lettura.	

-rwrule	Metodo di autenticazione per l'accesso in lettura/scrittura.	
-superuser	Metodo di autenticazione per l'accesso del superutente.	
-anon	ID utente a cui sono mappati gli utenti anonimi.	

È necessario creare una o più regole per ciascun criterio di esportazione.

<b>-ruleindex</b>	<b>-clientmatch</b>	<b>-rorule</b>	<b>-rwrule</b>	<b>-superuser</b>	<b>-anon</b>
Esempi	0.0.0.0/0,@rootaccess_netgroup	qualsiasi	krb5	sis	65534
1					
2					
3					
...					
n					

### Parametri per la creazione di un volume

Questi valori vengono forniti con `volume create` se si sta creando un volume invece di un qtree.

Campo	Descrizione	Il tuo valore
-vserver	Il nome di una SVM nuova o esistente che ospiterà il nuovo volume.	
-volume	Un nome descrittivo univoco fornito per il nuovo volume.	
-aggregate	Il nome di un aggregato nel cluster con spazio sufficiente per il nuovo volume NFS.	
-size	Un numero intero fornito per le dimensioni del nuovo volume.	

<code>-user</code>	Nome o ID dell'utente impostato come proprietario della directory principale del volume.	
<code>-group</code>	Nome o ID del gruppo impostato come proprietario della directory principale del volume.	
<code>--security-style</code>	USA lo stile di sicurezza UNIX per questo flusso di lavoro.	<code>unix</code>
<code>-junction-path</code>	Posizione sotto root (/) dove deve essere montato il nuovo volume.	
<code>-export-policy</code>	Se si intende utilizzare un criterio di esportazione esistente, è possibile immetterne il nome al momento della creazione del volume.	

### Parametri per la creazione di un qtree

Questi valori vengono forniti con `volume qtree create` se si sta creando un qtree invece di un volume.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM su cui risiede il volume contenente il qtree.	
<code>-volume</code>	Il nome del volume che conterrà il nuovo qtree.	
<code>-qtree</code>	Un nome descrittivo univoco fornito per il nuovo qtree, massimo 64 caratteri.	
<code>-qtree-path</code>	L'argomento del percorso qtree nel formato <code>/vol/volume_name/qtree_name\&gt;</code> può essere specificato invece di specificare volume e qtree come argomenti separati.	
<code>-unix-permissions</code>	Facoltativo: I permessi UNIX per qtree.	



-export-policy	Se si intende utilizzare un criterio di esportazione esistente, è possibile immetterne il nome al momento della creazione del qtree.	
----------------	--	--

## Configurare l'accesso NFS a una SVM

### Creare una SVM

Se non si dispone di almeno una SVM in un cluster per fornire l'accesso ai dati ai client NFS, è necessario crearne una.

#### Prima di iniziare

- A partire da ONTAP 9.13.1, è possibile impostare una capacità massima per una VM di storage. È inoltre possibile configurare gli avvisi quando SVM si avvicina a un livello di capacità di soglia. Per ulteriori informazioni, vedere [Gestire la capacità SVM](#).

#### Fasi

##### 1. Creare una SVM:

```
vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
ipspace_name
```

- Utilizzare l'impostazione UNIX per `-rootvolume-security-style` opzione.
- Utilizzare il C.UTF-8 predefinito `-language` opzione.
- Il `ipspace` l'impostazione è facoltativa.

##### 2. Verificare la configurazione e lo stato della SVM appena creata:

```
vserver show -vserver vserver_name
```

**Il Allowed Protocols** Il campo deve includere NFS. È possibile modificare questo elenco in un secondo momento.

**Il Vserver Operational State** il campo deve visualizzare `running` stato. Se viene visualizzato il `initializing` indica che alcune operazioni intermedie, ad esempio la creazione del volume root, non sono riuscite ed è necessario eliminare la SVM e ricrearla.

#### Esempi

Il seguente comando crea una SVM per l'accesso ai dati in IPspace ipspaceA:

```
cluster1::> vservers create -vservers vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspaces ipspaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

Il seguente comando indica che è stata creata una SVM con un volume root di 1 GB, che è stata avviata automaticamente e si trova in `running` stato. Il volume root dispone di un criterio di esportazione predefinito che non include alcuna regola, pertanto il volume root non viene esportato al momento della creazione.

```
cluster1::> vservers show -vservers vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: unix
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



A partire da ONTAP 9.13.1, è possibile impostare un modello di gruppo di policy QoS adattivo, applicando un limite di throughput e di soffitto ai volumi nella SVM. È possibile applicare questo criterio solo dopo aver creato la SVM. Per ulteriori informazioni su questo processo, vedere [Impostare un modello di gruppo di criteri adattativi](#).

## Verificare che il protocollo NFS sia attivato su SVM

Prima di poter configurare e utilizzare NFS su SVM, è necessario verificare che il

protocollo sia attivato.

### A proposito di questa attività

Questa operazione viene generalmente eseguita durante l'installazione di SVM, ma se il protocollo non è stato attivato durante l'installazione, è possibile attivarlo in un secondo momento utilizzando `vserver add-protocols` comando.



Una volta creato, non è possibile aggiungere o rimuovere un protocollo da un LIF.

È inoltre possibile disattivare i protocolli sulle SVM utilizzando `vserver remove-protocols` comando.

### Fasi

1. Controllare quali protocolli sono attualmente attivati e disattivati per SVM:

```
vserver show -vserver vserver_name -protocols
```

È inoltre possibile utilizzare `vserver show-protocols` Per visualizzare i protocolli attualmente abilitati su tutte le SVM nel cluster.

2. Se necessario, attivare o disattivare un protocollo:

- ° Per attivare il protocollo NFS:

```
vserver add-protocols -vserver vserver_name -protocols nfs
```

- ° Per disattivare un protocollo:

```
vserver remove-protocols -vserver vserver_name -protocols protocol_name  
[,protocol_name,...]
```

3. Verificare che i protocolli attivati e disattivati siano stati aggiornati correttamente:

```
vserver show -vserver vserver_name -protocols
```

### Esempio

Il seguente comando visualizza i protocolli attualmente attivati e disattivati (consentiti e non consentiti) sulla SVM denominata vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols  
Vserver           Allowed Protocols           Disallowed Protocols  
-----  
vs1.example.com   nfs                          cifs, fcp, iscsi, ndmp
```

Il seguente comando consente l'accesso tramite NFS aggiungendo `nfs` All'elenco dei protocolli abilitati sulla SVM denominato vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

### Aprire la policy di esportazione del volume root SVM

Il criterio di esportazione predefinito del volume root SVM deve includere una regola per

consentire a tutti i client l'accesso aperto tramite NFS. Senza tale regola, a tutti i client NFS viene negato l'accesso a SVM e ai suoi volumi.

### A proposito di questa attività

Quando viene creata una nuova SVM, viene creata automaticamente una policy di esportazione predefinita (chiamata predefinita) per il volume root della SVM. È necessario creare una o più regole per il criterio di esportazione predefinito prima che i client possano accedere ai dati sulla SVM.

Verificare che l'accesso sia aperto a tutti i client NFS nel criterio di esportazione predefinito e, in seguito, limitare l'accesso ai singoli volumi creando policy di esportazione personalizzate per singoli volumi o qtree.

### Fasi

1. Se si utilizza una SVM esistente, controllare il criterio di esportazione del volume root predefinito:

```
vserver export-policy rule show
```

L'output del comando dovrebbe essere simile a quanto segue:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

Vserver: vs1.example.com
Policy Name: default
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
RO Access Rule: any
RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: any
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

Se esiste una regola di questo tipo che consente l'accesso aperto, questa attività è completa. In caso contrario, passare alla fase successiva.

2. Creare una regola di esportazione per il volume root SVM:

```
vserver export-policy rule create -vserver vserver_name -policyname default
-ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any
-superuser any
```

Se la SVM contiene solo volumi protetti da Kerberos, è possibile impostare le opzioni della regola di esportazione `-rorule`, `-rwrule`, e `-superuser` per il volume root a `krb5` oppure `krb5i`. Ad esempio:

```
-rorule krb5i -rwrule krb5i -superuser krb5i
```

3. Verificare la creazione della regola utilizzando `vserver export-policy rule show` comando.

### Risultato

Qualsiasi client NFS può ora accedere a qualsiasi volume o qtree creato su SVM.

## Creare un server NFS

Dopo aver verificato che NFS sia concesso in licenza sul cluster, è possibile utilizzare `vserver nfs create` Per creare un server NFS su SVM e specificare le versioni NFS supportate.

### A proposito di questa attività

SVM può essere configurato per supportare una o più versioni di NFS. Se si supporta NFSv4 o versioni successive:

- Il nome del dominio di associazione ID utente NFSv4 deve essere lo stesso sul server NFSv4 e sui client di destinazione.

Non è necessario che sia uguale a un nome di dominio LDAP o NIS, purché il server NFSv4 e i client utilizzino lo stesso nome.

- I client di destinazione devono supportare l'impostazione NFSv4 Numeric ID (ID numerico NFSv4).
- Per motivi di sicurezza, è necessario utilizzare LDAP per i name service nelle implementazioni NFSv4.

### Prima di iniziare

La SVM deve essere stata configurata per consentire il protocollo NFS.

### Fasi

1. Verificare che NFS sia concesso in licenza sul cluster:

```
system license show -package nfs
```

In caso contrario, contattare il rappresentante commerciale.

2. Creare un server NFS:

```
vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0  
{enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids  
{enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
```

Puoi scegliere di abilitare qualsiasi combinazione di versioni NFS. Se si desidera supportare pNFS, è necessario abilitare entrambi `-v4.1` e `-v4.1-pnfs` opzioni.

Se si attiva la versione 4 o successiva, assicurarsi che le seguenti opzioni siano impostate correttamente:

- `-v4-id-domain`

Questo parametro opzionale specifica la parte di dominio del formato stringa dei nomi utente e gruppo, come definito dal protocollo NFSv4. Per impostazione predefinita, ONTAP utilizza il dominio NIS se impostato; in caso contrario, viene utilizzato il dominio DNS. Specificare un valore corrispondente al nome di dominio utilizzato dai client di destinazione.

- `-v4-numeric-ids`

Questo parametro opzionale specifica se il supporto per gli identificatori di stringa numerici negli attributi del proprietario NFSv4 è attivato. L'impostazione predefinita è attivata, ma è necessario

verificare che i client di destinazione lo supportino.

È possibile abilitare ulteriori funzionalità NFS in un secondo momento utilizzando `vserver nfs modify` comando.

3. Verificare che NFS sia in esecuzione:

```
vserver nfs status -vserver vserver_name
```

4. Verificare che NFS sia configurato come desiderato:

```
vserver nfs show -vserver vserver_name
```

## Esempi

Il seguente comando crea un server NFS sulla SVM denominata `vs1` con NFSv3 e NFSv4.0 abilitati:

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id  
-domain my_domain.com
```

I seguenti comandi verificano lo stato e i valori di configurazione del nuovo server NFS denominato `vs1`:

```
vs1::> vserver nfs status -vserver vs1  
The NFS server is running on Vserver "vs1".  
  
vs1::> vserver nfs show -vserver vs1  
  
Vserver: vs1  
General NFS Access: true  
NFS v3: enabled  
NFS v4.0: enabled  
UDP Protocol: enabled  
TCP Protocol: enabled  
Default Windows User: -  
NFSv4.0 ACL Support: disabled  
NFSv4.0 Read Delegation Support: disabled  
NFSv4.0 Write Delegation Support: disabled  
NFSv4 ID Mapping Domain: my_domain.com  
...
```

## Creare una LIF

LIF è un indirizzo IP associato a una porta fisica o logica. In caso di guasto di un componente, una LIF può eseguire il failover o essere migrata su una porta fisica diversa, continuando così a comunicare con la rete.

## Di cosa hai bisogno

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore up stato.
- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando `network subnet create` comando.

- Il meccanismo per specificare il tipo di traffico gestito da una LIF è stato modificato. Per ONTAP 9.5 e versioni precedenti, i LIF utilizzavano i ruoli per specificare il tipo di traffico che gestirebbe. A partire da ONTAP 9.6, le LIF utilizzano le policy di servizio per specificare il tipo di traffico che gestirebbe.

### A proposito di questa attività

- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Se si utilizza l'autenticazione Kerberos, attivare Kerberos su più LIF.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster utilizzando `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).
- A partire da ONTAP 9.7, se sono già presenti altre LIF per la SVM nella stessa sottorete, non è necessario specificare la porta home della LIF. ONTAP sceglie automaticamente una porta casuale sul nodo principale specificato nello stesso dominio di trasmissione delle altre LIF già configurate nella stessa sottorete.

A partire da ONTAP 9.4, FC-NVMe è supportato. Se si sta creando una LIF FC-NVMe, tenere presente quanto segue:

- Il protocollo NVMe deve essere supportato dall'adattatore FC su cui viene creato il LIF.
- FC-NVMe può essere l'unico protocollo dati sulle LIF dei dati.
- È necessario configurare un LIF che gestisca il traffico di gestione per ogni macchina virtuale di storage (SVM) che supporti LA SAN.
- Le LIF e gli spazi dei nomi NVMe devono essere ospitati sullo stesso nodo.
- È possibile configurare un solo NVMe LIF che gestisce il traffico dati per SVM

### Fasi

#### 1. Creare una LIF:

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol nfs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

Opzione	Descrizione
<b>ONTAP 9.5 e versioni precedenti</b>	<code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code>
<code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>	<code>false}`</code>

<b>ONTAP 9.6 e versioni successive</b>	<code>`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol nfs -home-node node_name -home-port port_name {-address IP_address -netmask IP_address</code>
<code>-subnet-name subnet_name} -firewall-policy data -auto-revert {true</code>	<code>false}`</code>

- Il `-role` Il parametro non è necessario quando si crea una LIF utilizzando una policy di servizio (a partire da ONTAP 9.6).
- Il `-data-protocol` Il parametro deve essere specificato al momento della creazione della LIF e non può essere modificato in seguito senza distruggere e ricreare la LIF dei dati.

Il `-data-protocol` Il parametro non è necessario quando si crea una LIF utilizzando una politica di servizio (a partire da ONTAP 9.6).

- `-home-node` È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

È inoltre possibile specificare se il LIF deve ripristinare automaticamente il nodo home e la porta home con `-auto-revert` opzione.

- `-home-port` È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
- È possibile specificare un indirizzo IP con `-address` e. `-netmask` oppure attivare l'allocazione da una subnet con `-subnet_name` opzione.
- Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene automaticamente aggiunto un percorso predefinito a tale gateway.
- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- Per `-firewall-policy` utilizzare lo stesso valore predefinito `data` Come ruolo LIF.

Se lo si desidera, è possibile creare e aggiungere un criterio firewall personalizzato in un secondo momento.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

- `-auto-revert` Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `false` in base alle policy di gestione della rete nel proprio ambiente.

2. Verificare che la LIF sia stata creata correttamente utilizzando `network interface show` comando.
3. Verificare che l'indirizzo IP configurato sia raggiungibile:



Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

4. Se si utilizza Kerberos, ripetere i passaggi da 1 a 3 per creare ulteriori LIF.

Kerberos deve essere attivato separatamente su ciascuno di questi LIF.

### Esempi

Il seguente comando crea una LIF e specifica i valori dell'indirizzo IP e della maschera di rete utilizzando `-address` e `-netmask` parametri:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port elc -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

Il seguente comando crea una LIF e assegna i valori dell'indirizzo IP e della maschera di rete dalla subnet specificata (denominata `client1_sub`):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port elc -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

Il seguente comando mostra tutti i LIF nel cluster-1. Data LIF `datalif1` e `datalif3` sono configurati con indirizzi IPv4 e `datalif4` è configurato con un indirizzo IPv6:

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
cluster-1					
cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a	
true					
node-1					
clus1	up/up	192.0.2.12/24	node-1	e0a	
true					
clus2	up/up	192.0.2.13/24	node-1	e0b	
true					
mgmt1	up/up	192.0.2.68/24	node-1	e1a	
true					
node-2					
clus1	up/up	192.0.2.14/24	node-2	e0a	
true					
clus2	up/up	192.0.2.15/24	node-2	e0b	
true					
mgmt1	up/up	192.0.2.69/24	node-2	e1a	
true					
vs1.example.com					
datalif1	up/down	192.0.2.145/30	node-1	e1c	
true					
vs3.example.com					
datalif3	up/up	192.0.2.146/30	node-2	e0c	
true					
datalif4	up/up	2001::2/64	node-2	e0c	
true					

5 entries were displayed.

Il comando seguente mostra come creare una LIF dati NAS assegnata a default-data-files politica di servizio:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

### Abilitare il DNS per la risoluzione del nome host

È possibile utilizzare `vserver services name-service dns` Per abilitare il DNS su una SVM e configurarlo per l'utilizzo del DNS per la risoluzione dei nomi host. I nomi host

vengono risolti utilizzando server DNS esterni.

### Di cosa hai bisogno

Per la ricerca dei nomi host, è necessario che sia disponibile un server DNS a livello di sito.

È necessario configurare più server DNS per evitare un singolo punto di errore. Il `vserver services name-service dns create` Viene visualizzato un messaggio di avviso se si immette un solo nome server DNS.

### A proposito di questa attività

La *Guida alla gestione della rete* contiene informazioni sulla configurazione del DNS dinamico sulla SVM.

### Fasi

#### 1. Abilitare il DNS sulla SVM:

```
vserver services name-service dns create -vserver vserver_name -domains
domain_name -name-servers ip_addresses -state enabled
```

Il seguente comando abilita i server DNS esterni su SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



A partire da ONTAP 9.2, la `vserver services name-service dns create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non riesce a contattare il server dei nomi.

#### 2. Visualizzare le configurazioni del dominio DNS utilizzando `vserver services name-service dns show` comando.

Il seguente comando visualizza le configurazioni DNS per tutte le SVM nel cluster:

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

Il seguente comando visualizza informazioni dettagliate sulla configurazione DNS per SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. Convalidare lo stato dei server dei nomi utilizzando `vserver services name-service dns check` comando.

Il `vserver services name-service dns check` Il comando è disponibile a partire da ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
-----	-----	-----	
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

## Configurare i name service

### Panoramica sulla configurazione dei name service

A seconda della configurazione del sistema storage, ONTAP deve essere in grado di cercare informazioni su host, utenti, gruppi o netgroup per fornire un accesso appropriato ai client. Per ottenere queste informazioni, è necessario configurare i name service per consentire a ONTAP di accedere ai name service locali o esterni.

È necessario utilizzare un servizio di nomi come NIS o LDAP per facilitare la ricerca dei nomi durante l'autenticazione del client. Si consiglia di utilizzare LDAP quando possibile per una maggiore sicurezza, in particolare durante l'implementazione di NFSv4 o versioni successive. È inoltre necessario configurare utenti e gruppi locali nel caso in cui i server dei nomi esterni non siano disponibili.

Le informazioni del servizio di nome devono essere mantenute sincronizzate su tutte le origini.

### Configurare la tabella name service switch

È necessario configurare correttamente la tabella dello switch del name service per consentire a ONTAP di consultare i name service locali o esterni per recuperare le informazioni di mappatura di host, utenti, gruppi, netgroup o nomi.

### Di cosa hai bisogno

È necessario decidere quali servizi di nomi utilizzare per la mappatura di host, utenti, gruppi, netgroup o nomi, in base all'ambiente in uso.

Se si intende utilizzare netgroup, tutti gli indirizzi IPv6 specificati nei netgroup devono essere abbreviati e compressi come specificato in RFC 5952.

### A proposito di questa attività

Non includere fonti di informazioni che non vengono utilizzate. Ad esempio, se NIS non viene utilizzato nell'ambiente, non specificare `-sources nis` opzione.

### Fasi

1. Aggiungere le voci necessarie alla tabella dei name service switch:

```
vserver services name-service ns-switch create -vserver vserver_name -database database_name -sources source_names
```

2. Verificare che la tabella name service switch contenga le voci previste nell'ordine desiderato:

```
vserver services name-service ns-switch show -vserver vserver_name
```

Se si desidera apportare delle correzioni, è necessario utilizzare `vserver services name-service ns-switch modify` oppure `vserver services name-service ns-switch delete` comandi.

### Esempio

Nell'esempio riportato di seguito viene creata una nuova voce nella tabella name service switch per SVM vs1 che utilizza il file netgroup locale e un server NIS esterno per cercare le informazioni del netgroup in tale ordine:

```
cluster::> vserver services name-service ns-switch create -vserver vs1  
-database netgroup -sources files,nis
```

### Al termine

- Per consentire l'accesso ai dati, è necessario configurare i name service specificati per SVM.
- Se si elimina un servizio di nomi per SVM, è necessario rimuoverlo anche dalla tabella di switch del servizio di nomi.

L'accesso del client al sistema di storage potrebbe non funzionare come previsto, se non si riesce a eliminare il name service dalla tabella di switch del name service.

### Configurare utenti e gruppi UNIX locali

#### Panoramica sulla configurazione di utenti e gruppi UNIX locali

È possibile utilizzare utenti e gruppi UNIX locali su SVM per l'autenticazione e la mappatura dei nomi. È possibile creare manualmente utenti e gruppi UNIX oppure caricare un file contenente utenti o gruppi UNIX da un URI (Uniform Resource Identifier).

Per impostazione predefinita, è previsto un limite massimo di 32,768 gruppi di utenti UNIX locali e membri del gruppo combinati nel cluster. L'amministratore del cluster può modificare questo limite.

## Creare un utente UNIX locale

È possibile utilizzare `vserver services name-service unix-user create` Per creare utenti UNIX locali. Un utente UNIX locale è un utente UNIX creato sull'opzione SVM as a UNIX name service da utilizzare nell'elaborazione delle mappature dei nomi.

### Fase

1. Creare un utente UNIX locale:

```
vserver services name-service unix-user create -vserver vserver_name -user  
user_name -id integer -primary-gid integer -full-name full_name
```

`-user user_name` specifica il nome utente. La lunghezza del nome utente deve essere pari o inferiore a 64 caratteri.

`-id integer` Specifica l'ID utente assegnato.

`-primary-gid integer` Specifica l'ID del gruppo primario. In questo modo l'utente viene aggiunto al gruppo primario. Dopo aver creato l'utente, è possibile aggiungerlo manualmente a qualsiasi altro gruppo desiderato.

### Esempio

Il seguente comando crea un utente UNIX locale denominato johnm (nome completo "John Miller") sulla SVM denominata vs1. L'utente ha l'ID 123 e l'ID del gruppo primario 100.

```
node::> vserver services name-service unix-user create -vserver vs1 -user  
johnm -id 123  
-primary-gid 100 -full-name "John Miller"
```

## Caricare utenti UNIX locali da un URI

In alternativa alla creazione manuale di singoli utenti UNIX locali in SVM, è possibile semplificare l'attività caricando un elenco di utenti UNIX locali in SVM da un URI (Uniform Resource Identifier) (`vserver services name-service unix-user load-from-uri`).

### Fasi

1. Creare un file contenente l'elenco degli utenti UNIX locali che si desidera caricare.

Il file deve contenere informazioni sull'utente in UNIX `/etc/passwd` formato:

```
user_name: password: user_ID: group_ID: full_name
```

Il comando elimina il valore di `password` e i valori dei campi dopo `full_name` campo (`home_directory` e `shell`).

Le dimensioni massime supportate dei file sono 2.5 MB.

2. Verificare che l'elenco non contenga informazioni duplicate.

Se l'elenco contiene voci duplicate, il caricamento dell'elenco non riesce e viene visualizzato un messaggio di errore.

3. Copiare il file su un server.

Il server deve essere raggiungibile dal sistema di storage su HTTP, HTTPS, FTP o FTPS.

4. Determinare l'URI del file.

L'URI è l'indirizzo fornito al sistema di storage per indicare la posizione del file.

5. Caricare il file contenente l'elenco degli utenti UNIX locali nelle SVM dall'URI:

```
vserver services name-service unix-user load-from-uri -vserver vserver_name  
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite {true false}` specifica se sovrascrivere le voci. L'impostazione predefinita è `false`.

### Esempio

Il seguente comando carica un elenco di utenti UNIX locali dall'URI `ftp://ftp.example.com/passwd` Nella SVM denominata `vs1`. Gli utenti esistenti sulla SVM non vengono sovrascritti dalle informazioni dell'URI.

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/passwd -overwrite false
```

### Creare un gruppo UNIX locale

È possibile utilizzare `vserver services name-service unix-group create` Per creare gruppi UNIX locali per SVM. I gruppi UNIX locali vengono utilizzati con gli utenti UNIX locali.

#### Fase

1. Creare un gruppo UNIX locale:

```
vserver services name-service unix-group create -vserver vserver_name -name  
group_name -id integer
```

`-name group_name` specifica il nome del gruppo. La lunghezza del nome del gruppo non deve superare i 64 caratteri.

`-id integer` Specifica l'ID del gruppo assegnato.

### Esempio

Il seguente comando crea un gruppo locale denominato `eng` sulla SVM denominata `vs1`. Il gruppo ha l'ID 101.

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name  
eng -id 101
```

## Aggiungere un utente a un gruppo UNIX locale

È possibile utilizzare `vserver services name-service unix-group adduser` Comando per aggiungere un utente a un gruppo UNIX supplementare locale a SVM.

### Fase

1. Aggiunta di un utente a un gruppo UNIX locale:

```
vserver services name-service unix-group adduser -vserver vserver_name -name group_name -username user_name
```

`-name group_name` Specifica il nome del gruppo UNIX a cui aggiungere l'utente oltre al gruppo primario dell'utente.

### Esempio

Il seguente comando aggiunge un utente denominato `max` a un gruppo UNIX locale denominato `eng` sulla SVM denominata `vs1`:

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name  
eng  
-username max
```

## Caricare i gruppi UNIX locali da un URI

In alternativa alla creazione manuale di singoli gruppi UNIX locali, è possibile caricare un elenco di gruppi UNIX locali nelle SVM da un URI (Uniform Resource Identifier) utilizzando `vserver services name-service unix-group load-from-uri` comando.

### Fasi

1. Creare un file contenente l'elenco dei gruppi UNIX locali che si desidera caricare.

Il file deve contenere informazioni di gruppo in UNIX `/etc/group` formato:

```
group_name: password: group_ID: comma_separated_list_of_users
```

Il comando elimina il valore di `password` campo.

La dimensione massima supportata del file è di 1 MB.

La lunghezza massima di ciascuna riga del file di gruppo è di 32,768 caratteri.

2. Verificare che l'elenco non contenga informazioni duplicate.

L'elenco non deve contenere voci duplicate, altrimenti il caricamento dell'elenco non riesce. Se sono già presenti voci in SVM, è necessario impostare `-overwrite` parametro a `true` per sovrascrivere tutte le voci esistenti con il nuovo file o assicurarsi che il nuovo file non contenga voci che duplicano le voci esistenti.

3. Copiare il file su un server.



Il server deve essere raggiungibile dal sistema di storage su HTTP, HTTPS, FTP o FTPS.

#### 4. Determinare l'URI del file.

L'URI è l'indirizzo fornito al sistema di storage per indicare la posizione del file.

#### 5. Caricare il file contenente l'elenco dei gruppi UNIX locali nella SVM dall'URI:

```
vserver services name-service unix-group load-from-uri -vserver vserver_name  
-uri {ftp|http|ftps|https}://uri -overwrite {true|false}
```

`-overwrite true false` specifica se sovrascrivere le voci. L'impostazione predefinita è `false`. Se si specifica questo parametro come `true`, ONTAP sostituisce l'intero database locale dei gruppi UNIX della SVM specificata con le voci del file che si sta caricando.

### Esempio

Il seguente comando carica un elenco di gruppi UNIX locali dall'URI `ftp://ftp.example.com/group` Nella SVM denominata `vs1`. I gruppi esistenti sulla SVM non vengono sovrascritti dalle informazioni dell'URI.

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1  
-uri ftp://ftp.example.com/group -overwrite false
```

### Lavorare con i netgroup

#### Panoramica sull'utilizzo dei netgroup

È possibile utilizzare netgroup per l'autenticazione degli utenti e per associare i client nelle regole dei criteri di esportazione. È possibile fornire l'accesso ai netgroup da server di nomi esterni (LDAP o NIS) oppure caricare netgroup da un URI (Uniform Resource Identifier) nelle SVM utilizzando `vserver services name-service netgroup load` comando.

#### Di cosa hai bisogno

Prima di lavorare con i netgroup, è necessario verificare che siano soddisfatte le seguenti condizioni:

- Tutti gli host nei netgroup, indipendentemente dall'origine (NIS, LDAP o file locali), devono disporre di record DNS sia in avanti (A) che in retromarcia (PTR) per fornire ricerche DNS coerenti in avanti e indietro.

Inoltre, se un indirizzo IP di un client ha più record PTR, tutti questi nomi host devono essere membri del netgroup e avere record A corrispondenti.

- I nomi di tutti gli host nei netgroup, indipendentemente dalla loro origine (NIS, LDAP o file locali), devono essere scritti correttamente e utilizzare il maiuscolo/minuscolo corretto. Le incongruenze dei casi nei nomi host utilizzati nei netgroup possono causare comportamenti imprevisti, come i controlli di esportazione non riusciti.
- Tutti gli indirizzi IPv6 specificati nei netgroup devono essere abbreviati e compressi come specificato in RFC 5952.

Ad esempio, `2011:hu9:0:0:0:0:3:1` deve essere ridotto a `2011:hu9::3:1`.

## A proposito di questa attività

Quando si lavora con netgroup, è possibile eseguire le seguenti operazioni:

- È possibile utilizzare `vserver export-policy netgroup check-membership` Per determinare se un IP client è membro di un determinato netgroup.
- È possibile utilizzare `vserver services name-service getxxbyyy netgrp` per verificare se un client fa parte di un netgroup.

Il servizio sottostante per la ricerca viene selezionato in base all'ordine di switch name service configurato.

## Caricare i netgroup nelle SVM

Uno dei metodi che è possibile utilizzare per associare i client nelle regole dei criteri di esportazione consiste nell'utilizzare gli host elencati in netgroup. È possibile caricare netgroup da un URI (Uniform Resource Identifier) in SVM in alternativa all'utilizzo di netgroup memorizzati in server di nomi esterni (`vserver services name-service netgroup load`).

## Di cosa hai bisogno

I file netgroup devono soddisfare i seguenti requisiti prima di essere caricati in una SVM:

- Il file deve utilizzare lo stesso formato di file di testo netgroup utilizzato per popolare NIS.

ONTAP controlla il formato del file di testo del netgroup prima di caricarlo. Se il file contiene errori, non viene caricato e viene visualizzato un messaggio che indica le correzioni da eseguire nel file. Dopo aver corretto gli errori, è possibile ricaricare il file netgroup nella SVM specificata.

- I caratteri alfabetici nei nomi host nel file netgroup devono essere minuscoli.
- La dimensione massima supportata del file è di 5 MB.
- Il livello massimo supportato per i netgroup di nidificazione è 1000.
- È possibile utilizzare solo i nomi host DNS primari quando si definiscono i nomi host nel file netgroup.

Per evitare problemi di accesso all'esportazione, i nomi host non devono essere definiti utilizzando i record CNAME DNS o round robin.

- Le porzioni di triplice utente e di dominio nel file netgroup devono essere mantenute vuote perché ONTAP non le supporta.

È supportata solo la parte host/IP.

## A proposito di questa attività

ONTAP supporta le ricerche netgroup-by-host per il file netgroup locale. Dopo aver caricato il file netgroup, ONTAP crea automaticamente una mappa netgroup.byhost per abilitare le ricerche netgroup-by-host. In questo modo è possibile accelerare notevolmente le ricerche dei netgroup locali durante l'elaborazione delle regole dei criteri di esportazione per valutare l'accesso al client.

## Fase

1. Caricare i netgroup nelle SVM da un URI:

```
vserver services name-service netgroup load -vserver vserver_name -source
```

```
{ftp|http|ftps|https}://uri
```

Il caricamento del file netgroup e la creazione della mappa netgroup.byhost possono richiedere alcuni minuti.

Se si desidera aggiornare i netgroup, è possibile modificare il file e caricare il file netgroup aggiornato nella SVM.

### Esempio

Il seguente comando carica le definizioni di netgroup nella SVM denominata vs1 dall'URL HTTP `http://intranet/downloads/corp-netgroup`:

```
vs1::> vserver services name-service netgroup load -vserver vs1  
-source http://intranet/downloads/corp-netgroup
```

### Verificare lo stato delle definizioni dei netgroup

Dopo aver caricato i netgroup nella SVM, è possibile utilizzare `vserver services name-service netgroup status` per verificare lo stato delle definizioni dei netgroup. In questo modo è possibile determinare se le definizioni dei netgroup sono coerenti su tutti i nodi che eseguono la SVM.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Verificare lo stato delle definizioni dei netgroup:

```
vserver services name-service netgroup status
```

È possibile visualizzare ulteriori informazioni in una vista più dettagliata.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

### Esempio

Una volta impostato il livello di privilegio, il seguente comando visualizza lo stato del netgroup per tutte le SVM:

```
vs1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when

directed to do so by technical support.

Do you wish to continue? (y or n): y

```
vs1::*> vserver services name-service netgroup status
```

Virtual

Server	Node	Load Time	Hash Value
--------	------	-----------	------------

-----	-----	-----	-----
-----	-----	-----	-----

vs1

	node1	9/20/2006 16:04:53	
e6cb38ec1396a280c0d2b77e3a84eda2			

	node2	9/20/2006 16:06:26	
e6cb38ec1396a280c0d2b77e3a84eda2			

	node3	9/20/2006 16:08:08	
e6cb38ec1396a280c0d2b77e3a84eda2			

	node4	9/20/2006 16:11:33	
e6cb38ec1396a280c0d2b77e3a84eda2			

### Creare una configurazione di dominio NIS

Se nel proprio ambiente viene utilizzato un NIS (Network Information Service) per i name service, è necessario creare una configurazione di dominio NIS per SVM utilizzando `vserver services name-service nis-domain create` comando.

### Di cosa hai bisogno

Tutti i server NIS configurati devono essere disponibili e raggiungibili prima di configurare il dominio NIS sulla SVM.

Se si intende utilizzare NIS per le ricerche nelle directory, le mappe nei server NIS non possono contenere più di 1,024 caratteri per ciascuna voce. Non specificare il server NIS non conforme a questo limite. In caso contrario, l'accesso client dipendente dalle voci NIS potrebbe non riuscire.

### A proposito di questa attività

È possibile creare più domini NIS. Tuttavia, è possibile utilizzare solo un'opzione impostata su `active`.

Se il database NIS contiene un `netgroup.byhost` map, ONTAP può utilizzarlo per ricerche più rapide. Il `netgroup.byhost` e `netgroup` le mappe nella directory devono essere sempre sincronizzate per evitare problemi di accesso al client. A partire da ONTAP 9.7, NIS `netgroup.byhost` le voci possono essere memorizzate nella cache utilizzando `vserver services name-service nis-domain netgroup-database` comandi.

L'utilizzo di NIS per la risoluzione dei nomi host non è supportato.

### Fasi

## 1. Creare una configurazione di dominio NIS:

```
vserver services name-service nis-domain create -vserver vs1 -domain  
domain_name -active true -servers IP_addresses
```

È possibile specificare fino a 10 server NIS.



A partire da ONTAP 9.2, il campo `-nis-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server NIS.

## 2. Verificare che il dominio sia stato creato:

```
vserver services name-service nis-domain show
```

### Esempio

Il seguente comando crea e crea una configurazione di dominio NIS attiva per un dominio NIS chiamato nisdomain sulla SVM denominata vs1 con un server NIS all'indirizzo IP 192.0.2.180:

```
vs1::> vserver services name-service nis-domain create -vserver vs1  
-domain nisdomain -active true -nis-servers 192.0.2.180
```

### Utilizzare LDAP

#### Panoramica sull'utilizzo di LDAP

Se nel proprio ambiente viene utilizzato LDAP per i name service, è necessario collaborare con l'amministratore LDAP per determinare i requisiti e le configurazioni appropriate del sistema di storage, quindi attivare SVM come client LDAP.

A partire da ONTAP 9.10.1, l'associazione del canale LDAP è supportata per impostazione predefinita sia per le connessioni LDAP di Active Directory che per quelle di servizi nome. ONTAP proverà l'associazione del canale con connessioni LDAP solo se Start-TLS o LDAPS è attivato insieme alla sicurezza della sessione impostata su Sign o Seal. Per disattivare o riabilitare l'associazione dei canali LDAP con i server dei nomi, utilizzare `-try-channel-binding` con il `ldap client modify` comando.

Per ulteriori informazioni, vedere ["2020 requisiti di binding del canale LDAP e firma LDAP per Windows"](#).

- Prima di configurare LDAP per ONTAP, verificare che l'implementazione del sito soddisfi le Best practice per la configurazione del server e del client LDAP. In particolare, devono essere soddisfatte le seguenti condizioni:
  - Il nome di dominio del server LDAP deve corrispondere alla voce del client LDAP.
  - I tipi di hash della password utente LDAP supportati dal server LDAP devono includere quelli supportati da ONTAP:
    - CRYPT (tutti i tipi) e SHA-1 (SHA, SSHA).
    - A partire da ONTAP 9.8, hash SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, Sono supportati anche SSHA-384 e SSHA-512).
  - Se il server LDAP richiede misure di protezione della sessione, è necessario configurarle nel client LDAP.

Sono disponibili le seguenti opzioni di sicurezza della sessione:

- Firma LDAP (verifica dell'integrità dei dati) e firma e sigillatura LDAP (verifica e crittografia dell'integrità dei dati)
- AVVIARE TLS
- LDAPS (LDAP su TLS o SSL)
- Per abilitare le query LDAP firmate e sealed, è necessario configurare i seguenti servizi:
  - I server LDAP devono supportare il meccanismo GSSAPI (Kerberos) SASL.
  - I server LDAP devono disporre di record DNS A/AAAA e di record PTR impostati sul server DNS.
  - I server Kerberos devono avere record SRV presenti sul server DNS.
- Per abilitare L'AVVIO di TLS o LDAPS, tenere in considerazione i seguenti punti.
  - L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.
  - Se si utilizza LDAPS, il server LDAP deve essere abilitato per TLS o per SSL in ONTAP 9.5 e versioni successive. SSL non è supportato in ONTAP 9.0-9.4.
  - Nel dominio deve essere già configurato un server dei certificati.
- Per abilitare la funzione LDAP referral chasing (in ONTAP 9.5 e versioni successive), devono essere soddisfatte le seguenti condizioni:
  - Entrambi i domini devono essere configurati con una delle seguenti relazioni di trust:
    - Bidirezionale
    - Unidirezionale, in cui il primario si affida al dominio di riferimento
    - Genitore-figlio
  - Il DNS deve essere configurato in modo da risolvere tutti i nomi dei server indicati.
  - Le password di dominio devono essere le stesse per autenticare quando --bind-as-cifs-server è impostato su true.

Le seguenti configurazioni non sono supportate con la funzione LDAP referral chasing.



- Per tutte le versioni di ONTAP:
  - Client LDAP su una SVM amministrativa
- Per ONTAP 9.8 e versioni precedenti (sono supportati nella versione 9.9.1 e successive):
  - Firma e sigillatura LDAP (il `-session-security` opzionale)
  - Connessioni TLS crittografate (il `-use-start-tls` opzionale)
  - Comunicazioni tramite la porta LDAPS 636 (la `-use-ldaps-for-ad-ldap` opzionale)

- È necessario inserire uno schema LDAP durante la configurazione del client LDAP su SVM.

Nella maggior parte dei casi, uno degli schemi ONTAP predefiniti sarà appropriato. Tuttavia, se lo schema LDAP nel proprio ambiente differisce da questi, è necessario creare un nuovo schema client LDAP per ONTAP prima di creare il client LDAP. Rivolgersi all'amministratore LDAP per informazioni sui requisiti dell'ambiente in uso.

- L'utilizzo di LDAP per la risoluzione dei nomi host non è supportato.

## Per ulteriori informazioni

- ["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#)
- ["Installare il certificato della CA principale autofirmato su SVM"](#)

## Creare un nuovo schema del client LDAP

Se lo schema LDAP nell'ambiente in uso differisce dai valori predefiniti di ONTAP, è necessario creare un nuovo schema del client LDAP per ONTAP prima di creare la configurazione del client LDAP.

### A proposito di questa attività

La maggior parte dei server LDAP può utilizzare gli schemi predefiniti forniti da ONTAP:

- MS-ad-BIS (lo schema preferito per la maggior parte dei server ad Windows 2012 e successivi)
- AD-IDMU (server ad Windows 2008, Windows 2012 e versioni successive)
- AD-SFU (server ad Windows 2003 e precedenti)
- RFC-2307 (SERVER LDAP UNIX)

Se è necessario utilizzare uno schema LDAP non predefinito, è necessario crearlo prima di creare la configurazione del client LDAP. Consultare l'amministratore LDAP prima di creare un nuovo schema.

Gli schemi LDAP predefiniti forniti da ONTAP non possono essere modificati. Per creare un nuovo schema, creare una copia e modificarla di conseguenza.

### Fasi

1. Visualizzare i modelli di schema del client LDAP esistenti per identificare quello che si desidera copiare:

```
vserver services name-service ldap client schema show
```

2. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

3. Creare una copia dello schema di un client LDAP esistente:

```
vserver services name-service ldap client schema copy -vserver vserver_name  
-schema existing_schema_name -new-schema-name new_schema_name
```

4. Modificare il nuovo schema e personalizzarlo in base all'ambiente:

```
vserver services name-service ldap client schema modify
```

5. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Creare una configurazione del client LDAP

Se si desidera che ONTAP acceda ai servizi LDAP o Active Directory esterni del proprio ambiente, è necessario prima configurare un client LDAP sul sistema di archiviazione.

## Di cosa hai bisogno

Uno dei primi tre server nell'elenco dei domini risolti di Active Directory deve essere attivo e fornire i dati. In caso contrario, questa attività non riesce.



Vi sono più server, tra cui più di due server inattivi in qualsiasi momento.

## Fasi

1. Rivolgersi all'amministratore LDAP per determinare i valori di configurazione appropriati per `vserver services name-service ldap client create` comando:

- a. Specificare una connessione basata su dominio o su indirizzo ai server LDAP.

Il `-ad-domain` e `-servers` le opzioni si escludono a vicenda.

- Utilizzare `-ad-domain` Opzione per attivare la ricerca del server LDAP nel dominio Active Directory.
  - È possibile utilizzare `-restrict-discovery-to-site` Opzione per limitare il rilevamento del server LDAP al sito predefinito CIFS per il dominio specificato. Se si utilizza questa opzione, è necessario specificare anche il sito predefinito CIFS con `-default-site`.
- È possibile utilizzare `-preferred-ad-servers` Opzione per specificare uno o più server Active Directory preferiti in base all'indirizzo IP in un elenco delimitato da virgole. Una volta creato il client, è possibile modificare questo elenco utilizzando `vserver services name-service ldap client modify` comando.
- Utilizzare `-servers` Opzione per specificare uno o più server LDAP (Active Directory o UNIX) per indirizzo IP in un elenco delimitato da virgole.



Il `-servers` L'opzione è obsoleta in ONTAP 9.2. Iniziando con ONTAP 9,2, la `-ldap-servers` il campo sostituisce `-servers` campo. Questo campo può contenere un nome host o un indirizzo IP per il server LDAP.

- b. Specificare uno schema LDAP predefinito o personalizzato.

La maggior parte dei server LDAP può utilizzare gli schemi di sola lettura predefiniti forniti da ONTAP. Si consiglia di utilizzare questi schemi predefiniti, a meno che non sia necessario fare diversamente. In tal caso, è possibile creare uno schema personalizzato copiando uno schema predefinito (di sola lettura) e modificando la copia.

Schemi predefiniti:

- MS-AD-BIS

Basato su RFC-2307bis, questo è lo schema LDAP preferito per la maggior parte delle implementazioni LDAP standard di Windows 2012 e versioni successive.

- AD-IDMU

Basato su Active Directory Identity Management per UNIX, questo schema è appropriato per la maggior parte dei server ad Windows 2008, Windows 2012 e versioni successive.

- AD-SFU



Basato su Active Directory Services per UNIX, questo schema è appropriato per la maggior parte dei server ad Windows 2003 e precedenti.

- RFC-2307

In base a RFC-2307 (*un approccio per l'utilizzo di LDAP come Network Information Service*), questo schema è appropriato per la maggior parte dei server UNIX ad.

c. Selezionare valori di binding.

- `-min-bind-level {anonymous|simple|sasl}` specifica il livello minimo di autenticazione bind.

Il valore predefinito è **anonymous**.

- `-bind-dn LDAP_DN` specifica l'utente di binding.

Per i server Active Directory, è necessario specificare l'utente nel modulo account (DOMINIO/utente) o principale (`user@domain.com`). In caso contrario, è necessario specificare l'utente nel formato nome distinto (`CN=user,DC=domain,DC=com`).

- `-bind-password password` specifica la password di bind.

d. Selezionare le opzioni di sicurezza della sessione, se necessario.

È possibile attivare la firma e il sealing LDAP o LDAP su TLS, se richiesto dal server LDAP.

- `--session-security {none|sign|seal}`

È possibile attivare la firma (`sign`, integrità dei dati), firma e sigillatura (`seal`, integrità dei dati e crittografia), o nessuna delle due `none`, nessuna firma o sigillatura). Il valore predefinito è `none`.

Dovresti anche impostare `-min-bind-level {sasl}` a meno che non si desideri che l'autenticazione bind venga meno a. **anonymous** oppure **simple** se la `sign` e il `seal` non vengono a buon fine.

- `-use-start-tls {true|false}`

Se impostato su **true** E il server LDAP lo supporta, il client LDAP utilizza una connessione TLS crittografata al server. Il valore predefinito è **false**. Per utilizzare questa opzione, è necessario installare un certificato CA principale autofirmato del server LDAP.



Se nella VM di storage è stato aggiunto un server SMB a un dominio e il server LDAP è uno dei controller di dominio del dominio principale del server SMB, è possibile modificare l' `-session-security-for-ad-ldap` utilizzando l'opzione `vserver cifs security modify` comando.

e. Selezionare i valori di porta, query e base.

I valori predefiniti sono consigliati, ma è necessario verificare con l'amministratore LDAP che siano appropriati per l'ambiente in uso.

- `-port port` Specifica la porta del server LDAP.

Il valore predefinito è 389.

Se si intende utilizzare Start TLS per proteggere la connessione LDAP, è necessario utilizzare la porta predefinita 389. Start TLS (Avvia TLS) inizia come una connessione non crittografata sulla porta predefinita LDAP 389 e la connessione viene quindi aggiornata a TLS. Se si modifica la porta, l'avvio TLS non riesce.

- `-query-timeout integer` specifica il timeout della query in secondi.

L'intervallo consentito va da 1 a 10 secondi. Il valore predefinito è 3 secondi.

- `-base-dn LDAP_DN` Specifica il DN di base.

Se necessario, è possibile inserire più valori (ad esempio, se è attivata la funzione LDAP referral chasing). Il valore predefinito è "" (root).

- `-base-scope {base|onelevel|subtree}` specifica l'ambito di ricerca di base.

Il valore predefinito è subtree.

- `-referral-enabled {true|false}` Specifica se è attivata la funzione LDAP referral chasing.

A partire da ONTAP 9.5, questo consente al client LDAP di indirizzare le richieste di ricerca ad altri server ONTAP se il server LDAP primario restituisce una risposta di riferimento LDAP che indica la presenza dei record desiderati sui server LDAP citati. Il valore predefinito è **false**.

Per cercare i record presenti nei server LDAP indicati, è necessario aggiungere la base dn dei record indicati alla base-dn come parte della configurazione del client LDAP.

## 2. Creazione di una configurazione del client LDAP sulla VM di storage:

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```



È necessario fornire il nome della VM di archiviazione quando si crea una configurazione client LDAP.

## 3. Verificare che la configurazione del client LDAP sia stata creata correttamente:

```
vserver services name-service ldap client show -client-config
client_config_name
```

## Esempi

Il seguente comando crea una nuova configurazione del client LDAP denominata ldap1 per la Storage VM VS1 da utilizzare con un server Active Directory per LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

Il seguente comando crea una nuova configurazione del client LDAP denominata ldap1 per la VM di storage VS1 in modo che funzioni con un server Active Directory per LDAP su cui è richiesta la firma e la sigillatura e il rilevamento del server LDAP è limitato a un sito specifico per il dominio specificato:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

Il seguente comando crea una nuova configurazione del client LDAP denominata ldap1 per la VM di storage VS1 in modo che funzioni con un server Active Directory per LDAP in cui è richiesta la ricerca del riferimento LDAP:

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

Il seguente comando modifica la configurazione del client LDAP denominata ldap1 per la macchina virtuale di storage VS1 specificando il DN di base:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

Il seguente comando modifica la configurazione del client LDAP denominata ldap1 per la VM di storage VS1 abilitando la ricerca del riferimento:

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com" -referral-enabled true
```

## Associare la configurazione del client LDAP alle SVM

Per attivare LDAP su una SVM, è necessario utilizzare `vserver services name-service ldap create` Comando per associare una configurazione del client LDAP a SVM.

### Di cosa hai bisogno

- Un dominio LDAP deve già esistere all'interno della rete e deve essere accessibile al cluster su cui si trova la SVM.
- Una configurazione del client LDAP deve esistere su SVM.

### Fasi

#### 1. Abilitare LDAP su SVM:

```
vserver services name-service ldap create -vserver vserver_name -client-config client_config_name
```



A partire da ONTAP 9.2, la `vserver services name-service ldap create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non è in grado di contattare il server dei nomi.

Il seguente comando abilita LDAP su "vs1" SVM e lo configura per utilizzare la configurazione del client LDAP "ldap1":

```
cluster1::> vserver services name-service ldap create -vserver vs1  
-client-config ldap1 -client-enabled true
```

#### 2. Convalidare lo stato dei server dei nomi utilizzando il comando di controllo `ldap name-service` dei servizi `vserver`.

Il seguente comando convalida i server LDAP su SVM vs1.

```
cluster1::> vserver services name-service ldap check -vserver vs1  
  
| Vserver: vs1 |  
| Client Configuration Name: c1 |  
| LDAP Status: up |  
| LDAP Status Details: Successfully connected to LDAP server  
"10.11.12.13". |
```

Il comando `name service check` è disponibile a partire da ONTAP 9.2.

## Verificare le origini LDAP nella tabella `name service switch`

È necessario verificare che le origini LDAP per i servizi nome siano elencate correttamente nella tabella di switch del servizio nome per SVM.

**Fasi**

1. Visualizza il contenuto della tabella corrente dello switch name service:

```
vserver services name-service ns-switch show -vserver svm_name
```

Il comando seguente mostra i risultati per SVM My\_SVM:

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
Source
Vserver      Database      Order
-----
My_SVM       hosts         files,
              dns
My_SVM       group         files,ldap
My_SVM       passwd        files,ldap
My_SVM       netgroup      files
My_SVM       namemap       files
5 entries were displayed.
```

namemap specifica le origini per la ricerca delle informazioni di mappatura dei nomi e in quale ordine. In un ambiente UNIX, questa voce non è necessaria. La mappatura dei nomi è necessaria solo in un ambiente misto che utilizza sia UNIX che Windows.

2. Aggiornare ns-switch voce appropriata:

Se si desidera aggiornare la voce ns-switch per...	Immettere il comando...
Informazioni sull'utente	<code>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</code>
Informazioni sul gruppo	<code>vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files</code>
Informazioni sul netgroup	<code>vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files</code>

**Utilizza Kerberos con NFS per una sicurezza elevata**

**Panoramica sull'utilizzo di Kerberos con NFS per una maggiore sicurezza**

Se nel proprio ambiente viene utilizzato Kerberos per l'autenticazione avanzata, è necessario collaborare con l'amministratore Kerberos per determinare i requisiti e le configurazioni appropriate del sistema di storage, quindi attivare la SVM come client

## Kerberos.

L'ambiente deve soddisfare le seguenti linee guida:

- Prima di configurare Kerberos per ONTAP, l'implementazione del sito deve seguire le Best practice per la configurazione del server e del client Kerberos.
- Se possibile, utilizzare NFSv4 o versioni successive se è richiesta l'autenticazione Kerberos.

NFSv3 può essere utilizzato con Kerberos. Tuttavia, i benefici di sicurezza completi di Kerberos sono realizzati solo nelle implementazioni ONTAP di NFSv4 o versioni successive.

- Per promuovere l'accesso ridondante al server, è necessario attivare Kerberos su diversi file di dati LIF su più nodi del cluster utilizzando lo stesso SPN.
- Quando Kerberos è attivato su SVM, è necessario specificare uno dei seguenti metodi di sicurezza nelle regole di esportazione per volumi o qtree, a seconda della configurazione del client NFS.
  - `krb5` (Protocollo Kerberos v5)
  - `krb5i` (Protocollo Kerberos v5 con controllo dell'integrità mediante checksum)
  - `krb5p` (Protocollo Kerberos v5 con servizio di privacy)

Oltre al server e ai client Kerberos, è necessario configurare i seguenti servizi esterni affinché ONTAP supporti Kerberos:

- Servizio di directory

È necessario utilizzare un servizio directory sicuro nel proprio ambiente, ad esempio Active Directory o OpenLDAP, configurato per l'utilizzo di LDAP su SSL/TLS. Non utilizzare NIS, le cui richieste vengono inviate in testo non crittografato e quindi non sono sicure.

- NTP

È necessario disporre di un server dell'orario di lavoro che esegue NTP. Ciò è necessario per evitare errori di autenticazione Kerberos dovuti a un disallineamento temporale.

- DNS (Domain Name Resolution)

Ciascun client UNIX e ciascun LIF SVM devono disporre di un record di servizio (SRV) appropriato registrato con il KDC nelle zone di ricerca in avanti e indietro. Tutti i partecipanti devono essere risolvibili correttamente tramite DNS.

### Verificare le autorizzazioni per la configurazione Kerberos

Kerberos richiede l'impostazione di determinate autorizzazioni UNIX per il volume root SVM e per utenti e gruppi locali.

#### Fasi

1. Visualizzare le autorizzazioni pertinenti sul volume root SVM:

```
volume show -volume root_vol_name-fields user,group,unix-permissions
```

Il volume root di SVM deve avere la seguente configurazione:

Nome...	Impostazione in corso...
UID	Root o ID 0
GID	Root o ID 0
Autorizzazioni UNIX	755

Se questi valori non vengono visualizzati, utilizzare `volume modify` per aggiornarli.

## 2. Visualizzare gli utenti UNIX locali:

```
vserver services name-service unix-user show -vserver vserver_name
```

La SVM deve avere i seguenti utenti UNIX configurati:

Nome utente	ID utente	ID gruppo primario	Commento
nfs	500	0	<p>Necessario per la fase DI INIT GSS.</p> <p>Il primo componente dell'SPN dell'utente client NFS viene utilizzato come utente.</p> <p>L'utente nfs non è richiesto se esiste una mappatura dei nomi Kerberos-UNIX per l'SPN dell'utente client NFS.</p>
root	0	0	Necessario per il montaggio.

Se questi valori non vengono visualizzati, è possibile utilizzare `vserver services name-service unix-user modify` per aggiornarli.

## 3. Visualizzare i gruppi UNIX locali:

```
vserver services name-service unix-group show -vserver vserver_name
```

La SVM deve avere i seguenti gruppi UNIX configurati:

Nome del gruppo	ID gruppo
daemon	1
root	0

Se questi valori non vengono visualizzati, è possibile utilizzare `vserver services name-service unix-group modify` per aggiornarli.

### Creare una configurazione di autenticazione Kerberos NFS

Se si desidera che ONTAP acceda a server Kerberos esterni nel proprio ambiente, è necessario prima configurare SVM in modo che utilizzi un'area Kerberos esistente. A tale scopo, è necessario raccogliere i valori di configurazione per il server KDC Kerberos, quindi utilizzare `vserver nfs kerberos realm create`. Per creare la configurazione dell'area di autenticazione Kerberos su una SVM.

#### Di cosa hai bisogno

L'amministratore del cluster deve aver configurato NTP sul sistema di storage, sul client e sul server KDC per evitare problemi di autenticazione. Le differenze di tempo tra un client e un server (disallineamento del clock) sono una causa comune di errori di autenticazione.

#### Fasi

1. Rivolgersi all'amministratore Kerberos per determinare i valori di configurazione appropriati da fornire con `vserver nfs kerberos realm create` comando.
2. Creare una configurazione di area di autenticazione Kerberos su SVM:

```
vserver nfs kerberos realm create -vserver vserver_name -realm realm_name  
{AD_KDC_server_values |AD_KDC_server_values} -comment "text"
```

3. Verificare che la configurazione dell'area di autenticazione Kerberos sia stata creata correttamente:

```
vserver nfs kerberos realm show
```

#### Esempi

Il seguente comando crea una configurazione del realm Kerberos NFS per SVM vs1 che utilizza un server Microsoft Active Directory come server KDC. L'area di autenticazione Kerberos è AUTH.EXAMPLE.COM. Il server Active Directory è denominato ad-1 e il suo indirizzo IP è 10.10.8.14. L'inclinazione dell'orologio consentita è di 300 secondi (impostazione predefinita). L'indirizzo IP del server KDC è 10.10.8.14 e il numero di porta è 88 (impostazione predefinita). "Microsoft Kerberos config" è il commento.

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm  
AUTH.EXAMPLE.COM -adserver-name ad-1  
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88  
-kdc-vendor Microsoft  
-comment "Microsoft Kerberos config"
```

Il seguente comando crea una configurazione di autenticazione Kerberos NFS per SVM vs1 che utilizza un KDC MIT. L'area di autenticazione Kerberos è SECURITY.EXAMPLE.COM. L'inclinazione dell'orologio consentita è di 300 secondi. L'indirizzo IP del server KDC è 10.10.9.1 e il numero di porta è 88. Il vendor di KDC è un altro a indicare un vendor UNIX. L'indirizzo IP del server amministrativo è 10.10.9.1 e il numero di porta è 749 (impostazione predefinita). L'indirizzo IP del server delle password è 10.10.9.1 e il numero di porta è 464 (impostazione predefinita). Il commento è "UNIX Kerberos config".



```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm  
SECURITY.EXAMPLE.COM. -clock-skew 300  
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1  
-adminserver-port 749  
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX  
Kerberos config"
```

### Configurare i tipi di crittografia consentiti per NFS Kerberos

Per impostazione predefinita, ONTAP supporta i seguenti tipi di crittografia per NFS Kerberos: DES, 3DES, AES-128 e AES-256. È possibile configurare i tipi di crittografia consentiti per ogni SVM in modo che si adattino ai requisiti di sicurezza per il proprio ambiente specifico utilizzando `vserver nfs modify` con il `-permitted-enc-types` parametro.

#### A proposito di questa attività

Per una maggiore compatibilità con i client, ONTAP supporta sia la crittografia DES debole che la crittografia AES avanzata per impostazione predefinita. Ciò significa, ad esempio, che se si desidera aumentare la protezione e l'ambiente lo supporta, è possibile utilizzare questa procedura per disattivare DES e 3DES e richiedere ai client di utilizzare solo la crittografia AES.

Si consiglia di utilizzare la crittografia più efficace disponibile. Per ONTAP, cioè AES-256. Verificare con l'amministratore di KDC che questo livello di crittografia sia supportato nell'ambiente in uso.

- L'attivazione o la disattivazione completa di AES (sia AES-128 che AES-256) su SVM è un'interruzione perché distrugge il file DES principal/keytab originale, richiedendo quindi la disattivazione della configurazione Kerberos su tutti i LIF per SVM.

Prima di apportare questa modifica, verificare che i client NFS non si basino sulla crittografia AES su SVM.

- L'attivazione o la disattivazione DI DES o 3DES non richiede modifiche alla configurazione Kerberos sui LIF.

#### Fase

1. Attivare o disattivare il tipo di crittografia consentito:

Se si desidera attivare o disattivare...	Attenersi alla procedura descritta di seguito...
DES o 3DES	<p>a. Configurare i tipi di crittografia Kerberos NFS consentiti per SVM:</p> <pre>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Separare più tipi di crittografia con una virgola.</p> <p>b. Verificare che la modifica sia stata eseguita correttamente:</p> <pre>vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre>
AES-128 o AES-256	<p>a. Identificare su quali SVM e LIF Kerberos sono attivati:</p> <pre>vserver nfs kerberos interface show</pre> <p>b. Disattiva Kerberos su tutti i LIF della SVM il cui tipo di crittografia Kerberos NFS consentiva di modificare:</p> <pre>vserver nfs kerberos interface disable -lif lif_name</pre> <p>c. Configurare i tipi di crittografia Kerberos NFS consentiti per SVM:</p> <pre>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</pre> <p>Separare più tipi di crittografia con una virgola.</p> <p>d. Verificare che la modifica sia stata eseguita correttamente:</p> <pre>vserver nfs show -vserver vserver_name -fields permitted-enc- types</pre> <p>e. Riabilitare Kerberos su tutti i LIF su SVM:</p> <pre>vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name</pre> <p>f. Verificare che Kerberos sia attivato su tutti i LIF:</p> <pre>vserver nfs kerberos interface show</pre>

#### Attivare Kerberos su una LIF dati

È possibile utilizzare `vserver nfs kerberos interface enable` Comando per abilitare Kerberos su una LIF dati. In questo modo, SVM può utilizzare i servizi di sicurezza Kerberos per NFS.

**A proposito di questa attività**

Se si utilizza un KDC Active Directory, i primi 15 caratteri di qualsiasi SPN utilizzato devono essere univoci tra le SVM all'interno di un'area di autenticazione o di un dominio.

**Fasi**

- 1. Creare la configurazione Kerberos NFS:

```
vserver nfs kerberos interface enable -vserver vserver_name -lif
logical_interface -spn service_principal_name
```

ONTAP richiede la chiave segreta per l'SPN del KDC per abilitare l'interfaccia Kerberos.

Per i KDC Microsoft, viene contattato il KDC e vengono inviati un prompt di nome utente e password alla CLI per ottenere la chiave segreta. Se è necessario creare l'SPN in un'unità organizzativa diversa dell'area Kerberos, è possibile specificare l'opzione `-ou` parametro.

Per i KDC non Microsoft, è possibile ottenere la chiave segreta utilizzando uno dei due metodi seguenti:

Se...	È inoltre necessario includere il seguente parametro con il comando...
Disponere delle credenziali di amministratore di KDC per recuperare la chiave direttamente dal KDC	<code>-admin-username kdc_admin_username</code>
Non si dispone delle credenziali di amministratore di KDC, ma di un file keytab del KDC contenente la chiave	<code>-keytab-uri {ftp</code>

- 2. Verificare che Kerberos sia stato attivato su LIF:

```
vserver nfs kerberos-config show
```

- 3. Ripetere i passaggi 1 e 2 per attivare Kerberos su più LIF.

**Esempio**

Il seguente comando crea e verifica una configurazione Kerberos NFS per la SVM denominata vs1 sull'interfaccia logica ves03-d1, con l'SPN `nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM` nell'OU `lab2ou`:

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
      Logical
Vserver Interface Address      Kerberos  SPN
-----
vs0      ves01-a1
          10.10.10.30 disabled -
vs2      ves01-d1
          10.10.10.40 enabled  nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

## Aggiungere capacità di storage a una SVM abilitata per NFS

### Aggiunta di capacità di storage a una panoramica SVM abilitata per NFS

Per aggiungere capacità di storage a una SVM abilitata per NFS, è necessario creare un volume o un qtree per fornire un container di storage e creare o modificare un criterio di esportazione per tale container. È quindi possibile verificare l'accesso del client NFS dal cluster e verificare l'accesso dai sistemi client.

#### Di cosa hai bisogno

- NFS deve essere completamente configurato su SVM.
- Il criterio di esportazione predefinito del volume root SVM deve contenere una regola che consenta l'accesso a tutti i client.
- Tutti gli aggiornamenti della configurazione dei name service devono essere completi.
- Eventuali aggiunte o modifiche a una configurazione Kerberos devono essere completate.

### Creare una policy di esportazione

Prima di creare regole di esportazione, è necessario creare un criterio di esportazione per conservarle. È possibile utilizzare `vserver export-policy create` per creare un criterio di esportazione.

#### Fasi

1. Creare una policy di esportazione:

```
vserver export-policy create -vserver vserver_name -policyname policy_name
```

Il nome del criterio può contenere fino a 256 caratteri.

2. Verificare che il criterio di esportazione sia stato creato:

```
vserver export-policy show -policyname policy_name
```

## Esempio

I seguenti comandi creano e verificano la creazione di una policy di esportazione denominata `exp1` sulla SVM denominata `vs1`:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
-----
vs1              exp1
```

## Aggiungere una regola a un criterio di esportazione

Senza regole, i criteri di esportazione non possono fornire l'accesso client ai dati. Per creare una nuova regola di esportazione, è necessario identificare i client e selezionare un formato di corrispondenza client, selezionare i tipi di accesso e di sicurezza, specificare un mapping anonimo dell'ID utente, selezionare un numero di indice della regola e selezionare il protocollo di accesso. È quindi possibile utilizzare `vserver export-policy rule create` per aggiungere la nuova regola a un criterio di esportazione.

### Di cosa hai bisogno

- Il criterio di esportazione a cui si desidera aggiungere le regole di esportazione deve già esistere.
- Il DNS deve essere configurato correttamente sui dati SVM e i server DNS devono avere le voci corrette per i client NFS.

Questo perché ONTAP esegue ricerche DNS utilizzando la configurazione DNS dei dati SVM per determinati formati di corrispondenza client, e gli errori nella corrispondenza delle regole dei criteri di esportazione possono impedire l'accesso ai dati del client.

- Se si esegue l'autenticazione con Kerberos, è necessario determinare quale dei seguenti metodi di protezione viene utilizzato sui client NFS:
  - `krb5` (Protocollo Kerberos V5)
  - `krb5i` (Protocollo Kerberos V5 con controllo dell'integrità mediante checksum)
  - `krb5p` (Protocollo Kerberos V5 con servizio di privacy)

### A proposito di questa attività

Non è necessario creare una nuova regola se una regola esistente in un criterio di esportazione copre i requisiti di accesso e corrispondenza del client.

Se si esegue l'autenticazione con Kerberos e si accede a tutti i volumi della SVM tramite Kerberos, è possibile impostare le opzioni della regola di esportazione `-rorule`, `-rwrule`, e. `-superuser` per il volume root a. `krb5`, `krb5i`, o. `krb5p`.

### Fasi

1. Identificare i client e il formato di corrispondenza del client per la nuova regola.

Il `-clientmatch` option specifica i client a cui si applica la regola. È possibile specificare valori di corrispondenza client singoli o multipli; le specifiche di valori multipli devono essere separate da virgole. È possibile specificare la corrispondenza in uno dei seguenti formati:

Formato di corrispondenza del client	Esempio
Nome di dominio preceduto da "." carattere	<code>.example.com</code> oppure <code>.example.com, .example.net, ...</code>
Nome host	<code>host1</code> oppure <code>host1, host2, ...</code>
Indirizzo IPv4	<code>10.1.12.24</code> oppure <code>10.1.12.24, 10.1.12.25, ...</code>
Indirizzo IPv4 con una subnet mask espressa come numero di bit	<code>10.1.12.10/4</code> oppure <code>10.1.12.10/4, 10.1.12.11/4, ...</code>
Indirizzo IPv4 con una maschera di rete	<code>10.1.16.0/255.255.255.0</code> oppure <code>10.1.16.0/255.255.255.0, 10.1.17.0/255.255.255.0, ...</code>
Indirizzo IPv6 in formato punteggiato	<code>::1.2.3.4</code> oppure <code>::1.2.3.4, ::1.2.3.5, ...</code>
Indirizzo IPv6 con una subnet mask espressa come numero di bit	<code>ff::00/32</code> oppure <code>ff::00/32, ff::01/32, ...</code>
Un singolo netgroup con il nome del netgroup preceduto dal carattere @	<code>@netgroup1</code> oppure <code>@netgroup1, @netgroup2, ...</code>

È inoltre possibile combinare tipi di definizioni client, ad esempio `.example.com, @netgroup1`.

Quando si specificano gli indirizzi IP, tenere presente quanto segue:

- Non è consentito inserire un intervallo di indirizzi IP, ad esempio `10.1.12.10-10.1.12.70`.

Le voci in questo formato vengono interpretate come una stringa di testo e trattate come nome host.

- Quando si specificano singoli indirizzi IP nelle regole di esportazione per la gestione granulare dell'accesso client, non specificare gli indirizzi IP assegnati in modo dinamico (ad esempio DHCP) o temporaneo (ad esempio IPv6).

In caso contrario, il client perde l'accesso quando cambia l'indirizzo IP.

- Non è consentito inserire un indirizzo IPv6 con una maschera di rete, ad esempio `ff::12/ff::00`.

## 2. Selezionare i tipi di accesso e di sicurezza per le corrispondenze dei client.

È possibile specificare una o più delle seguenti modalità di accesso per i client che eseguono l'autenticazione con i tipi di protezione specificati:

- `-rorule` (accesso di sola lettura)
- `-rwrule` (accesso di lettura/scrittura)
- `-superuser` (accesso root)



Un client può ottenere l'accesso in lettura/scrittura solo per un tipo di protezione specifico se la regola di esportazione consente l'accesso in sola lettura anche per quel tipo di protezione. Se il parametro di sola lettura è più restrittivo per un tipo di protezione rispetto al parametro di lettura/scrittura, il client potrebbe non ottenere l'accesso di lettura/scrittura. Lo stesso vale per l'accesso dei superutenti.

È possibile specificare un elenco separato da virgole di più tipi di protezione per una regola. Se si specifica il tipo di protezione come `any` oppure `never`, non specificare altri tipi di protezione. Scegliere tra i seguenti tipi di protezione validi:

Quando il tipo di protezione è impostato su...	Un client corrispondente può accedere ai dati esportati...
<code>any</code>	Sempre, indipendentemente dal tipo di sicurezza in entrata.
<code>none</code>	Se elencati da soli, ai client con qualsiasi tipo di protezione viene concesso l'accesso come anonimo. Se elencato con altri tipi di protezione, ai client con un tipo di protezione specificato viene concesso l'accesso e ai client con qualsiasi altro tipo di protezione viene concesso l'accesso come anonimo.
<code>never</code>	Mai, indipendentemente dal tipo di sicurezza in entrata.
<code>krb5</code>	Se autenticato da Kerberos 5. Authentication Only (solo autenticazione): L'intestazione di ogni richiesta e risposta viene firmata.
<code>krb5i</code>	Se autenticato da Kerberos 5i. Autenticazione e integrità: L'intestazione e il corpo di ogni richiesta e risposta vengono firmati.
<code>krb5p</code>	Se autenticato da Kerberos 5p. Autenticazione, integrità e privacy: L'intestazione e il corpo di ogni richiesta e risposta vengono firmati e il payload dei dati NFS viene crittografato.
<code>ntlm</code>	Se autenticato da CIFS NTLM.
<code>sys</code>	Se autenticato da NFS AUTH_SYS.

Il tipo di protezione consigliato è `sys`. Oppure, se si utilizza Kerberos, ``krb5,krb5i,0.krb5p`.

Se si utilizza Kerberos con NFSv3, la regola dei criteri di esportazione deve consentire `-rorule e`. `-rwrule` accesso a `sys` oltre a `krb5`. Ciò è dovuto alla necessità di consentire l'accesso NLM (Network Lock Manager) all'esportazione.

### 3. Specificare un mapping anonimo dell'ID utente.

Il `-anon` L'opzione specifica un ID utente UNIX o un nome utente mappato alle richieste del client che arrivano con un ID utente 0 (zero), che in genere è associato al nome utente `root`. Il valore predefinito è 65534. I client NFS in genere associano l'ID utente 65534 con il nome utente nessuno (noto anche come *root squashing*). In ONTAP, questo ID utente è associato all'utente `pcuser`. Per disattivare l'accesso da parte di qualsiasi client con un ID utente pari a 0, specificare un valore di 65535.

### 4. Selezionare l'ordine di indice della regola.

Il `-ruleindex` option specifica il numero di indice per la regola. Le regole vengono valutate in base al loro ordine nell'elenco dei numeri di indice; le regole con numeri di indice inferiori vengono valutate per prime. Ad esempio, la regola con indice numero 1 viene valutata prima della regola con indice numero 2.

Se si desidera aggiungere...	Quindi...
La prima regola per un criterio di esportazione	Invio 1.
Regole aggiuntive per una policy di esportazione	<div>a. Visualizzare le regole esistenti nel criterio: <code>vserver export-policy rule show -instance -policyname <i>your_policy</i></code></div> <div>b. Selezionare un numero di indice per la nuova regola in base all'ordine in cui deve essere valutata.</div>

### 5. Selezionare il valore di accesso NFS applicabile: `{nfs|nfs3|nfs4}`.

`nfs` corrisponde a qualsiasi versione, `nfs3` e `nfs4` associare solo le versioni specifiche.

### 6. Creare la regola di esportazione e aggiungerla a un criterio di esportazione esistente:

```
vserver export-policy rule create -vserver vserver_name -policyname policy_name -ruleindex integer -protocol {nfs|nfs3|nfs4} -clientmatch { text | "text,text,..." } -rorule security_type -rwrule security_type -superuser security_type -anon user_ID
```

### 7. Visualizzare le regole per il criterio di esportazione per verificare la presenza della nuova regola:

```
vserver export-policy rule show -policyname policy_name
```

Il comando visualizza un riepilogo per il criterio di esportazione, incluso un elenco di regole applicate a tale criterio. ONTAP assegna a ogni regola un numero di indice della regola. Una volta conosciuto il numero di indice della regola, è possibile utilizzarlo per visualizzare informazioni dettagliate sulla regola di esportazione specificata.



8. Verificare che le regole applicate ai criteri di esportazione siano configurate correttamente:

```
vserver export-policy rule show -policyname policy_name -vserver vserver_name
-ruleindex integer
```

### Esempi

I seguenti comandi creano e verificano la creazione di una regola di esportazione su SVM denominata vs1 in un criterio di esportazione denominato rs1. La regola ha il numero di indice 1. La regola corrisponde a qualsiasi client nel dominio eng.company.com e al netgroup @netgroup1. La regola attiva tutti gli accessi NFS. Consente l'accesso in sola lettura e in lettura/scrittura agli utenti autenticati con AUTH\_SYS. I client con ID utente UNIX 0 (zero) vengono anonimizzati a meno che non vengano autenticati con Kerberos.

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname expl
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5
```

```
vs1::> vserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs1	expl	1	nfs	eng.company.com, @netgroup1	sys

```
vs1::> vserver export-policy rule show -policyname expl -vserver vs1
-ruleindex 1
```

```

Vserver: vs1
Policy Name: expl
Rule Index: 1
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
RO Access Rule: sys
RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true
```

I seguenti comandi creano e verificano la creazione di una regola di esportazione su SVM denominata vs2 in un criterio di esportazione denominato expol2. La regola ha il numero di indice 21. La regola consente di confrontare i client con i membri del netgroup dev\_netgroup\_main. La regola attiva tutti gli accessi NFS. Consente l'accesso in sola lettura per gli utenti autenticati con AUTH\_SYS e richiede l'autenticazione Kerberos per l'accesso in lettura-scrittura e root. Ai client con ID utente UNIX 0 (zero) viene negato l'accesso root a meno che non vengano autenticati con Kerberos.

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5
```

```
vs2::> vserver export-policy rule show -policyname nfs_policy
```

Virtual Server	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
vs2	expol2	21	nfs	@dev_netgroup_main	sys

```
vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21
```

```

Vserver: vs2
Policy Name: expol2
Rule Index: 21
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
RO Access Rule: sys
RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
Superuser Security Types: krb5
Honor SetUID Bits in SETATTR: true
Allow Creation of Devices: true

```

## Creare un volume o un contenitore di storage qtrees

### Creare un volume

È possibile creare un volume e specificarne il punto di giunzione e altre proprietà utilizzando `volume create` comando.

### A proposito di questa attività

Un volume deve includere un *percorso di giunzione* per rendere i dati disponibili ai client. È possibile specificare il percorso di giunzione quando si crea un nuovo volume. Se si crea un volume senza specificare un percorso di giunzione, è necessario *montare* il volume nello spazio dei nomi SVM utilizzando `volume mount` comando.

### Prima di iniziare

- NFS deve essere configurato e in esecuzione.
- Lo stile di sicurezza SVM deve essere UNIX.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilità analisi del file system](#).

## Fasi

### 1. Creare il volume con un punto di giunzione:

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path [-policy
export_policy_name]
```

Le scelte per `-junction-path` sono i seguenti:

- Direttamente sotto root, ad esempio `/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio direttamente nel volume root SVM.

- In una directory esistente, ad esempio `/existing_dir/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio in un volume esistente (in una gerarchia esistente), espresso come directory.

Se si desidera creare un volume in una nuova directory (in una nuova gerarchia sotto un nuovo volume), ad esempio, `/new_dir/new_vol`, Quindi, è necessario creare prima un nuovo volume padre che sia congiunto al volume root SVM. Creare quindi il nuovo volume figlio nel percorso di giunzione del nuovo volume padre (nuova directory).

+ se si intende utilizzare un criterio di esportazione esistente, è possibile specificarlo al momento della creazione del volume. È inoltre possibile aggiungere un criterio di esportazione in un secondo momento con `volume modify` comando.

### 2. Verificare che il volume sia stato creato con il punto di giunzione desiderato:

```
volume show -vserver svm_name -volume volume_name -junction
```

## Esempi

Il seguente comando crea un nuovo volume denominato `users1` su SVM `vs1.example.com` e sull'aggregato `aggr1`. Il nuovo volume è disponibile all'indirizzo `/users`. Il volume ha una dimensione di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	users1	true	/users	RW_volume

Il seguente comando crea un nuovo volume denominato "home4" su SVM "vs1.example.com" e l'aggregato "aggr1". La directory /eng/ Esiste già nello spazio dei nomi per vs1 SVM e il nuovo volume è disponibile all'indirizzo /eng/home, che diventa la home directory di /eng/ namespace. Il volume è di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction

```

		Junction		Junction
Vserver	Volume	Active	Junction Path	Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

### Creare un qtree

È possibile creare un qtree per contenere i dati e specificarne le proprietà utilizzando volume qtree create comando.

#### Di cosa hai bisogno

- La SVM e il volume che conterrà il nuovo qtree devono già esistere.
- Lo stile di sicurezza SVM deve essere UNIX e NFS deve essere configurato e in esecuzione.

#### Fasi

##### 1. Creare il qtree:

```
volume qtree create -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree path } -security-style unix [-policy
export_policy_name]
```

È possibile specificare il volume e il qtree come argomenti separati o specificare l'argomento del percorso qtree nel formato /vol/volume\_name/\_qtree\_name.

Per impostazione predefinita, i qtree ereditano i criteri di esportazione del volume principale, ma possono essere configurati per l'utilizzo dei propri. Se si intende utilizzare un criterio di esportazione esistente, è possibile specificarlo al momento della creazione del qtree. È inoltre possibile aggiungere un criterio di esportazione in un secondo momento con volume qtree modify comando.

##### 2. Verificare che il qtree sia stato creato con il percorso di giunzione desiderato:

```
volume qtree show -vserver vserver_name { -volume volume_name -qtree
qtree_name | -qtree-path qtree path }
```

### Esempio

Nell'esempio seguente viene creato un qtree chiamato qt01 situato su SVM vs1.example.com che ha un percorso di giunzione /vol/data1:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path  
/vol/data1/qt01 -security-style unix  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path  
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com  
          Volume Name: data1  
          Qtree Name: qt01  
Actual (Non-Junction) Qtree Path: /vol/data1/qt01  
          Security Style: unix  
          Oplock Mode: enable  
          Unix Permissions: ---rwxr-xr-x  
          Qtree Id: 2  
          Qtree Status: normal  
          Export Policy: default  
Is Export Policy Inherited: true
```

## Accesso sicuro a NFS tramite policy di esportazione

### Accesso sicuro a NFS tramite policy di esportazione

È possibile utilizzare policy di esportazione per limitare l'accesso NFS a volumi o qtree a client che corrispondono a parametri specifici. Quando si effettua il provisioning di nuovo storage, è possibile utilizzare policy e regole esistenti, aggiungere regole a policy esistenti o creare nuove policy e regole. È inoltre possibile verificare la configurazione dei criteri di esportazione



A partire da ONTAP 9.3, è possibile attivare il controllo della configurazione dei criteri di esportazione come processo in background che registra eventuali violazioni delle regole in un elenco di regole di errore. Il `vserver export-policy config-checker` I comandi richiamano il controllo e visualizzano i risultati, che è possibile utilizzare per verificare la configurazione ed eliminare le regole errate dal criterio. I comandi convalidano solo la configurazione di esportazione per i nomi host, i netgroup e gli utenti anonimi.

### Gestire l'ordine di elaborazione delle regole di esportazione

È possibile utilizzare `vserver export-policy rule setindex` per impostare manualmente il numero di indice di una regola di esportazione esistente. In questo modo è possibile specificare la precedenza con cui ONTAP applica le regole di esportazione alle richieste del client.

#### A proposito di questa attività

Se il nuovo numero di indice è già in uso, il comando inserisce la regola nel punto specificato e riordina l'elenco di conseguenza.

## Fase

1. Modificare il numero di indice di una regola di esportazione specificata:

```
vserver export-policy rule setindex -vserver virtual_server_name -policyname  
policy_name -ruleindex integer -newruleindex integer
```

## Esempio

Il seguente comando modifica il numero di indice di una regola di esportazione al numero di indice 3 in quello 2 in una policy di esportazione denominata rs1 sulla SVM denominata vs1:

```
vs1::> vserver export-policy rule setindex -vserver vs1  
-policyname rs1 -ruleindex 3 -newruleindex 2
```

## Assegnare un criterio di esportazione a un volume

Ogni volume contenuto nella SVM deve essere associato a un criterio di esportazione che contenga regole di esportazione per consentire ai client di accedere ai dati nel volume.

### A proposito di questa attività

È possibile associare un criterio di esportazione a un volume quando si crea il volume o in qualsiasi momento dopo averlo creato. È possibile associare un criterio di esportazione al volume, anche se un criterio può essere associato a più volumi.

## Fasi

1. Se non è stato specificato un criterio di esportazione al momento della creazione del volume, assegnare un criterio di esportazione al volume:

```
volume modify -vserver vserver_name -volume volume_name -policy  
export_policy_name
```

2. Verificare che il criterio sia stato assegnato al volume:

```
volume show -volume volume_name -fields policy
```

## Esempio

I seguenti comandi assegnano il criterio di esportazione nfs\_policy al volume vol1 su SVM vs1 e ne verificano l'assegnazione:

```
cluster::> volume modify -vserver vs1 -volume vol1 -policy nfs_policy  
  
cluster::>volume show -volume vol -fields policy  
vserver volume      policy  
-----  
vs1      vol1      nfs_policy
```

## Assegnare un criterio di esportazione a un qtree

Invece di esportare un intero volume, è possibile esportare un qtree specifico su un volume per renderlo direttamente accessibile ai client. È possibile esportare un qtree assegnandogli un criterio di esportazione. È possibile assegnare il criterio di esportazione quando si crea un nuovo qtree o modificando un qtree esistente.

### Di cosa hai bisogno

Il criterio di esportazione deve esistere.

### A proposito di questa attività

Per impostazione predefinita, i qtree ereditano il criterio di esportazione padre del volume contenente, se non diversamente specificato al momento della creazione.

È possibile associare un criterio di esportazione a un qtree quando si crea il qtree o in qualsiasi momento dopo la creazione del qtree. È possibile associare un criterio di esportazione al qtree, anche se un criterio può essere associato a molti qtree.

### Fasi

1. Se non è stato specificato un criterio di esportazione al momento della creazione del qtree, assegnare un criterio di esportazione al qtree:

```
volume qtree modify -vserver vs1 -qtree-path /vol/vol1/qtree_name -export-policy export_policy_name
```

2. Verificare che il criterio sia stato assegnato al qtree:

```
volume qtree show -qtree qtree_name -fields export-policy
```

### Esempio

I seguenti comandi assegnano il criterio di esportazione `nfs_policy` al qtree `qt1` su SVM `vs1` e ne verificano l'assegnazione:

```
cluster::> volume modify -vserver vs1 -qtree-path /vol/vol1/qt1 -policy nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
-----
vs1      data1  qt01  nfs_policy
```

### Verificare l'accesso del client NFS dal cluster

È possibile consentire ai client selezionati di accedere alla condivisione impostando le autorizzazioni per i file UNIX su un host di amministrazione UNIX. È possibile controllare l'accesso del client utilizzando `vserver export-policy check-access`, regolando le regole di esportazione secondo necessità.

### Fasi

1. Nel cluster, controllare l'accesso del client alle esportazioni utilizzando `vserver export-policy check-access` comando.

Il seguente comando controlla l'accesso in lettura/scrittura per un client NFSv3 con l'indirizzo IP 1.2.3.4 nel volume home2. L'output del comando indica che il volume utilizza il criterio di esportazione `exp-home-dir` e che l'accesso è negato.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
```

Path	Policy	Policy Owner	Policy Owner Type	Rule Index	Access
/	default	vs1_root	volume	1	read
/eng	default	vs1_root	volume	1	read
/eng/home2	exp-home-dir	home2	volume	1	denied

3 entries were displayed.

2. Esaminare l'output per determinare se il criterio di esportazione funziona come previsto e se l'accesso client si comporta come previsto.

In particolare, è necessario verificare quali criteri di esportazione vengono utilizzati dal volume o dal qtree e il tipo di accesso che ne deriva dal client.

3. Se necessario, riconfigurare le regole dei criteri di esportazione.

## Verificare l'accesso NFS dai sistemi client

Dopo aver verificato l'accesso NFS al nuovo oggetto storage, è necessario verificare la configurazione accedendo a un host di amministrazione NFS e leggendo i dati da e scrivendo i dati su SVM. Ripetere il processo come utente non root su un sistema client.

### Di cosa hai bisogno

- Il sistema client deve disporre di un indirizzo IP consentito dalla regola di esportazione specificata in precedenza.
- È necessario disporre delle informazioni di accesso per l'utente root.

### Fasi

1. Sul cluster, verificare l'indirizzo IP della LIF che ospita il nuovo volume:

```
network interface show -vserver svm_name
```

2. Accedere come utente root al sistema client host di amministrazione.
3. Modificare la directory nella cartella mount:

```
cd /mnt/
```



4. Creare e montare una nuova cartella utilizzando l'indirizzo IP di SVM:

a. Creare una nuova cartella:

```
mkdir /mnt/folder
```

b. Montare il nuovo volume in questa nuova directory:

```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

c. Modificare la directory nella nuova cartella:

```
cd folder
```

I seguenti comandi creano una cartella denominata test1, montano il volume vol1 all'indirizzo IP 192.0.2.130 sulla cartella di montaggio test1 e cambiano nella nuova directory test1:

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. Creare un nuovo file, verificarne l'esistenza e scriverne del testo:

a. Creare un file di test:

```
touch filename
```

b. Verificare che il file esista.:

```
ls -l filename
```

c. Immettere:

```
cat > filename
```

Digitare del testo, quindi premere Ctrl+D per scrivere il testo nel file di prova.

d. Visualizzare il contenuto del file di test.

```
cat filename
```

e. Rimuovere il file di test:

```
rm filename
```

f. Tornare alla directory principale:

```
cd ..
```

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. Come root, impostare la proprietà e le autorizzazioni UNIX desiderate sul volume montato.

7. Su un sistema client UNIX identificato nelle regole di esportazione, accedere come uno degli utenti autorizzati che ora ha accesso al nuovo volume e ripetere le procedure descritte nei passaggi da 3 a 5 per verificare che sia possibile montare il volume e creare un file.

## Dove trovare ulteriori informazioni

Una volta verificato l'accesso al client NFS, è possibile eseguire una configurazione NFS aggiuntiva o aggiungere l'accesso SAN. Una volta completato l'accesso al protocollo, è necessario proteggere il volume root della SVM (Storage Virtual Machine).

### Configurazione NFS

È possibile configurare ulteriormente l'accesso NFS utilizzando le seguenti informazioni e report tecnici:

- ["Gestione NFS"](#)

Descrive come configurare e gestire l'accesso ai file utilizzando NFS.

- ["Report tecnico di NetApp 4067: Guida all'implementazione e alle Best practice di NFS"](#)

Funge da guida operativa NFSv3 e NFSv4 e fornisce una panoramica del sistema operativo ONTAP con particolare attenzione a NFSv4.

- ["Report tecnico di NetApp 4073: Autenticazione unificata sicura"](#)

Spiega come configurare ONTAP per l'utilizzo con server Kerberos versione 5 (krb5) basati su UNIX per l'autenticazione dello storage NFS e Active Directory (ad) come provider di identità KDC e LDAP (Lightweight Directory Access Protocol).

- ["Report tecnico di NetApp 3580: Guida ai miglioramenti e alle Best practice di NFSv4 per l'implementazione di Data ONTAP"](#)

Descrive le Best practice da seguire durante l'implementazione dei componenti NFSv4 su client AIX, Linux o Solaris collegati a sistemi che eseguono ONTAP.

### Configurazione di rete

È possibile configurare ulteriormente le funzioni di rete e i servizi di gestione dei nomi utilizzando i seguenti report tecnici e informativi:

- ["Gestione NFS"](#)

Descrive come configurare e gestire il networking ONTAP.

- ["Report tecnico di NetApp 4182: Considerazioni sulla progettazione dello storage Ethernet e Best practice per le configurazioni di Clustered Data ONTAP"](#)

Descrive l'implementazione delle configurazioni di rete ONTAP e fornisce scenari di implementazione di rete comuni e consigli sulle Best practice.

- ["Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"](#)

Spiega come configurare LDAP, NIS, DNS e la configurazione dei file locali per scopi di autenticazione.

## Configurazione del protocollo SAN

Se si desidera fornire o modificare l'accesso SAN alla nuova SVM, è possibile utilizzare le informazioni di configurazione FC o iSCSI, disponibili per più sistemi operativi host.

## Protezione del volume root

Dopo aver configurato i protocolli su SVM, assicurarsi che il volume root sia protetto:

- ["Protezione dei dati"](#)

Descrive come creare un mirror di condivisione del carico per proteggere il volume root SVM, una Best practice NetApp per le SVM abilitate per NAS. Viene inoltre descritto come eseguire rapidamente il ripristino da guasti o perdite di volume promuovendo il volume root SVM da un mirror di condivisione del carico.

## Le differenze tra le esportazioni ONTAP e quelle 7-Mode

### Le differenze tra le esportazioni ONTAP e quelle 7-Mode

Se non si ha familiarità con il modo in cui ONTAP implementa le esportazioni NFS, è possibile confrontare i tool di configurazione per l'esportazione di 7-Mode e ONTAP, oltre a 7-Mode di esempio `/etc/exports` file con criteri e regole in cluster.

In ONTAP non c'è `/etc/exports` file e no `exportfs` comando. È invece necessario definire un criterio di esportazione. Le policy di esportazione consentono di controllare l'accesso al client in maniera molto simile a quella di 7-Mode, ma offrono funzionalità aggiuntive come la possibilità di riutilizzare la stessa policy di esportazione per più volumi.

### Informazioni correlate


["Gestione NFS"](#)

["Report tecnico di NetApp 4067: Guida all'implementazione e alle Best practice di NFS"](#)

### Confronto delle esportazioni in 7-Mode e ONTAP

Le esportazioni in ONTAP sono definite e utilizzate in modo diverso rispetto agli ambienti 7-Mode.

Aree di differenza	7-Mode	ONTAP
Come vengono definite le esportazioni	Le esportazioni sono definite in <code>/etc/exports</code> file.	Le esportazioni vengono definite creando una policy di esportazione all'interno di una SVM. Una SVM può includere più criteri di esportazione.

Scopo dell'esportazione	<ul style="list-style-type: none"> <li>• Le esportazioni si applicano a un percorso di file o qtree specificato.</li> <li>• È necessario creare una voce separata in <code>/etc/exports</code> per ogni percorso di file o qtree.</li> <li>• Le esportazioni sono persistenti solo se sono definite in <code>/etc/exports</code> file.</li> </ul>	<ul style="list-style-type: none"> <li>• I criteri di esportazione si applicano a un intero volume, inclusi tutti i percorsi di file e i qtree contenuti nel volume.</li> <li>• Se si desidera, è possibile applicare i criteri di esportazione a più volumi.</li> <li>• Tutte le policy di esportazione sono persistenti durante i riavvii del sistema.</li> </ul>
Recinzione (specifica di accessi diversi per client specifici per le stesse risorse)	Per fornire a client specifici un accesso diverso a una singola risorsa esportata, è necessario elencare ciascun client e l'accesso consentito in <code>/etc/exports</code> file.	Le policy di esportazione sono composte da una serie di regole di esportazione individuali. Ogni regola di esportazione definisce autorizzazioni di accesso specifiche per una risorsa ed elenca i client che dispongono di tali autorizzazioni. Per specificare un accesso diverso per client specifici, è necessario creare una regola di esportazione per ogni set specifico di autorizzazioni di accesso, elencare i client che dispongono di tali autorizzazioni e aggiungere le regole ai criteri di esportazione.
Alias del nome	Quando si definisce un'esportazione, è possibile scegliere di rendere il nome dell'esportazione diverso dal nome del percorso del file. Utilizzare il <code>-actual</code> quando si definisce un'esportazione in <code>/etc/exports</code> file.	<p>È possibile scegliere di rendere il nome del volume esportato diverso dal nome del volume effettivo. A tale scopo, è necessario montare il volume con un nome di percorso di giunzione personalizzato all'interno dello spazio dei nomi SVM.</p> <div>  <p>Per impostazione predefinita, i volumi vengono montati con il relativo nome del volume. Per personalizzare il nome del percorso di giunzione di un volume, è necessario smontarlo, rinominarlo e rimontarlo.</p> </div>

## Esempi di policy di esportazione ONTAP

È possibile rivedere criteri di esportazione di esempio per comprendere meglio il funzionamento delle policy di esportazione in ONTAP.

### Esempio di implementazione ONTAP di un'esportazione in 7-Mode

Nell'esempio riportato di seguito viene illustrata un'esportazione in 7-Mode così come viene visualizzata in `/etc/export` file:

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:  
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

Per riprodurre questa esportazione come criterio di esportazione in cluster, è necessario creare un criterio di esportazione con tre regole di esportazione e quindi assegnare il criterio di esportazione al volume vol1.

Regola	Elemento	Valore
Regola 1	-clientmatch (specifica del client)	@readonly_netgroup
-ruleindex(posizione della regola di esportazione nell'elenco delle regole)	1	-protocol
nfs	-rorule(consenti accesso di sola lettura)	sys (Client autenticato con AUTH_SYS)
-rwrule(consenti accesso in lettura/scrittura)	never	-superuser(consenti accesso superutente)
none(root <i>squashed</i> ad anon)	Articolo 2	-clientmatch
@rootaccess_netgroup	-ruleindex	2
-protocol	nfs	-rorule
sys	-rwrule	sys
-superuser	sys	Articolo 3
-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2	-ruleindex
3	-protocol	nfs

Regola	Elemento	Valore
-rorule	sys	-rwrule
sys	-superuser	none

1. Creare una policy di esportazione chiamata exp\_vol1:

```
vserver export-policy create -vserver NewSVM -policyname exp_vol1
```

2. Creare tre regole con i seguenti parametri nel comando base:

- Comando di base:

```
vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
```

- Parametri della regola:

```
-clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
-rwrule never -superuser none+ -clientmatch @rootaccess_netgroup -ruleindex
2 -protocol nfs -rorule sys -rwrule sys -superuser sys+ -clientmatch
@readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3 -protocol nfs -rorule
sys -rwrule sys -superuser none
```

3. Assegnare il criterio al volume vol1:

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

### Esempio di consolidamento delle esportazioni 7-Mode

L'esempio seguente mostra un 7-Mode /etc/export file che include una riga per ciascuno dei 10 qtree:

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

In ONTAP, è necessario uno dei due criteri per ogni qtree: Uno con una regola che include -clientmatch host1519s, o con una regola che include -clientmatch host2057s.

1. Creare due policy di esportazione chiamate exp\_vol1q1 e exp\_vol1q2:

- vserver export-policy create -vserver NewSVM -policyname exp\_vol1q1

- vserver export-policy create -vserver NewSVM -policyname exp\_vol1q2

2. Creare una regola per ogni policy:

- `vserver export-policy rule create -vserver NewSVM -policyname exp_vollq1 -clientmatch host1519s -rwrule sys -superuser sys`
- `vserver export-policy rule create -vserver NewSVM -policyname exp_vollq2 -clientmatch host1519s -rwrule sys -superuser sys`

### 3. Applicare i criteri alle qtree:

- `volume qtree modify -vserver NewSVM -qtree-path /vol/voll/q_1472 -export -policy exp_vollq1`
- [prossimo 4 qtree...]
- `volume qtree modify -vserver NewSVM -qtree-path /vol/voll/q_2237 -export -policy exp_vollq2`
- [prossimo 4 qtree...]

Se in un secondo momento è necessario aggiungere qtree aggiuntivi per tali host, si utilizzerebbero le stesse policy di esportazione.

## Gestisci NFS con la CLI

### Panoramica di riferimento di NFS

ONTAP include funzionalità di accesso ai file disponibili per il protocollo NFS. È possibile attivare un server NFS ed esportare volumi o qtree.

Eseguire questa procedura nei seguenti casi:

- Vuoi conoscere la gamma di funzionalità del protocollo NFS di ONTAP.
- Si desidera eseguire attività di configurazione e manutenzione meno comuni, non la configurazione NFS di base.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

## Comprendere l'accesso al file NAS

### Spazi dei nomi e punti di giunzione

#### Panoramica degli spazi dei nomi e dei punti di giunzione

Un *namespace* NAS è un raggruppamento logico di volumi Uniti in *punti di giunzione* per creare una singola gerarchia di file system. Un client con autorizzazioni sufficienti può accedere ai file nello spazio dei nomi senza specificare la posizione dei file nello storage. I volumi Junctioned possono risiedere in qualsiasi punto del cluster.

Invece di montare ogni volume contenente un file di interesse, i client NAS montano un NFS *export* o accedono a una *share*. SMB. L'esportazione o la condivisione rappresenta l'intero namespace o una posizione intermedia all'interno dello spazio dei nomi. Il client accede solo ai volumi montati sotto il proprio access point.

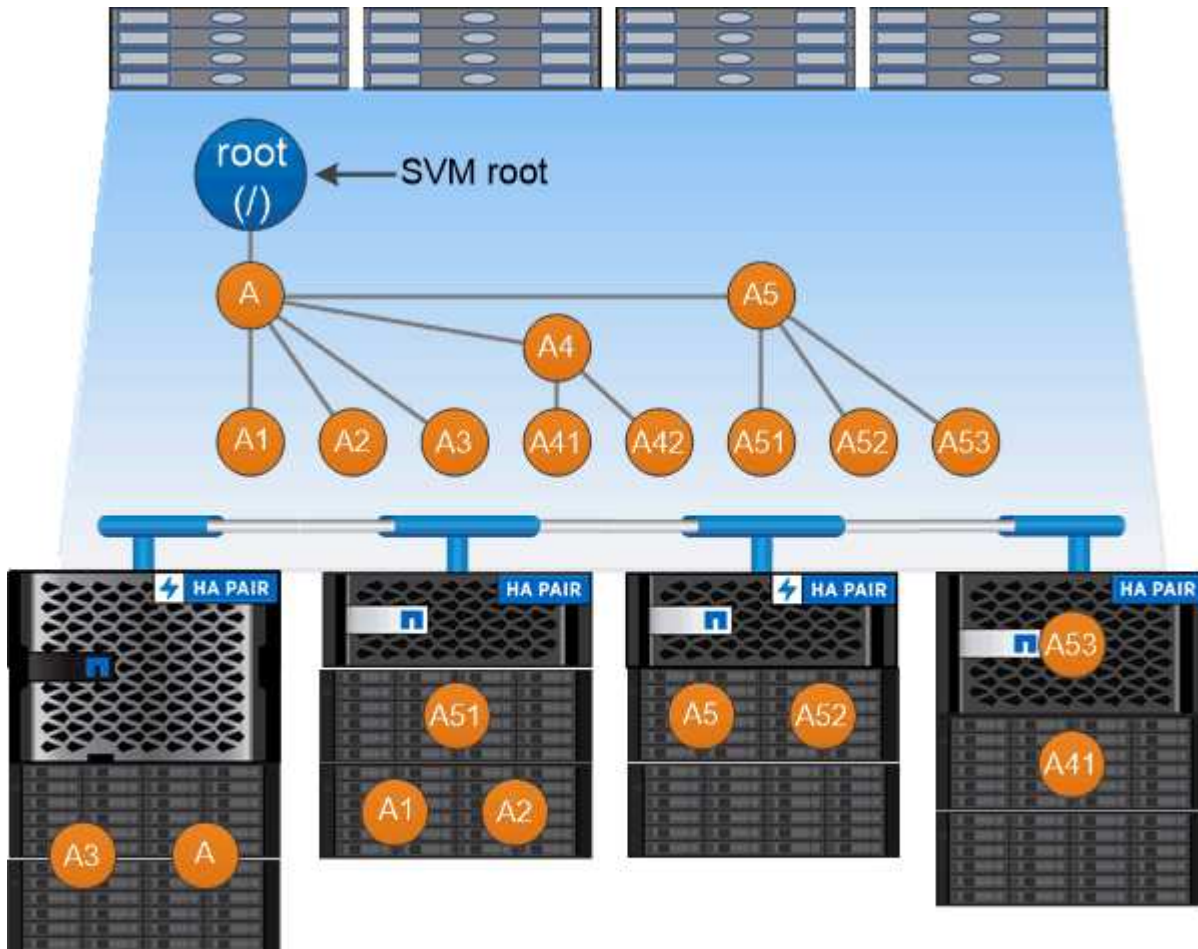
È possibile aggiungere volumi allo spazio dei nomi in base alle esigenze. È possibile creare punti di giunzione direttamente sotto una giunzione di un volume padre o in una directory all'interno di un volume. Il percorso di

una giunzione di volume per un volume denominato “vol3” potrebbe essere /vol1/vol2/vol3, o. /vol1/dir2/vol3, o persino /dir1/dir2/vol3. Il percorso è chiamato *percorso di giunzione*.

Ogni SVM dispone di uno spazio dei nomi univoco. Il volume root SVM è il punto di ingresso della gerarchia dello spazio dei nomi.



Per garantire che i dati rimangano disponibili in caso di interruzione o failover di un nodo, è necessario creare una copia *mirror per la condivisione del carico* per il volume root SVM.



*A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.*

### Esempio

Nell'esempio riportato di seguito viene creato un volume denominato “home4” situato su SVM vs1 con un percorso di giunzione /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```



## Quali sono le tipiche architetture dello spazio dei nomi NAS

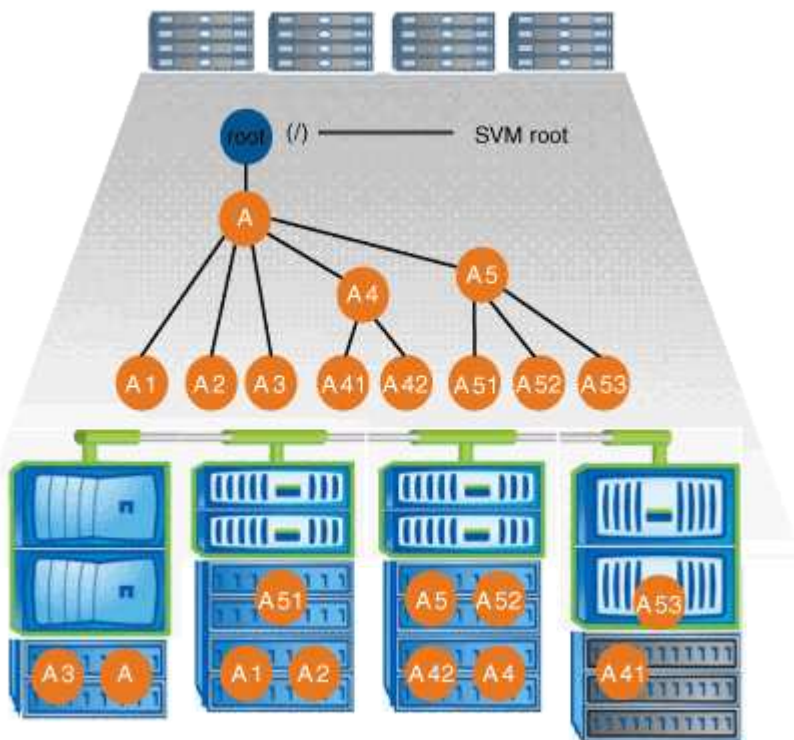
Esistono diverse architetture dello spazio dei nomi NAS tipiche che è possibile utilizzare per creare lo spazio dei nomi SVM. È possibile scegliere l'architettura dello spazio dei nomi che soddisfa le esigenze di business e workflow.

La parte superiore dello spazio dei nomi è sempre il volume root, rappresentato da una barra (/). L'architettura dello spazio dei nomi sotto la radice si suddivide in tre categorie di base:

- Un singolo albero ramificato, con una sola giunzione alla radice dello spazio dei nomi
- Più alberi ramificati, con più punti di giunzione alla radice dello spazio dei nomi
- Più volumi standalone, ciascuno con un punto di giunzione separato per la radice dello spazio dei nomi

### Namespace con singolo albero ramificato

Un'architettura con un singolo albero ramificato ha un singolo punto di inserimento alla radice dello spazio dei nomi SVM. Il singolo punto di inserimento può essere un volume giuntato o una directory sotto la root. Tutti gli altri volumi vengono montati nei punti di giunzione sotto il singolo punto di inserimento (che può essere un volume o una directory).

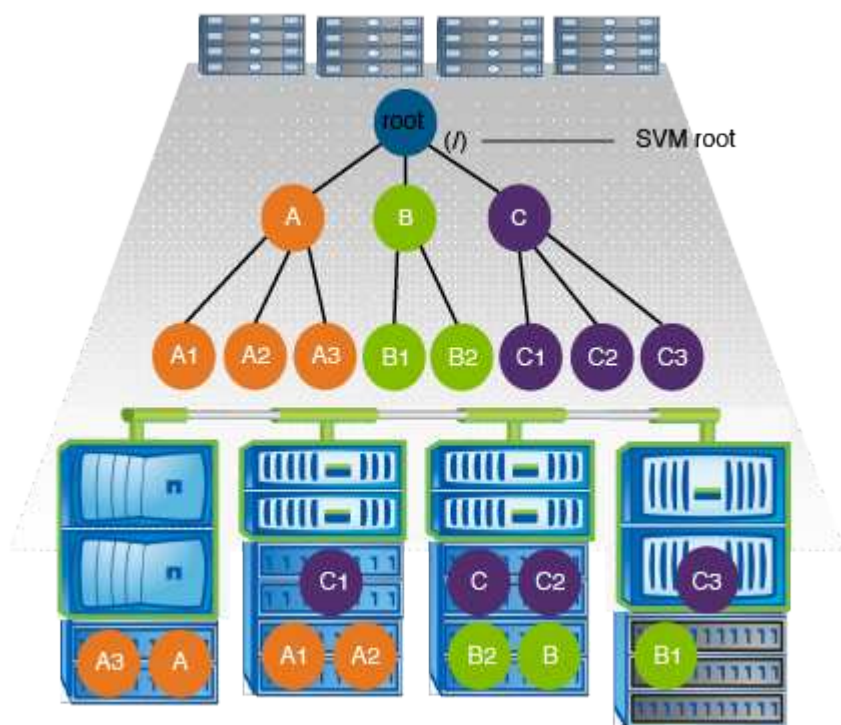


Ad esempio, una configurazione tipica di giunzione di volumi con l'architettura dello spazio dei nomi sopra descritta potrebbe essere simile alla seguente configurazione, in cui tutti i volumi sono congiunti sotto il singolo punto di inserimento, che è una directory denominata "data":

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	corp1	true	/data/dir1/corp1	RW_volume
vs1	corp2	true	/data/dir1/corp2	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	eng1	true	/data/data1/eng1	RW_volume
vs1	eng2	true	/data/data1/eng2	RW_volume
vs1	sales	true	/data/data1/sales	RW_volume
vs1	vol1	true	/data/vol1	RW_volume
vs1	vol2	true	/data/vol2	RW_volume
vs1	vol3	true	/data/vol3	RW_volume
vs1	vs1_root	-	/	-

### Namespace con più alberi ramificati

Un'architettura con più alberi ramificati ha più punti di inserimento alla radice dello spazio dei nomi SVM. I punti di inserimento possono essere volumi congiunti o directory sotto la radice. Tutti gli altri volumi vengono montati nei punti di giunzione sotto i punti di inserimento (che possono essere volumi o directory).

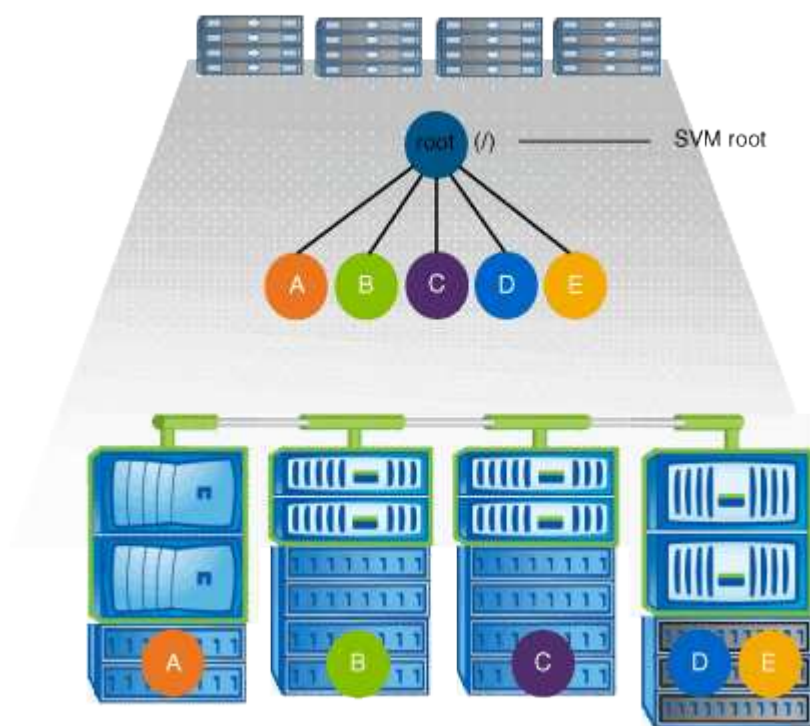


Ad esempio, una configurazione tipica di giunzione del volume con l'architettura dello spazio dei nomi di cui sopra potrebbe essere simile alla seguente configurazione, in cui sono presenti tre punti di inserimento nel volume root della SVM. Due punti di inserimento sono directory denominate "data" e "projects". Un punto di inserimento è un volume giuntato denominato "audit":

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	audit	true	/audit	RW_volume
vs1	audit_logs1	true	/audit/logs1	RW_volume
vs1	audit_logs2	true	/audit/logs2	RW_volume
vs1	audit_logs3	true	/audit/logs3	RW_volume
vs1	eng	true	/data/eng	RW_volume
vs1	mktg1	true	/data/mktg1	RW_volume
vs1	mktg2	true	/data/mktg2	RW_volume
vs1	project1	true	/projects/project1	RW_volume
vs1	project2	true	/projects/project2	RW_volume
vs1	vs1_root	-	/	-

### Namespace con più volumi standalone

In un'architettura con volumi standalone, ogni volume ha un punto di inserimento nella directory principale dello spazio dei nomi SVM; tuttavia, il volume non è giuntato sotto un altro volume. Ogni volume ha un percorso univoco ed è posto direttamente sotto la root oppure è posto sotto una directory sotto la root.



Ad esempio, una configurazione tipica di giunzione del volume con l'architettura dello spazio dei nomi di cui sopra potrebbe essere simile alla seguente configurazione, in cui sono presenti cinque punti di inserimento nel volume root della SVM, con ciascun punto di inserimento che rappresenta un percorso per un volume.

Vserver	Volume	Junction		Junction
		Active	Junction Path	Path Source
vs1	eng	true	/eng	RW_volume
vs1	mktg	true	/vol/mktg	RW_volume
vs1	project1	true	/project1	RW_volume
vs1	project2	true	/project2	RW_volume
vs1	sales	true	/sales	RW_volume
vs1	vs1_root	-	/	-

## Come ONTAP controlla l'accesso ai file

### Panoramica delle modalità di controllo dell'accesso ai file da parte di ONTAP

ONTAP controlla l'accesso ai file in base alle restrizioni basate sull'autenticazione e sui file specificate dall'utente.

Quando un client si connette al sistema di storage per accedere ai file, ONTAP deve eseguire due operazioni:

- Autenticazione

ONTAP deve autenticare il client verificando l'identità con un'origine attendibile. Inoltre, il tipo di autenticazione del client è un metodo che può essere utilizzato per determinare se un client può accedere ai dati durante la configurazione dei criteri di esportazione (facoltativo per CIFS).

- Autorizzazione

ONTAP deve autorizzare l'utente confrontando le credenziali dell'utente con le autorizzazioni configurate nel file o nella directory e determinando il tipo di accesso, se presente, da fornire.

Per gestire correttamente il controllo dell'accesso ai file, ONTAP deve comunicare con servizi esterni come server NIS, LDAP e Active Directory. La configurazione di un sistema storage per l'accesso ai file mediante CIFS o NFS richiede la configurazione dei servizi appropriati in base all'ambiente in uso in ONTAP.

### Restrizioni basate sull'autenticazione

Con le restrizioni basate sull'autenticazione, è possibile specificare quali macchine client e quali utenti possono connettersi alla SVM (Storage Virtual Machine).

ONTAP supporta l'autenticazione Kerberos da server UNIX e Windows.

### Restrizioni basate su file

ONTAP valuta tre livelli di sicurezza per determinare se un'entità è autorizzata a eseguire un'azione richiesta su file e directory che risiedono su una SVM. L'accesso è determinato dalle autorizzazioni effettive dopo la valutazione dei tre livelli di protezione.

Qualsiasi oggetto di storage può contenere fino a tre tipi di livelli di sicurezza:

- Sicurezza di esportazione (NFS) e condivisione (SMB)

La sicurezza di esportazione e condivisione si applica all'accesso client a una data esportazione NFS o condivisione SMB. Gli utenti con privilegi amministrativi possono gestire la sicurezza a livello di esportazione e condivisione dai client SMB e NFS.

- Protezione di file e directory di Access Guard a livello di storage

La sicurezza di Access Guard a livello di storage si applica all'accesso dei client SMB e NFS ai volumi SVM. Sono supportate solo le autorizzazioni di accesso NTFS. Affinché ONTAP esegua controlli di sicurezza sugli utenti UNIX per l'accesso ai dati sui volumi per i quali è stato applicato Storage-Level Access Guard, l'utente UNIX deve eseguire il mapping a un utente Windows sulla SVM proprietaria del volume.



Se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, la protezione Storage-Level Access Guard non viene visualizzata. La protezione di Storage-Level Access Guard non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX).

- Sicurezza nativa a livello di file in NTFS, UNIX e NFSv4

La protezione nativa a livello di file esiste nel file o nella directory che rappresenta l'oggetto di storage. È possibile impostare la sicurezza a livello di file da un client. Le autorizzazioni dei file sono efficaci indipendentemente dal fatto che SMB o NFS vengano utilizzati per accedere ai dati.

## Come ONTAP gestisce l'autenticazione del client NFS

### Panoramica su come ONTAP gestisce l'autenticazione del client NFS

I client NFS devono essere autenticati correttamente prima di poter accedere ai dati sulla SVM. ONTAP autentica i client verificando le credenziali UNIX in base ai servizi di nomi configurati.

Quando un client NFS si connette a SVM, ONTAP ottiene le credenziali UNIX per l'utente controllando i diversi name service, a seconda della configurazione dei name service di SVM. ONTAP può controllare le credenziali per gli account UNIX locali, i domini NIS e i domini LDAP. Almeno uno di questi deve essere configurato in modo che ONTAP possa autenticare correttamente l'utente. È possibile specificare più servizi di nomi e l'ordine in cui ONTAP li cerca.

In un ambiente NFS puro con stili di sicurezza dei volumi UNIX, questa configurazione è sufficiente per autenticare e fornire l'accesso corretto ai file per un utente che si connette da un client NFS.

Se si utilizzano stili di protezione di volumi misti, NTFS o unificati, ONTAP deve ottenere un nome utente SMB per l'utente UNIX per l'autenticazione con un controller di dominio Windows. Ciò può avvenire mappando singoli utenti utilizzando account UNIX locali o domini LDAP oppure utilizzando un utente SMB predefinito. È possibile specificare quali servizi di nomi ONTAP esegue la ricerca in quale ordine o specificare un utente SMB predefinito.

### Modalità di utilizzo dei servizi di nome da parte di ONTAP

ONTAP utilizza i name service per ottenere informazioni su utenti e client. ONTAP utilizza queste informazioni per autenticare gli utenti che accedono ai dati sul sistema di storage o ne amministrano l'amministrazione e per mappare le credenziali dell'utente in un

ambiente misto.

Quando si configura il sistema di storage, è necessario specificare i servizi dei nomi che si desidera utilizzare per ottenere le credenziali utente per l'autenticazione di ONTAP. ONTAP supporta i seguenti servizi per i nomi:

- Utenti locali (file)
- NIS (External NIS Domain)
- Domini LDAP esterni (LDAP)

Si utilizza `vserver services name-service ns-switch` Famiglia di comandi per configurare le SVM con le origini per la ricerca delle informazioni di rete e l'ordine in cui eseguirne la ricerca. Questi comandi forniscono le funzionalità equivalenti di `/etc/nsswitch.conf` File su sistemi UNIX.

Quando un client NFS si connette a SVM, ONTAP verifica i servizi dei nomi specificati per ottenere le credenziali UNIX per l'utente. Se i name service sono configurati correttamente e ONTAP è in grado di ottenere le credenziali UNIX, ONTAP autentica correttamente l'utente.

In un ambiente con stili di sicurezza misti, ONTAP potrebbe dover mappare le credenziali dell'utente. Per consentire a ONTAP di mappare correttamente le credenziali dell'utente, è necessario configurare i name service in modo appropriato per l'ambiente in uso.

ONTAP utilizza inoltre i servizi di nome per autenticare gli account amministratore di SVM. È necessario tenere presente questo aspetto durante la configurazione o la modifica dello switch del name service per evitare di disattivare accidentalmente l'autenticazione per gli account amministratore SVM. Per ulteriori informazioni sugli utenti di amministrazione di SVM, vedere ["Autenticazione amministratore e RBAC"](#).

#### **In che modo ONTAP garantisce l'accesso ai file SMB dai client NFS**

ONTAP utilizza la semantica di protezione del file system di Windows NT per determinare se un utente UNIX, su un client NFS, ha accesso a un file con autorizzazioni NTFS.

A tale scopo, ONTAP converte l'ID utente UNIX dell'utente in una credenziale SMB e utilizza la credenziale SMB per verificare che l'utente disponga dei diritti di accesso al file. Una credenziale SMB è costituita da un identificatore di protezione (SID) primario, di solito il nome utente Windows dell'utente, e da uno o più SID di gruppo che corrispondono ai gruppi Windows di cui l'utente è membro.

Il tempo impiegato da ONTAP per convertire l'UID UNIX in una credenziale SMB può essere compreso tra decine di millisecondi e centinaia di millisecondi, poiché il processo richiede il contatto con un controller di dominio. ONTAP esegue il mapping dell'UID alla credenziale SMB e inserisce il mapping in una cache delle credenziali per ridurre il tempo di verifica causato dalla conversione.

#### **Come funziona la cache delle credenziali NFS**

Quando un utente NFS richiede l'accesso alle esportazioni NFS sul sistema di storage, ONTAP deve recuperare le credenziali dell'utente dai name server esterni o dai file locali per autenticare l'utente. ONTAP memorizza quindi queste credenziali in una cache interna per riferimenti futuri. La comprensione del funzionamento delle cache delle credenziali NFS consente di gestire potenziali problemi di performance e accesso.

Senza la cache delle credenziali, ONTAP dovrebbe eseguire query sui servizi dei nomi ogni volta che un utente NFS ha richiesto l'accesso. In un sistema storage occupato a cui molti utenti accedono, questo può causare rapidamente gravi problemi di performance, causando ritardi indesiderati o addirittura negazioni



dell'accesso al client NFS.

Con la cache delle credenziali, ONTAP recupera le credenziali dell'utente e le memorizza per un periodo di tempo prestabilito per un accesso rapido e semplice nel caso in cui il client NFS invii un'altra richiesta. Questo metodo offre i seguenti vantaggi:

- Semplifica il carico sul sistema storage gestendo meno richieste ai name server esterni (come NIS o LDAP).
- Semplifica il carico sui server dei nomi esterni inviando loro un numero inferiore di richieste.
- Accelera l'accesso degli utenti eliminando i tempi di attesa per ottenere le credenziali da origini esterne prima che l'utente possa essere autenticato.

ONTAP memorizza le credenziali positive e negative nella cache delle credenziali. Le credenziali positive significano che l'utente è stato autenticato e ha ottenuto l'accesso. Le credenziali negative significano che l'utente non è stato autenticato e l'accesso è stato negato.

Per impostazione predefinita, ONTAP memorizza le credenziali positive per 24 ore, ovvero, dopo l'autenticazione iniziale di un utente, ONTAP utilizza le credenziali memorizzate nella cache per tutte le richieste di accesso da parte di tale utente per 24 ore. Se l'utente richiede l'accesso dopo 24 ore, il ciclo ha inizio: ONTAP ignora le credenziali memorizzate nella cache e ottiene nuovamente le credenziali dall'origine del name service appropriata. Se le credenziali sono state modificate nel server dei nomi durante le 24 ore precedenti, ONTAP memorizza nella cache le credenziali aggiornate per l'utilizzo nelle 24 ore successive.

Per impostazione predefinita, ONTAP memorizza le credenziali negative per due ore, ovvero, dopo aver inizialmente negato l'accesso a un utente, ONTAP continua a negare qualsiasi richiesta di accesso da parte di tale utente per due ore. Se l'utente richiede l'accesso dopo 2 ore, il ciclo ricomincia: ONTAP ottiene nuovamente le credenziali dall'origine del name service appropriata. Se le credenziali sono state modificate nel server dei nomi nelle due ore precedenti, ONTAP memorizza nella cache le credenziali aggiornate per l'utilizzo nelle due ore successive.

## Creare e gestire volumi di dati in spazi dei nomi NAS

### Creare volumi di dati con punti di giunzione specificati

È possibile specificare il punto di giunzione quando si crea un volume di dati. Il volume risultante viene montato automaticamente nel punto di giunzione ed è immediatamente disponibile per la configurazione dell'accesso NAS.

#### Prima di iniziare

- L'aggregato in cui si desidera creare il volume deve già esistere.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilita analisi del file system](#).



I seguenti caratteri non possono essere utilizzati nel percorso di giunzione: \* N. " > < | ? .

+ inoltre, la lunghezza del percorso di giunzione non può superare i 255 caratteri.

## Fasi

### 1. Creare il volume con un punto di giunzione:

```
volume create -vserver vs1 -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path junction_path
```

Il percorso di giunzione deve iniziare con root (/) e può contenere sia directory che volumi congiunti. Il percorso di giunzione non deve contenere il nome del volume. I percorsi di giunzione sono indipendenti dal nome del volume.

Specificare uno stile di sicurezza del volume è facoltativo. Se non si specifica uno stile di protezione, ONTAP crea il volume con lo stesso stile di protezione applicato al volume root della macchina virtuale di storage (SVM). Tuttavia, lo stile di sicurezza del volume root potrebbe non corrispondere allo stile di sicurezza che si desidera applicare al volume di dati creato. Si consiglia di specificare lo stile di protezione quando si crea il volume per ridurre al minimo i problemi di accesso ai file difficili da risolvere.

Il percorso di giunzione è privo di maiuscole e minuscole; /ENG è uguale a. /eng. Se si crea una condivisione CIFS, Windows considera il percorso di giunzione come se fosse sensibile alla distinzione tra maiuscole e minuscole. Ad esempio, se la giunzione è /ENG, il percorso di una condivisione SMB deve iniziare con /ENG, non /eng.

Per personalizzare un volume di dati, è possibile utilizzare molti parametri opzionali. Per ulteriori informazioni, consultare le pagine man del `volume create` comando.

### 2. Verificare che il volume sia stato creato con il punto di giunzione desiderato:

```
volume show -vserver vs1 -volume volume_name -junction
```

## Esempio

Nell'esempio riportato di seguito viene creato un volume denominato "home4" situato su SVM vs1 con un percorso di giunzione /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -volume home4 -junction
```

		Junction		Junction
Vserver	Volume	Active	Junction Path	Path Source
vs1	home4	true	/eng/home	RW_volume

## Creare volumi di dati senza specificare punti di giunzione

È possibile creare un volume di dati senza specificare un punto di giunzione. Il volume risultante non viene montato automaticamente e non è disponibile per la configurazione per l'accesso NAS. È necessario montare il volume prima di poter configurare le condivisioni SMB o le esportazioni NFS per quel volume.



## Prima di iniziare

- L'aggregato in cui si desidera creare il volume deve già esistere.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilita analisi del file system](#).

## Fasi

1. Creare il volume senza un punto di giunzione utilizzando il seguente comando:

```
volume create -vserver vs1 -volume volume_name -aggregate
aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed}
```

Specificare uno stile di sicurezza del volume è facoltativo. Se non si specifica uno stile di protezione, ONTAP crea il volume con lo stesso stile di protezione applicato al volume root della macchina virtuale di storage (SVM). Tuttavia, lo stile di sicurezza del volume root potrebbe non corrispondere allo stile di sicurezza che si desidera applicare al volume di dati. Si consiglia di specificare lo stile di protezione quando si crea il volume per ridurre al minimo i problemi di accesso ai file difficili da risolvere.

Per personalizzare un volume di dati, è possibile utilizzare molti parametri opzionali. Per ulteriori informazioni, consultare le pagine man del `volume create` comando.

2. Verificare che il volume sia stato creato senza un punto di giunzione:

```
volume show -vserver vs1 -volume volume_name -junction
```

## Esempio

Nell'esempio seguente viene creato un volume denominato "sales" situato su SVM vs1 che non è montato in un punto di giunzione:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

		Junction		Junction
Vserver	Volume	Active	Junction Path	Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

## Montare o smontare i volumi esistenti nello spazio dei nomi NAS

È necessario montare un volume sullo spazio dei nomi NAS prima di poter configurare l'accesso del client NAS ai dati contenuti nei volumi SVM (Storage Virtual Machine). È possibile montare un volume su un punto di giunzione se non è attualmente montato. È anche possibile smontare i volumi.

### A proposito di questa attività

Se si smonta e si porta un volume offline, tutti i dati all'interno del punto di giunzione, inclusi i dati nei volumi con punti di giunzione contenuti nello spazio dei nomi del volume non montato, sono inaccessibili ai client NAS.



Per interrompere l'accesso del client NAS a un volume, non è sufficiente smontare semplicemente il volume. È necessario portare il volume offline o eseguire altre operazioni per assicurarsi che le cache degli handle dei file sul lato client siano invalidate. Per ulteriori informazioni, consultare il seguente articolo della Knowledge base:

["I client NFSv3 hanno ancora accesso a un volume dopo essere stati rimossi dallo spazio dei nomi in ONTAP"](#)

Quando si disinstalla e si disconnette un volume, i dati all'interno del volume non vengono persi. Inoltre, vengono mantenute le policy di esportazione dei volumi esistenti e le condivisioni SMB create sul volume o su directory e punti di giunzione all'interno del volume non montato. Se si rimonta il volume non montato, i client NAS possono accedere ai dati contenuti nel volume utilizzando le policy di esportazione e le condivisioni SMB esistenti.

### Fasi

1. Eseguire l'azione desiderata:

Se si desidera...	Immettere i comandi...
Montare un volume	<pre>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</pre>
Smontare un volume	<pre>volume unmount -vserver svm_name -volume volume_name  volume offline -vserver svm_name -volume volume_name</pre>

2. Verificare che il volume si trovi nello stato di montaggio desiderato:

```
volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active
```

### Esempi

Nell'esempio seguente viene montato un volume denominato "sques" situato su SVM "VS1" al punto di giunzione "/sales»":

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active
```

vserver	volume	state	junction-path	junction-active
vs1	data	online	/data	true
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

Il seguente esempio smonta e porta offline un volume chiamato "dati" situato su SVM "VS1":

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-active
```

vserver	volume	state	junction-path	junction-active
vs1	data	offline	-	-
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

## Visualizzare le informazioni sul punto di giunzione e sul montaggio del volume

È possibile visualizzare informazioni sui volumi montati per le macchine virtuali di storage (SVM) e sui punti di giunzione in cui vengono montati i volumi. È inoltre possibile determinare quali volumi non sono montati su un punto di giunzione. È possibile utilizzare queste informazioni per comprendere e gestire lo spazio dei nomi SVM.

### Fase

1. Eseguire l'azione desiderata:

Se si desidera visualizzare...	Immettere il comando...
Informazioni riepilogative sui volumi montati e non montati su SVM	<code>volume show -vserver vserver_name -junction</code>
Informazioni dettagliate sui volumi montati e non montati su SVM	<code>volume show -vserver vserver_name -volume volume_name -instance</code>

Informazioni specifiche sui volumi montati e non montati su SVM

- a. Se necessario, è possibile visualizzare campi validi per `-fields` utilizzando il seguente comando:  
`volume show -fields ?`
- b. Visualizzare le informazioni desiderate utilizzando `-fields` parametro:  
`volume show -vserver vs1 -fields fieldname,...`

## Esempi

Nell'esempio seguente viene visualizzato un riepilogo dei volumi montati e non montati su SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Junction Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	true	/sales	RW_volume

Nell'esempio seguente vengono visualizzate informazioni sui campi specificati per i volumi che si trovano su SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume    aggregate size state  type security-style junction-path
junction-parent node
-----
vs2      data1      aggr3      2GB  online RW    unix      -            -
node3
vs2      data2      aggr3      1GB  online RW    ntfs      /data2
vs2_root node3
vs2      data2_1    aggr3      8GB  online RW    ntfs      /data2/d2_1
data2    node3
vs2      data2_2    aggr3      8GB  online RW    ntfs      /data2/d2_2
data2    node3
vs2      pubs      aggr1      1GB  online RW    unix      /publications
vs2_root node1
vs2      images    aggr3      2TB  online RW    ntfs      /images
vs2_root node3
vs2      logs      aggr1      1GB  online RW    unix      /logs
vs2_root node1
vs2      vs2_root aggr3      1GB  online RW    ntfs      /            -
node3
```

## Configurare gli stili di sicurezza

### In che modo gli stili di sicurezza influiscono sull'accesso ai dati

#### Quali sono gli stili di sicurezza e i loro effetti

Esistono quattro diversi stili di sicurezza: UNIX, NTFS, misto e unificato. Ogni stile di sicurezza ha un effetto diverso sul modo in cui vengono gestite le autorizzazioni per i dati. È necessario comprendere i diversi effetti per assicurarsi di selezionare lo stile di sicurezza appropriato per i propri scopi.

È importante comprendere che gli stili di sicurezza non determinano quali tipi di client possono o non possono accedere ai dati. Gli stili di sicurezza determinano solo il tipo di autorizzazioni utilizzate da ONTAP per controllare l'accesso ai dati e il tipo di client in grado di modificare tali autorizzazioni.

Ad esempio, se un volume utilizza lo stile di sicurezza UNIX, i client SMB possono comunque accedere ai dati (purché autenticino e autorizzino correttamente) a causa della natura multiprotocollo di ONTAP. Tuttavia, ONTAP utilizza autorizzazioni UNIX che solo i client UNIX possono modificare utilizzando strumenti nativi.

Stile di sicurezza	Client in grado di modificare le autorizzazioni	Autorizzazioni che i client possono utilizzare	Risultato di uno stile di sicurezza efficace	Client che possono accedere ai file
UNIX	NFS	Bit di modalità NFSv3	UNIX	NFS e SMB
		ACL NFSv4.x		
NTFS	PMI	ACL NTFS	NTFS	
Misto	NFS o SMB	Bit di modalità NFSv3	UNIX	
		NFSv4.ACL		
		ACL NTFS	NTFS	
Unificato (solo per volumi infiniti, in ONTAP 9.4 e versioni precedenti).	NFS o SMB	Bit di modalità NFSv3	UNIX	
		ACL NFSv4.1		
		ACL NTFS	NTFS	

I volumi FlexVol supportano UNIX, NTFS e stili di sicurezza misti. Quando lo stile di sicurezza è misto o unificato, le autorizzazioni effettive dipendono dal tipo di client che ha modificato le autorizzazioni per ultima, perché gli utenti impostano lo stile di sicurezza su base individuale. Se l'ultimo client che ha modificato le autorizzazioni era un client NFSv3, le autorizzazioni sono bit di modalità UNIX NFSv3. Se l'ultimo client era un client NFSv4, le autorizzazioni sono ACL NFSv4. Se l'ultimo client era un client SMB, le autorizzazioni sono ACL NTFS di Windows.

Lo stile di sicurezza unificato è disponibile solo con volumi infiniti, che non sono più supportati in ONTAP 9.5 e versioni successive. Per ulteriori informazioni, vedere [Panoramica sulla gestione dei volumi FlexGroup](#).

A partire da ONTAP 9.2, la `show-effective-permissions al vserver security file-directory` il comando consente di visualizzare le autorizzazioni effettive concesse a un utente Windows o UNIX sul percorso di file o cartella specificato. Inoltre, il parametro opzionale `-share-name` consente di visualizzare l'autorizzazione di condivisione effettiva.



ONTAP imposta inizialmente alcune autorizzazioni predefinite per i file. Per impostazione predefinita, lo stile di sicurezza effettivo su tutti i dati nei volumi UNIX, misti e di sicurezza unificata è UNIX e il tipo di permessi effettivo è UNIX mode bits (0755 se non diversamente specificato) fino a quando non viene configurato da un client come consentito dallo stile di sicurezza predefinito. Per impostazione predefinita, lo stile di sicurezza effettivo su tutti i dati nei volumi di sicurezza NTFS è NTFS e dispone di un ACL che consente il controllo completo di tutti.

#### Dove e quando impostare gli stili di sicurezza

Gli stili di sicurezza possono essere impostati su volumi FlexVol (sia root che volumi di dati) e qtree. Gli stili di sicurezza possono essere impostati manualmente al momento della creazione, ereditati automaticamente o modificati in un secondo momento.

## Decidere quale stile di sicurezza utilizzare sulle SVM

Per aiutarti a decidere quale stile di sicurezza utilizzare su un volume, devi considerare due fattori. Il fattore principale è il tipo di amministratore che gestisce il file system. Il fattore secondario è il tipo di utente o servizio che accede ai dati sul volume.

Quando si configura lo stile di protezione su un volume, è necessario considerare le esigenze dell'ambiente per assicurarsi di selezionare lo stile di protezione migliore ed evitare problemi con la gestione delle autorizzazioni. Le seguenti considerazioni possono aiutarti a decidere:

Stile di sicurezza	Scegliere se...
UNIX	<ul style="list-style-type: none"><li>• Il file system è gestito da un amministratore UNIX.</li><li>• La maggior parte degli utenti sono client NFS.</li><li>• Un'applicazione che accede ai dati utilizza un utente UNIX come account del servizio.</li></ul>
NTFS	<ul style="list-style-type: none"><li>• Il file system è gestito da un amministratore di Windows.</li><li>• La maggior parte degli utenti è costituita da client SMB.</li><li>• Un'applicazione che accede ai dati utilizza un utente Windows come account del servizio.</li></ul>
Misto	<ul style="list-style-type: none"><li>• Il file system è gestito dagli amministratori UNIX e Windows e gli utenti sono costituiti da client NFS e SMB.</li></ul>

## Come funziona l'ereditarietà dello stile di sicurezza

Se non si specifica lo stile di protezione durante la creazione di un nuovo volume FlexVol o di un qtree, questo eredita il proprio stile di protezione in modi diversi.

Gli stili di sicurezza vengono ereditati nel modo seguente:

- Un volume FlexVol eredita lo stile di sicurezza del volume root del volume SVM contenente.
- Un qtree eredita lo stile di protezione del volume FlexVol contenente.
- Un file o una directory eredita lo stile di protezione del volume o qtree FlexVol contenente.

## In che modo ONTAP conserva le autorizzazioni UNIX

Quando i file in un volume FlexVol che dispongono attualmente di autorizzazioni UNIX vengono modificati e salvati dalle applicazioni Windows, ONTAP può conservare le autorizzazioni UNIX.

Quando le applicazioni sui client Windows modificano e salvano i file, leggono le proprietà di protezione del file, creano un nuovo file temporaneo, applicano tali proprietà al file temporaneo e assegnano al file temporaneo il nome del file originale.

Quando i client Windows eseguono una query per le proprietà di protezione, ricevono un ACL costruito che rappresenta esattamente le autorizzazioni UNIX. L'unico scopo di questo ACL costruito è quello di preservare le autorizzazioni UNIX del file, poiché i file vengono aggiornati dalle applicazioni Windows per garantire che i

file risultanti abbiano le stesse autorizzazioni UNIX. ONTAP non imposta alcun ACL NTFS utilizzando l'ACL costruito.

### **Gestire le autorizzazioni UNIX utilizzando la scheda protezione di Windows**

Se si desidera modificare le autorizzazioni UNIX di file o cartelle in volumi misti di sicurezza o qtree su SVM, è possibile utilizzare la scheda Security (protezione) sui client Windows. In alternativa, è possibile utilizzare applicazioni in grado di eseguire query e impostare gli ACL di Windows.

- Modifica delle autorizzazioni UNIX

È possibile utilizzare la scheda protezione di Windows per visualizzare e modificare le autorizzazioni UNIX per un volume misto di sicurezza o qtree. Se si utilizza la scheda principale di Windows Security per modificare le autorizzazioni UNIX, è necessario rimuovere prima l'ACE esistente che si desidera modificare (in questo modo i bit di modalità vengono impostati su 0) prima di apportare le modifiche. In alternativa, è possibile utilizzare l'editor avanzato per modificare le autorizzazioni.

Se vengono utilizzate le autorizzazioni di modalità, è possibile modificare direttamente le autorizzazioni di modalità per UID, GID e altri (tutti gli altri utenti con un account sul computer). Ad esempio, se l'UID visualizzato dispone delle autorizzazioni r-x, è possibile modificare le autorizzazioni UID in rwx.

- Modifica delle autorizzazioni UNIX in autorizzazioni NTFS

È possibile utilizzare la scheda protezione di Windows per sostituire gli oggetti di protezione UNIX con oggetti di protezione di Windows su un volume misto di tipo sicurezza o qtree in cui i file e le cartelle hanno uno stile di protezione efficace UNIX.

Prima di poter sostituire le voci di autorizzazione UNIX con gli oggetti utente e gruppo di Windows desiderati, è necessario rimuovere tutte le voci di autorizzazione UNIX elencate. È quindi possibile configurare gli ACL basati su NTFS sugli oggetti utente e Gruppo di Windows. Rimuovendo tutti gli oggetti di protezione UNIX e aggiungendo solo utenti e gruppi Windows a un file o a una cartella in un volume o qtree misto di sicurezza, è possibile modificare lo stile di protezione effettivo del file o della cartella da UNIX a NTFS.

Quando si modificano le autorizzazioni di una cartella, il comportamento predefinito di Windows consiste nel propagare queste modifiche a tutte le sottocartelle e a tutti i file. Pertanto, se non si desidera propagare una modifica dello stile di protezione a tutte le cartelle figlio, le sottocartelle e i file, è necessario modificare l'impostazione di propagazione desiderata.

### **Configurare gli stili di sicurezza sui volumi root SVM**

È possibile configurare lo stile di protezione del volume root SVM (Storage Virtual Machine) per determinare il tipo di autorizzazioni utilizzate per i dati sul volume root di SVM.

#### **Fasi**

1. Utilizzare `vserver create` con il `-rootvolume-security-style` parametro per definire lo stile di sicurezza.

Le opzioni possibili per lo stile di protezione del volume root sono: `unix`, `ntfs`, o `mixed`.



2. Visualizzare e verificare la configurazione, incluso lo stile di sicurezza del volume root della SVM creata:

```
vserver show -vserver vserver_name
```

### Configurare gli stili di sicurezza sui volumi FlexVol

È possibile configurare lo stile di sicurezza del volume FlexVol per determinare il tipo di autorizzazioni utilizzate per i dati sui volumi FlexVol della macchina virtuale di storage (SVM).

#### Fasi

1. Eseguire una delle seguenti operazioni:

Se il volume FlexVol...	Utilizzare il comando...
Non esiste ancora	<code>volume create</code> e includono <code>-security-style</code> parametro per specificare lo stile di sicurezza.
Esiste già	<code>volume modify</code> e includono <code>-security-style</code> parametro per specificare lo stile di sicurezza.

Le opzioni possibili per lo stile di protezione del volume FlexVol sono `unix`, `ntfs`, o `mixed`.

Se non si specifica uno stile di protezione durante la creazione di un volume FlexVol, il volume eredita lo stile di protezione del volume root.

Per ulteriori informazioni su `volume create` oppure `volume modify` comandi, vedere ["Gestione dello storage logico"](#).

2. Per visualizzare la configurazione, incluso lo stile di protezione del volume FlexVol creato, immettere il seguente comando:

```
volume show -volume volume_name -instance
```

### Configurare gli stili di sicurezza sui qtree

Lo stile di protezione del volume qtree viene configurato per determinare il tipo di autorizzazioni utilizzate per i dati su qtree.

#### Fasi

1. Eseguire una delle seguenti operazioni:

Se il qtree...	Utilizzare il comando...
Non esiste ancora	<code>volume qtree create</code> e includono <code>-security-style</code> parametro per specificare lo stile di sicurezza.
Esiste già	<code>volume qtree modify</code> e includono <code>-security-style</code> parametro per specificare lo stile di sicurezza.

Le opzioni possibili per lo stile di sicurezza qtree sono: `unix`, `ntfs`, o `mixed`.

Se non si specifica uno stile di protezione durante la creazione di un qtree, lo stile di protezione predefinito è `mixed`.

Per ulteriori informazioni su `volume qtree create` oppure `volume qtree modify` comandi, vedere ["Gestione dello storage logico"](#).

2. Per visualizzare la configurazione, incluso lo stile di sicurezza del qtree creato, immettere il seguente comando: `volume qtree show -qtree qtree_name -instance`

## Impostare l'accesso al file utilizzando NFS

### Impostare l'accesso al file utilizzando la panoramica NFS

È necessario completare una serie di passaggi per consentire ai client di accedere ai file sulle macchine virtuali di storage (SVM) utilizzando NFS. A seconda della configurazione corrente dell'ambiente, sono disponibili alcuni passaggi aggiuntivi opzionali.

Per consentire ai client di accedere ai file su SVM utilizzando NFS, è necessario completare le seguenti operazioni:

1. Abilitare il protocollo NFS su SVM.

È necessario configurare SVM per consentire l'accesso ai dati dai client tramite NFS.

2. Creare un server NFS su SVM.

Un server NFS è un'entità logica su SVM che consente a SVM di fornire file su NFS. È necessario creare il server NFS e specificare le versioni del protocollo NFS che si desidera consentire.

3. Configurare i criteri di esportazione su SVM.

È necessario configurare i criteri di esportazione per rendere disponibili volumi e qtree ai client.

4. Configurare il server NFS con la sicurezza appropriata e altre impostazioni a seconda della rete e dell'ambiente di storage.

Questo passaggio può includere la configurazione di Kerberos, LDAP, NIS, mappature dei nomi e utenti locali.

### Accesso sicuro a NFS tramite policy di esportazione

In che modo le policy di esportazione controllano l'accesso dei client ai volumi o ai qtree

I criteri di esportazione contengono una o più *regole di esportazione* che elaborano ogni richiesta di accesso client. Il risultato del processo determina se al client viene negato o concesso l'accesso e quale livello di accesso. Affinché i client possano accedere ai dati, è necessario che sulla macchina virtuale di storage (SVM) sia presente un criterio di esportazione con regole di esportazione.

Per configurare l'accesso del client al volume o al qtree, è necessario associare esattamente un criterio di

esportazione a ciascun volume o qtree. La SVM può contenere più policy di esportazione. Ciò consente di eseguire le seguenti operazioni per le SVM con più volumi o qtree:

- Assegnare criteri di esportazione diversi a ciascun volume o qtree di SVM per il controllo degli accessi dei singoli client a ciascun volume o qtree di SVM.
- Assegnare la stessa policy di esportazione a più volumi o qtree di SVM per un controllo identico dell'accesso client senza dover creare una nuova policy di esportazione per ciascun volume o qtree.

Se un client effettua una richiesta di accesso non consentita dalla policy di esportazione applicabile, la richiesta non riesce e viene visualizzato un messaggio di autorizzazione negata. Se un client non corrisponde a nessuna regola nella policy di esportazione, l'accesso viene negato. Se un criterio di esportazione è vuoto, tutti gli accessi vengono implicitamente negati.

È possibile modificare dinamicamente un criterio di esportazione su un sistema che esegue ONTAP.

### **Policy di esportazione predefinita per le SVM**

Ogni SVM dispone di un criterio di esportazione predefinito che non contiene regole. Prima che i client possano accedere ai dati su SVM, deve esistere un criterio di esportazione con regole. Ogni volume FlexVol contenuto nella SVM deve essere associato a una policy di esportazione.

Quando si crea una SVM, il sistema storage crea automaticamente una policy di esportazione predefinita chiamata `default` Per il volume root di SVM. È necessario creare una o più regole per il criterio di esportazione predefinito prima che i client possano accedere ai dati sulla SVM. In alternativa, è possibile creare una policy di esportazione personalizzata con regole. È possibile modificare e rinominare il criterio di esportazione predefinito, ma non è possibile eliminare il criterio di esportazione predefinito.

Quando si crea un volume FlexVol nella sua SVM contenente, il sistema di storage crea il volume e lo associa alla policy di esportazione predefinita per il volume root della SVM. Per impostazione predefinita, ogni volume creato in SVM è associato al criterio di esportazione predefinito per il volume root. È possibile utilizzare il criterio di esportazione predefinito per tutti i volumi contenuti in SVM oppure creare un criterio di esportazione univoco per ciascun volume. È possibile associare più volumi alla stessa policy di esportazione.

### **Come funzionano le regole di esportazione**

Le regole di esportazione sono gli elementi funzionali di una policy di esportazione. Le regole di esportazione consentono di associare le richieste di accesso client a un volume a parametri specifici configurati per determinare come gestire le richieste di accesso client.

Un criterio di esportazione deve contenere almeno una regola di esportazione per consentire l'accesso ai client. Se un criterio di esportazione contiene più di una regola, le regole vengono elaborate nell'ordine in cui appaiono nel criterio di esportazione. L'ordine delle regole è determinato dal numero di indice delle regole. Se una regola corrisponde a un client, vengono utilizzate le autorizzazioni di tale regola e non vengono elaborate ulteriori regole. Se nessuna regola corrisponde, al client viene negato l'accesso.

È possibile configurare le regole di esportazione per determinare le autorizzazioni di accesso del client utilizzando i seguenti criteri:

- Il protocollo di accesso al file utilizzato dal client che invia la richiesta, ad esempio NFSv4 o SMB.
- Identificatore del client, ad esempio nome host o indirizzo IP.

La dimensione massima di `-clientmatch` il campo è composto da 4096 caratteri.

- Il tipo di protezione utilizzato dal client per autenticare, ad esempio Kerberos v5, NTLM o AUTH\_SYS.

Se una regola specifica più criteri, il client deve corrispondere a tutti i criteri affinché la regola venga applicata.



A partire da ONTAP 9.3, è possibile attivare il controllo della configurazione dei criteri di esportazione come processo in background che registra eventuali violazioni delle regole in un elenco di regole di errore. Il `vserver export-policy config-checker` i comandi richiamano il controllo e visualizzano i risultati, che è possibile utilizzare per verificare la configurazione ed eliminare le regole errate dal criterio.

I comandi convalidano solo la configurazione di esportazione per i nomi host, i netgroup e gli utenti anonimi.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La richiesta di accesso client viene inviata utilizzando il protocollo NFSv3 e il client ha l'indirizzo IP 10.1.17.37.

Anche se il protocollo di accesso client corrisponde, l'indirizzo IP del client si trova in una subnet diversa da quella specificata nella regola di esportazione. Pertanto, la corrispondenza dei client non riesce e questa regola non si applica a questo client.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La richiesta di accesso client viene inviata utilizzando il protocollo NFSv4 e il client ha l'indirizzo IP 10.1.16.54.

Il protocollo di accesso client corrisponde e l'indirizzo IP del client si trova nella subnet specificata. Pertanto, la corrispondenza dei client viene eseguita correttamente e questa regola si applica a questo client. Il client ottiene l'accesso in lettura/scrittura indipendentemente dal tipo di protezione.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`

- -rorule any
- -rwrule krb5,ntlm

Il client n. 1 ha l'indirizzo IP 10.1.16.207, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH\_SYS.

Il protocollo di accesso client e l'indirizzo IP corrispondono per entrambi i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione con cui sono stati autenticati. Pertanto, entrambi i client ottengono l'accesso in sola lettura. Tuttavia, solo il client n. 1 ottiene l'accesso in lettura/scrittura perché per l'autenticazione è stato utilizzato il tipo di protezione approvato Kerberos v5. Il client n. 2 non ottiene l'accesso in lettura/scrittura.

#### Gestire i client con un tipo di protezione non elencato

Quando un client si presenta con un tipo di protezione non elencato in un parametro di accesso di una regola di esportazione, è possibile scegliere di negare l'accesso al client o di associarlo all'ID utente anonimo utilizzando invece l'opzione `none` nel parametro `access`.

Un client potrebbe presentarsi con un tipo di protezione non elencato in un parametro di accesso perché autenticato con un tipo di protezione diverso o non autenticato affatto (tipo di protezione AUTH\_NONE). Per impostazione predefinita, al client viene automaticamente negato l'accesso a tale livello. Tuttavia, è possibile aggiungere l'opzione `none` al parametro di accesso. Di conseguenza, i client con uno stile di sicurezza non elencato vengono mappati all'ID utente anonimo. Il `-anon` il parametro determina l'ID utente assegnato a tali client. L'ID utente specificato per `-anon` il parametro deve essere un utente valido configurato con le autorizzazioni che si ritiene appropriate per l'utente anonimo.

Valori validi per `-anon` intervallo di parametri da 0 a. 65535.

ID utente assegnato a. <code>-anon</code>	Gestione risultante delle richieste di accesso del client
0 - 65533	La richiesta di accesso client viene mappata all'ID utente anonimo e ottiene l'accesso in base alle autorizzazioni configurate per l'utente.
65534	La richiesta di accesso client viene mappata all'utente nessuno e ottiene l'accesso in base alle autorizzazioni configurate per l'utente. Questa è l'impostazione predefinita.
65535	La richiesta di accesso da qualsiasi client viene negata quando viene mappata a questo ID e il client si presenta con il tipo di sicurezza AUTH_NONE. La richiesta di accesso dai client con ID utente 0 viene negata quando viene mappata a questo ID e il client si presenta con qualsiasi altro tipo di sicurezza.

Quando si utilizza l'opzione `none`, è importante ricordare che il parametro di sola lettura viene elaborato per primo. Per configurare le regole di esportazione per i client con tipi di protezione non elencati, prendere in considerazione le seguenti linee guida:

Include la funzione di sola lettura <code>none</code>	La lettura/scrittura include <code>none</code>	Accesso risultante per i client con tipi di sicurezza non elencati
No	No	Negato
No	Sì	Negato perché viene elaborata per prima la sola lettura
Sì	No	Sola lettura come anonimo
Sì	Sì	Lettura/scrittura anonima

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

Il client n. 1 ha l'indirizzo IP 10.1.16.207, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH\_SYS.

Il client n. 3 ha l'indirizzo IP 10.1.16.234, invia una richiesta di accesso utilizzando il protocollo NFSv3 e non ha eseguito l'autenticazione (ovvero il tipo di protezione AUTH\_NONE).

Il protocollo di accesso client e l'indirizzo IP corrispondono per tutti e tre i client. Il parametro di sola lettura consente l'accesso in sola lettura ai client con il proprio ID utente autenticato con AUTH\_SYS. Il parametro di sola lettura consente l'accesso in sola lettura come utente anonimo con ID utente 70 ai client autenticati utilizzando qualsiasi altro tipo di protezione. Il parametro Read-write consente l'accesso in lettura/scrittura a qualsiasi tipo di protezione, ma in questo caso si applica solo ai client già filtrati dalla regola di sola lettura.

Pertanto, i client 1 e 3 ottengono l'accesso in lettura/scrittura solo come utente anonimo con ID utente 70. Il client n. 2 ottiene l'accesso in lettura/scrittura con il proprio ID utente.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`

- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

Il client n. 1 ha l'indirizzo IP 10.1.16.207, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH\_SYS.

Il client n. 3 ha l'indirizzo IP 10.1.16.234, invia una richiesta di accesso utilizzando il protocollo NFSv3 e non ha eseguito l'autenticazione (ovvero il tipo di protezione AUTH\_NONE).

Il protocollo di accesso client e l'indirizzo IP corrispondono per tutti e tre i client. Il parametro di sola lettura consente l'accesso in sola lettura ai client con il proprio ID utente autenticato con AUTH\_SYS. Il parametro di sola lettura consente l'accesso in sola lettura come utente anonimo con ID utente 70 ai client autenticati utilizzando qualsiasi altro tipo di protezione. Il parametro Read-write consente l'accesso in lettura/scrittura solo come utente anonimo.

Pertanto, il client n. 1 e il client n. 3 ottengono l'accesso in lettura/scrittura solo come utente anonimo con ID utente 70. Il client n. 2 ottiene l'accesso in sola lettura con il proprio ID utente, ma viene negato l'accesso in lettura/scrittura.

#### In che modo i tipi di sicurezza determinano i livelli di accesso del client

Il tipo di protezione autenticato dal client gioca un ruolo speciale nelle regole di esportazione. È necessario comprendere in che modo il tipo di protezione determina i livelli di accesso che il client ottiene a un volume o qtree.

I tre livelli di accesso possibili sono i seguenti:

1. Sola lettura
2. Lettura/scrittura
3. Superuser (per client con ID utente 0)

Poiché il livello di accesso in base al tipo di protezione viene valutato in questo ordine, è necessario osservare le seguenti regole quando si costruiscono i parametri del livello di accesso nelle regole di esportazione:

Per ottenere un livello di accesso da parte di un client...	Questi parametri di accesso devono corrispondere al tipo di sicurezza del client...
Utente normale di sola lettura	Sola lettura ( <code>-rorule</code> )
Lettura/scrittura utente normale	Sola lettura ( <code>-rorule</code> ) e read-write ( <code>-rwrule</code> )
Superuser di sola lettura	Sola lettura ( <code>-rorule</code> ) e <code>-superuser</code>
Lettura/scrittura superutente	Sola lettura ( <code>-rorule</code> ) e read-write ( <code>-rwrule</code> ) e <code>-superuser</code>

Di seguito sono riportati i tipi di protezione validi per ciascuno di questi tre parametri di accesso:

- `any`
- `none`
- `never`

Questo tipo di protezione non è valido per l'utilizzo con `-superuser` parametro.

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

Quando si abbina un tipo di sicurezza di un client a ciascuno dei tre parametri di accesso, si possono ottenere tre risultati:

Se il tipo di protezione del client...	Quindi il client...
Corrisponde a quello specificato nel parametro di accesso.	Ottiene l'accesso per quel livello con il proprio ID utente.
Non corrisponde a quello specificato, ma il parametro di accesso include l'opzione <code>none</code> .	Ottiene l'accesso per quel livello, ma come utente anonimo con l'ID utente specificato da <code>-anon</code> parametro.
Non corrisponde a quello specificato e il parametro di accesso non include l'opzione <code>none</code> .	Non ottiene alcun accesso per quel livello. questo non si applica a. <code>-superuser</code> parametro perché include sempre <code>none</code> anche se non specificato.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule sys, krb5`
- `-superuser krb5`

Il client n. 1 ha l'indirizzo IP 10.1.16.207, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH\_SYS.

Il client n. 3 ha l'indirizzo IP 10.1.16.234, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo



NFSv3 e non ha eseguito l'autenticazione (AUTH\_NONE).

Il protocollo di accesso client e l'indirizzo IP corrispondono a tutti e tre i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione. Il parametro Read-write consente l'accesso in lettura/scrittura ai client con il proprio ID utente autenticato con AUTH\_SYS o Kerberos v5. Il parametro superuser consente l'accesso del superutente ai client con ID utente 0 autenticati con Kerberos v5.

Pertanto, il client n. 1 ottiene l'accesso di lettura/scrittura superutente perché corrisponde a tutti e tre i parametri di accesso. Il client n. 2 ottiene l'accesso in lettura/scrittura ma non l'accesso al superutente. Il client n. 3 ottiene l'accesso in sola lettura, ma non l'accesso al superutente.

#### Gestire le richieste di accesso dei superutenti

Quando si configurano i criteri di esportazione, è necessario considerare ciò che si desidera che accada se il sistema storage riceve una richiesta di accesso client con ID utente 0, vale a dire come superutente, e impostare le regole di esportazione di conseguenza.

Nel mondo UNIX, un utente con ID utente 0 è noto come superutente, in genere chiamato root, che ha diritti di accesso illimitati su un sistema. L'utilizzo dei privilegi dei superutenti può essere pericoloso per diversi motivi, tra cui la violazione della sicurezza del sistema e dei dati.

Per impostazione predefinita, ONTAP esegue il mapping dei client che presentano l'ID utente 0 all'utente anonimo. Tuttavia, è possibile specificare `-superuser` Parametro nelle regole di esportazione per determinare come gestire i client che presentano ID utente 0 a seconda del tipo di protezione. Di seguito sono riportate le opzioni valide per `-superuser` parametro:

- any
- none

Questa è l'impostazione predefinita se non si specifica `-superuser` parametro.

- krb5
- ntlm
- sys

Esistono due modi diversi per gestire i client che presentano un ID utente 0, a seconda di `-superuser` configurazione dei parametri:

Se il <code>-superuser</code> parametro e tipo di sicurezza del client...	Quindi il client...
Corrispondenza	Ottiene l'accesso al superutente con ID utente 0.
Non corrispondono	Ottiene l'accesso come utente anonimo con l'ID utente specificato da <code>-anon</code> e le relative autorizzazioni assegnate. Ciò indipendentemente dal fatto che il parametro di sola lettura o di lettura/scrittura specifichi l'opzione <code>none</code> .

Se un client presenta l'ID utente 0 per accedere a un volume con lo stile di protezione NTFS e a. `-superuser` il parametro è impostato su `none`, ONTAP utilizza la mappatura dei nomi per l'utente anonimo per ottenere le credenziali corrette.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

Il client n. 1 ha l'indirizzo IP 10.1.16.207, ha l'ID utente 746, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH\_SYS.

Il protocollo di accesso client e l'indirizzo IP corrispondono per entrambi i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione con cui sono stati autenticati. Tuttavia, solo il client n. 1 ottiene l'accesso in lettura/scrittura perché per l'autenticazione è stato utilizzato il tipo di protezione approvato Kerberos v5.

Il client n. 2 non ottiene l'accesso superutente. Invece, viene mappato ad anonimo perché `-superuser` parametro non specificato. Ciò significa che il valore predefinito è `none` E mappa automaticamente l'ID utente 0 in anonimo. Il client n. 2 ottiene anche solo l'accesso in sola lettura perché il tipo di protezione non corrisponde al parametro di lettura/scrittura.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

Il client n. 1 ha l'indirizzo IP 10.1.16.207, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, ha l'ID utente 0, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH\_SYS.

Il protocollo di accesso client e l'indirizzo IP corrispondono per entrambi i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione con cui sono stati autenticati. Tuttavia, solo il client n. 1 ottiene l'accesso in lettura/scrittura perché per l'autenticazione è stato

utilizzato il tipo di protezione approvato Kerberos v5. Il client n. 2 non ottiene l'accesso in lettura/scrittura.

La regola di esportazione consente l'accesso al superutente per i client con ID utente 0. Il client n. 1 ottiene l'accesso al superutente perché corrisponde all'ID utente e al tipo di sicurezza per la modalità di sola lettura e. -superuser parametri. Il client n. 2 non ottiene l'accesso in lettura/scrittura o superutente perché il suo tipo di protezione non corrisponde al parametro di lettura/scrittura o a. -superuser parametro. Invece, il client n. 2 viene mappato all'utente anonimo, che in questo caso ha l'ID utente 0.

#### Modalità di utilizzo delle cache delle policy di esportazione da parte di ONTAP

Per migliorare le performance del sistema, ONTAP utilizza cache locali per memorizzare informazioni come nomi host e netgroup. Ciò consente a ONTAP di elaborare le regole delle policy di esportazione più rapidamente rispetto al recupero delle informazioni da fonti esterne. La comprensione delle cache e delle relative funzioni può aiutare a risolvere i problemi di accesso dei client.

I criteri di esportazione vengono configurati per controllare l'accesso dei client alle esportazioni NFS. Ogni policy di esportazione contiene regole e ogni regola contiene parametri che consentono di associare la regola ai client che richiedono l'accesso. Alcuni di questi parametri richiedono che ONTAP contatti un'origine esterna, ad esempio server DNS o NIS, per risolvere oggetti come nomi di dominio, nomi host o netgroup.

Queste comunicazioni con le fonti esterne richiedono una piccola quantità di tempo. Per aumentare le performance, ONTAP riduce il tempo necessario per risolvere gli oggetti delle regole dei criteri di esportazione memorizzando le informazioni in locale su ciascun nodo in diverse cache.

Nome della cache	Tipo di informazioni memorizzate
Accesso	Mappature dei client ai criteri di esportazione corrispondenti
Nome	Mapping dei nomi utente UNIX agli ID utente UNIX corrispondenti
ID	Mapping degli ID utente UNIX agli ID utente UNIX corrispondenti e agli ID gruppo UNIX estesi
Host	Mapping dei nomi host agli indirizzi IP corrispondenti
Netgroup	Mapping dei netgroup agli indirizzi IP corrispondenti dei membri
Showmount	Elenco delle directory esportate dallo spazio dei nomi SVM

Se si modificano le informazioni sui server dei nomi esterni dell'ambiente dopo il recupero e l'archiviazione in locale da parte di ONTAP, le cache potrebbero ora contenere informazioni obsolete. Sebbene ONTAP aggiorni automaticamente le cache dopo determinati periodi di tempo, diverse cache hanno tempi di scadenza e refresh e algoritmi diversi.

Un'altra possibile ragione per cui le cache contengono informazioni obsolete è quando ONTAP tenta di aggiornare le informazioni memorizzate nella cache ma incontra un errore quando tenta di comunicare con i

server dei nomi. In questo caso, ONTAP continua a utilizzare le informazioni attualmente memorizzate nelle cache locali per evitare interruzioni del client.

Di conseguenza, le richieste di accesso client che dovrebbero avere esito positivo potrebbero non riuscire e le richieste di accesso client che dovrebbero fallire potrebbero avere esito positivo. È possibile visualizzare e svuotare manualmente alcune cache delle policy di esportazione durante la risoluzione di tali problemi di accesso client.

#### **Come funziona la cache di accesso**

ONTAP utilizza una cache di accesso per memorizzare i risultati della valutazione delle regole dei criteri di esportazione per le operazioni di accesso client su un volume o qtree. Ciò comporta miglioramenti delle performance in quanto le informazioni possono essere recuperate molto più velocemente dalla cache di accesso rispetto al processo di valutazione delle regole dei criteri di esportazione ogni volta che un client invia una richiesta di i/O.

Ogni volta che un client NFS invia una richiesta di i/o per accedere ai dati su un volume o qtree, ONTAP deve valutare ogni richiesta di i/o per determinare se concedere o negare la richiesta di i/O. Questa valutazione implica il controllo di ogni regola dei criteri di esportazione dei criteri associati al volume o al qtree. Se il percorso al volume o al qtree comporta l'attraversamento di uno o più punti di giunzione, potrebbe essere necessario eseguire questa verifica per più policy di esportazione lungo il percorso.

Si noti che questa valutazione si verifica per ogni richiesta di i/o inviata da un client NFS, come lettura, scrittura, elenco, copia e altre operazioni, non solo per le richieste di montaggio iniziali.

Dopo che ONTAP ha identificato le regole dei criteri di esportazione applicabili e ha deciso se consentire o negare la richiesta, ONTAP crea una voce nella cache di accesso per memorizzare queste informazioni.

Quando un client NFS invia una richiesta di i/o, ONTAP prende nota dell'indirizzo IP del client, dell'ID della SVM e della policy di esportazione associata al volume di destinazione o al qtree, quindi verifica prima la presenza di una voce corrispondente nella cache di accesso. Se nella cache di accesso esiste una voce corrispondente, ONTAP utilizza le informazioni memorizzate per consentire o negare la richiesta di i/O. Se non esiste una voce corrispondente, ONTAP passa attraverso il normale processo di valutazione di tutte le regole di policy applicabili, come spiegato in precedenza.

Le voci della cache di accesso non utilizzate attivamente non vengono aggiornate. In questo modo si riducono le comunicazioni inutili e dispendiose con i name server esterni.

Il recupero delle informazioni dalla cache di accesso è molto più rapido rispetto all'intero processo di valutazione delle regole dei criteri di esportazione per ogni richiesta di i/O. Pertanto, l'utilizzo della cache di accesso migliora notevolmente le performance riducendo l'overhead dei controlli di accesso del client.

#### **Come funzionano i parametri della cache di accesso**

Diversi parametri controllano i periodi di refresh per le voci nella cache di accesso. La comprensione del funzionamento di questi parametri consente di modificarli per ottimizzare la cache di accesso e bilanciare le performance con la frequenza delle informazioni memorizzate.

La cache di accesso memorizza le voci costituite da una o più regole di esportazione applicabili ai client che tentano di accedere a volumi o qtree. Queste voci vengono memorizzate per un certo periodo di tempo prima dell'aggiornamento. Il tempo di refresh è determinato dai parametri della cache di accesso e dipende dal tipo di

voce della cache di accesso.

È possibile specificare i parametri della cache di accesso per le singole SVM. In questo modo, i parametri possono variare in base ai requisiti di accesso SVM. Le voci della cache di accesso che non vengono utilizzate attivamente non vengono aggiornate, il che riduce le comunicazioni inutili e dispendiose con i server di nomi esterni.

Tipo di voce della cache di accesso	Descrizione	Periodo di refresh in secondi
Voci positive	Voci della cache di accesso che non hanno portato ad un DOS (Access Denial) per i client.	Minimo: 300 Massimo: 86,400 Predefinito: 3,600
Voci negative	Voci della cache di accesso che hanno portato ad un DOS (Access Denial) per i client.	Minimo: 60 Massimo: 86,400 Predefinito: 3,600

### Esempio

Un client NFS tenta di accedere a un volume su un cluster. ONTAP associa il client a una regola dei criteri di esportazione e determina che il client ottiene l'accesso in base alla configurazione della regola dei criteri di esportazione. ONTAP memorizza la regola dei criteri di esportazione nella cache di accesso come voce positiva. Per impostazione predefinita, ONTAP mantiene la voce positiva nella cache di accesso per un'ora (3,600 secondi), quindi aggiorna automaticamente la voce per mantenere aggiornate le informazioni.

Per evitare che la cache di accesso si riempia inutilmente, è disponibile un parametro aggiuntivo per cancellare le voci della cache di accesso esistenti che non sono state utilizzate per un certo periodo di tempo per decidere l'accesso del client. Questo `-harvest-timeout` il parametro ha un intervallo consentito compreso tra 60 e 2,592,000 secondi e un'impostazione predefinita di 86,400 secondi.

### Rimuovere un criterio di esportazione da un qtree

Se si decide di non assegnare più un criterio di esportazione specifico a un qtree, è possibile rimuovere il criterio di esportazione modificando il qtree in modo da ereditare il criterio di esportazione del volume contenente. Per eseguire questa operazione, utilizzare `volume qtree modify` con il `-export-policy` e una stringa di nome vuota ("").

### Fasi

1. Per rimuovere un criterio di esportazione da un qtree, immettere il seguente comando:

```
volume qtree modify -vserver vserver_name -qtree-path  
/vol/volume_name/qtree_name -export-policy ""
```

2. Verificare che il qtree sia stato modificato di conseguenza:

```
volume qtree show -qtree qtree_name -fields export-policy
```

## Convalidare gli ID qtree per le operazioni del file qtree

ONTAP può eseguire un'ulteriore convalida facoltativa degli ID qtree. Questa convalida garantisce che le richieste di operazione del file client utilizzino un ID qtree valido e che i client possano spostare solo i file all'interno dello stesso qtree. È possibile attivare o disattivare questa convalida modificando il `-validate-qtrees-export` parametro. Questo parametro è attivato per impostazione predefinita.

### A proposito di questa attività

Questo parametro è valido solo se è stata assegnata una policy di esportazione direttamente a uno o più qtree sulla macchina virtuale di storage (SVM).

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera che la convalida dell'ID qtree sia...	Immettere il seguente comando...
Attivato	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export enabled</pre>
Disattivato	<pre>vserver nfs modify -vserver vserver_name -validate-qtrees-export disabled</pre>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Restrizioni dei criteri di esportazione e giunzioni nidificate per i volumi FlexVol

Se sono stati configurati criteri di esportazione per impostare un criterio meno restrittivo su una giunzione nidificata ma un criterio più restrittivo su una giunzione di livello superiore, l'accesso alla giunzione di livello inferiore potrebbe non riuscire.

È necessario garantire che le giunzioni di livello superiore abbiano policy di esportazione meno restrittive rispetto alle giunzioni di livello inferiore.

## Utilizzo di Kerberos con NFS per una maggiore sicurezza

### Supporto ONTAP per Kerberos

Kerberos offre un'autenticazione sicura e sicura per le applicazioni client/server. L'autenticazione consente di verificare le identità di utenti e processi di un server. Nell'ambiente ONTAP, Kerberos fornisce l'autenticazione tra le macchine virtuali di

## storage (SVM) e i client NFS.

In ONTAP 9, sono supportate le seguenti funzionalità Kerberos:

- Autenticazione Kerberos 5 con controllo dell'integrità (krb5i)

Krb5i utilizza checksum per verificare l'integrità di ogni messaggio NFS trasferito tra client e server. Ciò è utile sia per motivi di sicurezza (ad esempio, per garantire che i dati non siano stati manomessi) che per motivi di integrità dei dati (ad esempio, per prevenire la corruzione dei dati quando si utilizza NFS su reti non affidabili).

- Autenticazione Kerberos 5 con controllo della privacy (krb5p)

Krb5p utilizza checksum per crittografare tutto il traffico tra il client e il server. Questo è più sicuro e comporta un carico maggiore.

- Crittografia AES a 128 e 256 bit

Advanced Encryption Standard (AES) è un algoritmo di crittografia per la protezione dei dati elettronici. ONTAP supporta AES con chiavi a 128 bit (AES-128) e AES con chiavi a 256 bit (AES-256) per Kerberos per una maggiore protezione.

- Configurazioni di area di autenticazione Kerberos a livello di SVM

Gli amministratori di SVM possono ora creare configurazioni di area di autenticazione Kerberos a livello di SVM. Ciò significa che gli amministratori di SVM non devono più affidarsi all'amministratore del cluster per la configurazione dell'area di autenticazione Kerberos e possono creare singole configurazioni dell'area di autenticazione Kerberos in un ambiente multi-tenancy.

### Requisiti per la configurazione di Kerberos con NFS

Prima di configurare Kerberos con NFS sul sistema, è necessario verificare che alcuni elementi dell'ambiente di rete e di storage siano configurati correttamente.



La procedura per configurare l'ambiente dipende dalla versione e dal tipo di sistema operativo client, controller di dominio, Kerberos, DNS e così via. che stai utilizzando. La documentazione di tutte queste variabili non rientra nell'ambito di questo documento. Per ulteriori informazioni, consultare la documentazione relativa a ciascun componente.

Per un esempio dettagliato di come configurare ONTAP e Kerberos 5 con NFSv3 e NFSv4 in un ambiente che utilizza Active Directory di Windows Server 2008 R2 e host Linux, consultare il report tecnico 4073.

È necessario configurare prima i seguenti elementi:

### Requisiti dell'ambiente di rete

- Kerberos

È necessario disporre di una configurazione Kerberos funzionante con un centro di distribuzione delle chiavi (KDC), ad esempio Kerberos basato su Windows Active Directory o MIT Kerberos.

I server NFS devono utilizzare `nfs` come componente principale del computer.

- Servizio di directory

È necessario utilizzare un servizio directory sicuro nell'ambiente, ad esempio Active Directory o OpenLDAP, configurato per l'utilizzo di LDAP su SSL/TLS.

- NTP

È necessario disporre di un server dell'orario di lavoro che esegue NTP. Ciò è necessario per evitare errori di autenticazione Kerberos dovuti a un disallineamento temporale.

- DNS (Domain Name Resolution)

Ciascun client UNIX e ciascun LIF SVM devono disporre di un record di servizio (SRV) appropriato registrato con il KDC nelle zone di ricerca in avanti e indietro. Tutti i partecipanti devono essere risolvibili correttamente tramite DNS.

- Account utente

Ogni client deve disporre di un account utente nell'area Kerberos. I server NFS devono utilizzare "nfs" come componente principale del computer.

## Requisiti del client NFS

- NFS

Ciascun client deve essere configurato correttamente per comunicare in rete utilizzando NFSv3 o NFSv4.

I client devono supportare RFC1964 e RFC2203.

- Kerberos

Ciascun client deve essere configurato correttamente per utilizzare l'autenticazione Kerberos, inclusi i seguenti dettagli:

- La crittografia per la comunicazione TGS è attivata.

AES-256 per la massima sicurezza.

- Il tipo di crittografia più sicuro per la comunicazione TGT è attivato.
- Il dominio e l'area di autenticazione Kerberos sono configurati correttamente.
- Il GSS è attivato.

Quando si utilizzano le credenziali del computer:

- Non eseguire `gssd` con `-n` parametro.
- Non eseguire `kinit` come utente root.

- Ogni client deve utilizzare la versione più recente e aggiornata del sistema operativo.

In questo modo si ottiene la migliore compatibilità e affidabilità per la crittografia AES con Kerberos.

- DNS

Ciascun client deve essere configurato correttamente per utilizzare il DNS per la corretta risoluzione dei



nomi.

- NTP

Ciascun client deve essere sincronizzato con il server NTP.

- Informazioni su host e dominio

Di ogni client `/etc/hosts` e `/etc/resolv.conf` i file devono contenere rispettivamente il nome host e le informazioni DNS corretti.

- File keytab

Ogni client deve avere un file keytab dal KDC. L'area di autenticazione deve essere in lettere maiuscole. Il tipo di crittografia deve essere AES-256 per garantire la massima sicurezza.

- Opzionale: Per ottenere le migliori performance, i client traggono vantaggio dalla presenza di almeno due interfacce di rete: Una per la comunicazione con la rete locale e una per la comunicazione con la rete di storage.

## Requisiti di sistema per lo storage

- Licenza NFS

Il sistema storage deve avere una licenza NFS valida installata.

- Licenza CIFS

La licenza CIFS è opzionale. È necessario solo per il controllo delle credenziali Windows quando si utilizza la mappatura dei nomi multiprotocollo. Non è richiesto in un ambiente UNIX-only rigoroso.

- SVM

È necessario configurare almeno una SVM sul sistema.

- DNS su SVM

È necessario aver configurato il DNS su ogni SVM.

- Server NFS

È necessario aver configurato NFS su SVM.

- Crittografia AES

Per una maggiore sicurezza, è necessario configurare il server NFS in modo che consenta solo la crittografia AES-256 per Kerberos.

- Server SMB

Se si utilizza un ambiente multiprotocollo, è necessario aver configurato SMB su SVM. Il server SMB è necessario per la mappatura dei nomi multiprotocollo.

- Volumi

È necessario disporre di un volume root e di almeno un volume di dati configurati per l'utilizzo da parte di

SVM.

- Volume root

Il volume root di SVM deve avere la seguente configurazione:

Nome	Impostazione
Stile di sicurezza	UNIX
UID	Root o ID 0
GID	Root o ID 0
Autorizzazioni UNIX	777

A differenza del volume root, i volumi di dati possono avere uno stile di sicurezza.

- Gruppi UNIX

La SVM deve avere i seguenti gruppi UNIX configurati:

Nome del gruppo	ID gruppo
daemon	1
root	0
pcuser	65534 (creato automaticamente da ONTAP quando si crea la SVM)

- Utenti UNIX

La SVM deve avere i seguenti utenti UNIX configurati:

Nome utente	ID utente	ID gruppo primario	Commento
nfs	500	0	Necessario per la fase DI INIT GSS  Il primo componente dell'SPN dell'utente client NFS viene utilizzato come utente.

Nome utente	ID utente	ID gruppo primario	Commento
pcuser	65534	65534	Necessario per l'utilizzo multiprotocollo NFS e CIFS  Creato e aggiunto automaticamente al gruppo pcuser da ONTAP quando si crea la SVM.
root	0	0	Necessario per il montaggio

L'utente nfs non è richiesto se esiste una mappatura dei nomi Kerberos-UNIX per l'SPN dell'utente client NFS.

- Policy e regole di esportazione

È necessario aver configurato i criteri di esportazione con le regole di esportazione necessarie per i volumi root e dati e qtree. Se si accede a tutti i volumi della SVM tramite Kerberos, è possibile impostare le opzioni della regola di esportazione `-rorule`, `-rwrule`, e `-superuser` per il volume root a `krb5`, `krb5i`, o `krb5p`.

- Mappatura dei nomi Kerberos-UNIX

Se si desidera che l'utente identificato dall'utente client NFS SPN disponga delle autorizzazioni root, è necessario creare una mappatura dei nomi nella directory root.

## Informazioni correlate

["Report tecnico di NetApp 4073: Autenticazione unificata sicura"](#)

["Tool di matrice di interoperabilità NetApp"](#)

["Amministrazione del sistema"](#)

["Gestione dello storage logico"](#)

## Specificare il dominio ID utente per NFSv4

Per specificare il dominio ID utente, è possibile impostare `-v4-id-domain` opzione.

## A proposito di questa attività

Per impostazione predefinita, ONTAP utilizza il dominio NIS per il mapping dell'ID utente NFSv4, se impostato. Se non viene impostato un dominio NIS, viene utilizzato il dominio DNS. Potrebbe essere necessario impostare il dominio ID utente se, ad esempio, si dispone di più domini ID utente. Il nome di dominio deve corrispondere alla configurazione del dominio sul controller di dominio. Non è richiesto per NFSv3.

## Fase

1. Immettere il seguente comando:

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

## Configurare i name service

### Funzionamento della configurazione dello switch ONTAP name service

ONTAP memorizza le informazioni di configurazione del name service in una tabella equivalente a `/etc/nsswitch.conf` File su sistemi UNIX. È necessario comprendere la funzione della tabella e il modo in cui ONTAP la utilizza in modo da poterla configurare in modo appropriato per l'ambiente in uso.

La tabella ONTAP name service switch determina le origini del servizio di nomi che ONTAP consulta per recuperare le informazioni relative a un determinato tipo di informazioni sul servizio di nomi. ONTAP gestisce una tabella di switch del name service separata per ogni SVM.

### Tipi di database

La tabella memorizza un elenco di name service separato per ciascuno dei seguenti tipi di database:

Tipo di database	Definisce le origini del servizio nome per...	Le origini valide sono...
host	Conversione dei nomi host in indirizzi IP	file, dns
gruppo	Ricerca di informazioni sul gruppo di utenti	file, nis, ldap
password	Ricerca delle informazioni dell'utente	file, nis, ldap
netgroup	Ricerca di informazioni sul netgroup	file, nis, ldap
mappa dei nomi	Mappatura dei nomi utente	file, ldap

### Tipi di origine

Le origini specificano quale nome di origine del servizio utilizzare per recuperare le informazioni appropriate.

Specifica tipo di origine...	Per cercare informazioni in...	Gestito dalle famiglie di comandi...
file	File di origine locali	<pre>vserver services name- service unix-user vserver services name-service unix-group  vserver services name- service netgroup  vserver services name- service dns hosts</pre>
nis	Server NIS esterni come specificato nella configurazione del dominio NIS di SVM	<pre>vserver services name- service nis-domain</pre>
ldap	Server LDAP esterni come specificato nella configurazione del client LDAP di SVM	<pre>vserver services name- service ldap</pre>
dns	Server DNS esterni come specificato nella configurazione DNS di SVM	<pre>vserver services name- service dns</pre>

Anche se si prevede di utilizzare NIS o LDAP per l'accesso ai dati e l'autenticazione dell'amministrazione SVM, è comunque necessario includere `files` E configurare gli utenti locali come fallback nel caso in cui l'autenticazione NIS o LDAP non riesca.

### Protocolli utilizzati per accedere a fonti esterne

Per accedere ai server per le origini esterne, ONTAP utilizza i seguenti protocolli:

Origine esterna del name service	Protocollo utilizzato per l'accesso
NIS	UDP
DNS	UDP
LDAP	TCP

### Esempio

Nell'esempio seguente viene visualizzata la configurazione dello switch name service per SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source Order
-----	-----	-----
svm_1	hosts	files, dns
svm_1	group	files
svm_1	passwd	files
svm_1	netgroup	nis, files

Per cercare gli indirizzi IP degli host, ONTAP consulta innanzitutto i file di origine locali. Se la query non restituisce alcun risultato, i server DNS vengono controllati in seguito.

Per cercare informazioni su utenti o gruppi, ONTAP consulta solo i file di origine locali. Se la query non restituisce alcun risultato, la ricerca non riesce.

Per cercare informazioni sui netgroup, ONTAP consulta prima i server NIS esterni. Se la query non restituisce alcun risultato, viene selezionato il file netgroup locale.

Non sono presenti voci di name service per la mappatura dei nomi nella tabella per SVM svm\_1. Pertanto, ONTAP consulta solo i file di origine locali per impostazione predefinita.

### Informazioni correlate

["Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"](#)

### Utilizzare LDAP

#### Panoramica LDAP

Un server LDAP (Lightweight Directory Access Protocol) consente di gestire centralmente le informazioni dell'utente. Se si memorizza il database utente su un server LDAP nell'ambiente in uso, è possibile configurare il sistema di storage in modo che cerchi le informazioni utente nel database LDAP esistente.

- Prima di configurare LDAP per ONTAP, verificare che l'implementazione del sito soddisfi le Best practice per la configurazione del server e del client LDAP. In particolare, devono essere soddisfatte le seguenti condizioni:
  - Il nome di dominio del server LDAP deve corrispondere alla voce del client LDAP.
  - I tipi di hash della password utente LDAP supportati dal server LDAP devono includere quelli supportati da ONTAP:
    - CRYPT (tutti i tipi) e SHA-1 (SHA, SSHA).
    - A partire da ONTAP 9.8, hash SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, Sono supportati anche SSHA-384 e SSHA-512).
  - Se il server LDAP richiede misure di protezione della sessione, è necessario configurarle nel client LDAP.

Sono disponibili le seguenti opzioni di sicurezza della sessione:

- Firma LDAP (verifica dell'integrità dei dati) e firma e sigillatura LDAP (verifica e crittografia dell'integrità dei dati)
- AVVIARE TLS
- LDAPS (LDAP su TLS o SSL)
- Per abilitare le query LDAP firmate e sealed, è necessario configurare i seguenti servizi:
  - I server LDAP devono supportare il meccanismo GSSAPI (Kerberos) SASL.
  - I server LDAP devono disporre di record DNS A/AAAA e di record PTR impostati sul server DNS.
  - I server Kerberos devono avere record SRV presenti sul server DNS.
- Per abilitare L'AVVIO di TLS o LDAPS, tenere in considerazione i seguenti punti.
  - L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.
  - Se si utilizza LDAPS, il server LDAP deve essere abilitato per TLS o per SSL in ONTAP 9.5 e versioni successive. SSL non è supportato in ONTAP 9.0-9.4.
  - Nel dominio deve essere già configurato un server dei certificati.
- Per abilitare la funzione LDAP referral chasing (in ONTAP 9.5 e versioni successive), devono essere soddisfatte le seguenti condizioni:
  - Entrambi i domini devono essere configurati con una delle seguenti relazioni di trust:
    - Bidirezionale
    - Unidirezionale, in cui il primario si affida al dominio di riferimento
    - Genitore-figlio
  - Il DNS deve essere configurato in modo da risolvere tutti i nomi dei server indicati.
  - Le password di dominio devono essere le stesse per autenticare quando `--bind-as-cifs -server` impostare su true.



Le seguenti configurazioni non sono supportate con la funzione LDAP referral chasing.

- Per tutte le versioni di ONTAP:
- Client LDAP su una SVM amministrativa
- Per ONTAP 9.8 e versioni precedenti (sono supportati nella versione 9.9.1 e successive):
- Firma e sigillatura LDAP (il `-session-security` opzionale)
- Connessioni TLS crittografate (il `-use-start-tls` opzionale)
- Comunicazioni tramite la porta LDAPS 636 (la `-use-ldaps-for-ad-ldap` opzionale)

- A partire da ONTAP 9.11.1, è possibile utilizzare ["LDAP fast bind per l'autenticazione nsswitch."](#)
- È necessario inserire uno schema LDAP durante la configurazione del client LDAP su SVM.

Nella maggior parte dei casi, uno degli schemi ONTAP predefiniti sarà appropriato. Tuttavia, se lo schema LDAP nel proprio ambiente differisce da questi, è necessario creare un nuovo schema client LDAP per ONTAP prima di creare il client LDAP. Rivolgersi all'amministratore LDAP per informazioni sui requisiti dell'ambiente in uso.

- L'utilizzo di LDAP per la risoluzione dei nomi host non è supportato.

Per ulteriori informazioni, vedere ["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#).

## Concetti relativi alla firma e al sealing LDAP

A partire da ONTAP 9, è possibile configurare la firma e il sealing per abilitare la sicurezza della sessione LDAP sulle query a un server Active Directory (ad). È necessario configurare le impostazioni di sicurezza del server NFS sulla macchina virtuale di storage (SVM) in modo che corrispondano a quelle del server LDAP.

La firma conferma l'integrità dei dati del payload LDAP utilizzando la tecnologia a chiave segreta. Il sealing crittografa i dati del payload LDAP per evitare la trasmissione di informazioni sensibili in testo non crittografato. Un'opzione *LDAP Security Level* indica se il traffico LDAP deve essere firmato, firmato e sigillato o no. L'impostazione predefinita è `none`. test

La firma LDAP e il sealing sul traffico SMB sono attivati sulla SVM con `-session-security-for-ad-ldap` al `vserver cifs security modify` comando.

## Concetti LDAPS

È necessario comprendere alcuni termini e concetti relativi al modo in cui ONTAP protegge le comunicazioni LDAP. ONTAP può utilizzare TLS O LDAPS DI AVVIO per impostare sessioni autenticate tra server LDAP integrati in Active Directory o server LDAP basati su UNIX.

## Terminologia

È necessario comprendere alcuni termini relativi all'utilizzo di LDAPS da parte di ONTAP per proteggere le comunicazioni LDAP.

### • LDAP

(Lightweight Directory Access Protocol) protocollo per l'accesso e la gestione delle directory di informazioni. LDAP viene utilizzato come directory di informazioni per la memorizzazione di oggetti come utenti, gruppi e netgroup. LDAP fornisce inoltre servizi di directory che gestiscono questi oggetti e soddisfano le richieste LDAP dai client LDAP.

### • SSL

(Secure Sockets Layer) protocollo sviluppato per l'invio sicuro di informazioni su Internet. SSL è supportato da ONTAP 9 e versioni successive, ma è stato deprecato a favore di TLS.

### • TLS

(Transport Layer Security) un protocollo di tracciamento degli standard IETF basato sulle specifiche SSL precedenti. È il successore di SSL. TLS è supportato da ONTAP 9,5 e versioni successive.

### • LDAPS (LDAP su SSL o TLS)

Protocollo che utilizza TLS o SSL per proteggere le comunicazioni tra client LDAP e server LDAP. I termini *LDAP su SSL* e *LDAP su TLS* vengono talvolta utilizzati in modo intercambiabile. LDAPS è supportato da ONTAP 9,5 e versioni successive.



- In ONTAP 9.5-9.8, LDAPS può essere attivato solo sulla porta 636. A tale scopo, utilizzare `-use -ldaps-for-ad-ldap` con il `vserver cifs security modify` comando.
- A partire da ONTAP 9.9.1, LDAPS può essere attivato su qualsiasi porta, anche se la porta 636 rimane quella predefinita. A tale scopo, impostare `-ldaps-enabled` parametro a `true` e specificare il desiderato `-port` parametro. Per ulteriori informazioni, consultare `vserver services name-service ldap client create` pagina man



L'utilizzo di Start TLS anziché LDAPS è una Best practice di NetApp.

## • Avvia TLS

(Noto anche come *start\_tls*, *STARTTLS* e *STARTTLS*) un meccanismo per fornire comunicazioni sicure utilizzando i protocolli TLS.

ONTAP utilizza STARTTLS per proteggere la comunicazione LDAP e la porta LDAP predefinita (389) per comunicare con il server LDAP. Il server LDAP deve essere configurato in modo da consentire le connessioni sulla porta LDAP 389; in caso contrario, le connessioni LDAP TLS dalla SVM al server LDAP non funzionano.

## Utilizzo di LDAPS da parte di ONTAP

ONTAP supporta l'autenticazione del server TLS, che consente al client LDAP SVM di confermare l'identità del server LDAP durante l'operazione di binding. I client LDAP abilitati per TLS possono utilizzare tecniche standard di crittografia a chiave pubblica per verificare che il certificato e l'ID pubblico di un server siano validi e siano stati emessi da un'autorità di certificazione (CA) elencata nell'elenco delle CA attendibili del client.

LDAP supporta STARTTLS per crittografare le comunicazioni utilizzando TLS. STARTTLS inizia come connessione non crittografata sulla porta LDAP standard (389) e la connessione viene quindi aggiornata a TLS.

ONTAP supporta:

- LDAPS per il traffico SMB tra i server LDAP integrati in Active Directory e SVM
- LDAPS per il traffico LDAP per la mappatura dei nomi e altre informazioni UNIX

I server LDAP integrati in Active Directory o i server LDAP basati su UNIX possono essere utilizzati per memorizzare informazioni per la mappatura dei nomi LDAP e altre informazioni UNIX, come utenti, gruppi e netgroup.

- Certificati della CA principale autofirmati

Quando si utilizza un LDAP integrato in Active-Directory, il certificato root autofirmato viene generato quando il servizio certificati di Windows Server viene installato nel dominio. Quando si utilizza un server LDAP basato su UNIX per la mappatura dei nomi LDAP, il certificato root autofirmato viene generato e salvato utilizzando i mezzi appropriati per l'applicazione LDAP.

Per impostazione predefinita, LDAPS è disattivato.

## Attiva il supporto LDAP RFC2307bis

Se si desidera utilizzare LDAP e si desidera utilizzare le appartenenze a gruppi nidificati, è possibile configurare ONTAP per abilitare il supporto di LDAP RFC2307bis.

## Di cosa hai bisogno

È necessario aver creato una copia di uno degli schemi client LDAP predefiniti che si desidera utilizzare.

## A proposito di questa attività

Negli schemi client LDAP, gli oggetti di gruppo utilizzano l'attributo `memberUid`. Questo attributo può contenere più valori ed elenca i nomi degli utenti che appartengono a quel gruppo. Negli schemi client LDAP abilitati per RFC2307bis, gli oggetti di gruppo utilizzano l'attributo `uniqueMember`. Questo attributo può contenere il nome distinto completo (DN) di un altro oggetto nella directory LDAP. In questo modo è possibile utilizzare gruppi nidificati poiché i gruppi possono avere altri gruppi come membri.

L'utente non deve essere membro di più di 256 gruppi, inclusi i gruppi nidificati. ONTAP ignora tutti i gruppi che superano il limite di 256 gruppi.

Per impostazione predefinita, il supporto RFC2307bis è disattivato.



Il supporto RFC2307bis viene attivato automaticamente in ONTAP quando viene creato un client LDAP con lo schema MS-ad-BIS.

Per ulteriori informazioni, vedere ["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#).

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Modificare lo schema del client LDAP RFC2307 copiato per abilitare il supporto RFC2307bis:

```
vserver services name-service ldap client schema modify -vserver vserver_name  
-schema schema-name -enable-rfc2307bis true
```

3. Modificare lo schema in modo che corrisponda alla classe di oggetti supportata nel server LDAP:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -group-of-unique-names-object-class object_class
```

4. Modificare lo schema in modo che corrisponda al nome dell'attributo supportato nel server LDAP:

```
vserver services name-service ldap client schema modify -vserver vserver-name  
-schema schema_name -unique-member-attribute attribute_name
```

5. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Opzioni di configurazione per le ricerche nelle directory LDAP

È possibile ottimizzare le ricerche nelle directory LDAP, incluse le informazioni relative a utenti, gruppi e netgroup, configurando il client LDAP di ONTAP per la connessione ai server LDAP nel modo più appropriato per il proprio ambiente. È necessario capire quando sono sufficienti i valori di ricerca predefiniti di base e ambito LDAP e quali parametri specificare quando i valori personalizzati sono più appropriati.

Le opzioni di ricerca del client LDAP per le informazioni relative a utenti, gruppi e netgroup possono aiutare a evitare query LDAP non riuscite e, di conseguenza, l'accesso del client ai sistemi di storage non riuscito. Inoltre, contribuiscono a garantire che le ricerche siano il più efficienti possibile per evitare problemi di performance del client.

### Valori di base e di ricerca dell'ambito predefiniti

La base LDAP è il DN di base predefinito utilizzato dal client LDAP per eseguire query LDAP. Tutte le ricerche, incluse quelle relative a utenti, gruppi e netgroup, vengono eseguite utilizzando il DN di base. Questa opzione è appropriata quando la directory LDAP è relativamente piccola e tutte le voci pertinenti si trovano nello stesso DN.

Se non si specifica un DN di base personalizzato, il valore predefinito è `root`. Ciò significa che ogni query esegue la ricerca nell'intera directory. Sebbene questo massimizzi le possibilità di successo della query LDAP, può essere inefficiente e causare una riduzione significativa delle prestazioni con directory LDAP di grandi dimensioni.

L'ambito di base LDAP è l'ambito di ricerca predefinito utilizzato dal client LDAP per eseguire query LDAP. Tutte le ricerche, incluse quelle relative a utenti, gruppi e netgroup, vengono eseguite utilizzando l'ambito di base. Determina se la query LDAP ricerca solo la voce denominata, le voci di un livello al di sotto del DN o l'intera sottostruttura al di sotto del DN.

Se non si specifica un ambito di base personalizzato, il valore predefinito è `subtree`. Ciò significa che ogni query esegue la ricerca nell'intero sottostruttura sotto il DN. Sebbene questo massimizzi le possibilità di successo della query LDAP, può essere inefficiente e causare una riduzione significativa delle prestazioni con directory LDAP di grandi dimensioni.

### Valori di ricerca di base e ambito personalizzati

In alternativa, è possibile specificare valori di base e di ambito separati per le ricerche di utenti, gruppi e netgroup. La limitazione della base di ricerca e dell'ambito delle query in questo modo può migliorare significativamente le prestazioni, poiché limita la ricerca a una sottosezione più piccola della directory LDAP.

Se si specificano valori di base e ambito personalizzati, questi sovrascrivono la base di ricerca predefinita generale e l'ambito per le ricerche di utenti, gruppi e netgroup. I parametri per specificare i valori di base e ambito personalizzati sono disponibili a livello di privilegio avanzato.

Parametro client LDAP...	Specifica custom...
<code>-base-dn</code>	DN di base per tutte le ricerche LDAP è possibile inserire più valori, se necessario (ad esempio, se la funzione LDAP referral chasing è attivata in ONTAP 9.5 e versioni successive).
<code>-base-scope</code>	Ambito di base per tutte le ricerche LDAP
<code>-user-dn</code>	DNS di base per tutte le ricerche degli utenti LDAP questo parametro si applica anche alle ricerche di mappatura dei nomi utente.
<code>-user-scope</code>	Ambito di base per tutte le ricerche degli utenti LDAP questo parametro si applica anche alle ricerche di associazione dei nomi utente.

<code>-group-dn</code>	DNS di base per tutte le ricerche di gruppi LDAP
<code>-group-scope</code>	Ambito di base per tutte le ricerche di gruppi LDAP
<code>-netgroup-dn</code>	DNS di base per tutte le ricerche dei netgroup LDAP
<code>-netgroup-scope</code>	Ambito di base per tutte le ricerche dei netgroup LDAP

### Più valori DN di base personalizzati

Se la struttura della directory LDAP è più complessa, potrebbe essere necessario specificare più DNS di base per cercare determinate informazioni in più parti della directory LDAP. È possibile specificare più DNS per i parametri DN dell'utente, del gruppo e del netgroup separandoli con un punto e virgola (;) e racchiudendo l'intero elenco di ricerca DN con virgolette doppie ("). Se un DN contiene un punto e virgola, è necessario aggiungere un carattere di escape (\) immediatamente prima del punto e virgola nel DN.

Si noti che l'ambito si applica all'intero elenco di DNS specificato per il parametro corrispondente. Ad esempio, se si specifica un elenco di tre diversi DNS utente e sottostruttura per l'ambito utente, l'utente LDAP ricerca nell'intera sottostruttura ciascuno dei tre DNS specificati.

A partire da ONTAP 9.5, è anche possibile specificare LDAP *referral chasing*, che consente al client LDAP di indirizzare le richieste di ricerca ad altri server ONTAP se il server LDAP primario non restituisce una risposta di riferimento LDAP. Il client utilizza i dati di riferimento per recuperare l'oggetto di destinazione dal server descritto nei dati di riferimento. Per cercare oggetti presenti nei server LDAP indicati, è possibile aggiungere la base-dn degli oggetti indicati alla base-dn come parte della configurazione del client LDAP. Tuttavia, gli oggetti referralati vengono ricercati solo quando è attivata la funzione di referral chasing (ricerca riferimenti), utilizzando il `-referral-enabled true` Durante la creazione o la modifica del client LDAP.

### Migliorare le performance delle ricerche di directory LDAP netgroup-by-host

Se l'ambiente LDAP è configurato per consentire ricerche netgroup-by-host, è possibile configurare ONTAP in modo che ne tragga vantaggio ed eseguire ricerche netgroup-by-host. In questo modo è possibile accelerare notevolmente le ricerche dei netgroup e ridurre i possibili problemi di accesso al client NFS dovuti alla latenza durante le ricerche dei netgroup.

#### Di cosa hai bisogno

La directory LDAP deve contenere un `netgroup.byhost` mappa.

I server DNS devono contenere record di ricerca sia in avanti (A) che in retromarcia (PTR) per i client NFS.

Quando si specificano gli indirizzi IPv6 nei netgroup, è sempre necessario accorciare e comprimere ciascun indirizzo come specificato in RFC 5952.

#### A proposito di questa attività

I server NIS memorizzano le informazioni del netgroup in tre mappe distinte denominate `netgroup`, `netgroup.byuser`, e `netgroup.byhost`. Lo scopo di `netgroup.byuser` e `netgroup.byhost` maps consente di velocizzare le ricerche di netgroup. ONTAP può eseguire ricerche netgroup-by-host sui server NIS per migliorare i tempi di risposta del montaggio.

Per impostazione predefinita, le directory LDAP non dispongono di tale opzione `netgroup.byhost` mappare come i server NIS. Tuttavia, con l'aiuto di strumenti di terze parti, è possibile importare un NIS `netgroup.byhost` eseguire la mappatura nelle directory LDAP per consentire ricerche rapide `netgroup-by-host`. Se l'ambiente LDAP è stato configurato per consentire ricerche `netgroup-by-host`, è possibile configurare il client LDAP ONTAP con `netgroup.byhost` nome mappa, DN e ambito di ricerca per ricerche più rapide tra `netgroup` e `host`.

La ricezione più rapida dei risultati per le ricerche `netgroup-by-host` consente a ONTAP di elaborare più rapidamente le regole di esportazione quando i client NFS richiedono l'accesso alle esportazioni. In questo modo si riduce la possibilità di ritardi di accesso dovuti a problemi di latenza della ricerca nel `netgroup`.

## Fasi

1. Ottenere l'esatto nome completo del NIS `netgroup.byhost` mappatura importata nella directory LDAP.

Il DN della mappa può variare a seconda dello strumento di terze parti utilizzato per l'importazione. Per ottenere prestazioni ottimali, specificare il DN esatto della mappa.

2. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
3. Abilitare le ricerche `netgroup-by-host` nella configurazione client LDAP della macchina virtuale di storage (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost -dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

`-is-netgroup-byhost-enabled {true false}` Attiva o disattiva la ricerca `netgroup-by-host` delle directory LDAP. L'impostazione predefinita è `false`.

`-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` specifica il nome distinto di `netgroup.byhost` mappare la directory LDAP. Sovrascrive il DN di base per le ricerche `netgroup-by-host`. Se non si specifica questo parametro, ONTAP utilizza invece il DN di base.

`-netgroup-byhost-scope {base|onelevel subtree}` specifica l'ambito di ricerca per le ricerche `netgroup-by-host`. Se non si specifica questo parametro, l'impostazione predefinita è `subtree`.

Se la configurazione del client LDAP non esiste ancora, è possibile attivare le ricerche `netgroup-by-host` specificando questi parametri quando si crea una nuova configurazione del client LDAP utilizzando `vserver services name-service ldap client create` comando.



A partire da ONTAP 9.2, il campo `-ldap-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server LDAP.

4. Tornare al livello di privilegio admin: `set -privilege admin`

## Esempio

Il seguente comando modifica la configurazione del client LDAP esistente denominata `ldap_corp` per abilitare le ricerche `netgroup-by-host` utilizzando `netgroup.byhost` mappa denominata `"nisMapName="netgroup.byhost",DC=corp,DC=example,DC=com"` e l'ambito di ricerca predefinito `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

## Al termine

Il `netgroup.byhost` e `netgroup` le mappe nella directory devono essere sempre sincronizzate per evitare problemi di accesso al client.

## Informazioni correlate

["IETF RFC 5952: Una raccomandazione per la rappresentazione del testo dell'indirizzo IPv6"](#)

## Utilizza il binding rapido LDAP per l'autenticazione nsswitch

A partire da ONTAP 9.11.1, è possibile sfruttare la funzionalità LDAP *fast bind* (nota anche come *Concurrent BIND*) per richieste di autenticazione client più semplici e veloci. Per utilizzare questa funzionalità, il server LDAP deve supportare la funzionalità di associazione rapida.

## A proposito di questa attività

Senza il binding rapido, ONTAP utilizza il binding semplice LDAP per autenticare gli utenti amministratori con il server LDAP. Con questo metodo di autenticazione, ONTAP invia un nome utente o di gruppo al server LDAP, riceve la password hash memorizzata e confronta il codice hash del server con il codice hash generato localmente dalla password utente. Se sono identici, ONTAP concede l'autorizzazione di accesso.

Grazie alla funzionalità di associazione rapida, ONTAP invia solo le credenziali utente (nome utente e password) al server LDAP tramite una connessione sicura. Il server LDAP convalida quindi queste credenziali e richiede a ONTAP di concedere le autorizzazioni di accesso.

Uno dei vantaggi di fast bind è che non è necessario che ONTAP supporti ogni nuovo algoritmo di hashing supportato dai server LDAP, perché l'hashing delle password viene eseguito dal server LDAP.

## "Scopri come utilizzare fast bind."

È possibile utilizzare le configurazioni client LDAP esistenti per l'associazione rapida LDAP. Tuttavia, si consiglia vivamente di configurare il client LDAP per TLS o LDAPS; in caso contrario, la password viene inviata via cavo in testo normale.

Per abilitare il binding rapido LDAP in un ambiente ONTAP, è necessario soddisfare i seguenti requisiti:

- Gli utenti admin di ONTAP devono essere configurati su un server LDAP che supporti il fast bind.
- ONTAP SVM deve essere configurato per LDAP nel database name Services switch (nsswitch).
- Gli account di gruppo e utente amministratore di ONTAP devono essere configurati per l'autenticazione nsswitch utilizzando il collegamento rapido.

## Fasi

1. Verificare con l'amministratore LDAP che il collegamento rapido LDAP sia supportato sul server LDAP.
2. Assicurarsi che le credenziali dell'utente amministratore di ONTAP siano configurate sul server LDAP.
3. Verificare che l'amministratore o l'SVM dei dati sia configurato correttamente per il binding rapido LDAP.

- a. Per confermare che il server fast bind LDAP è elencato nella configurazione del client LDAP, immettere:

```
vserver services name-service ldap client show
```

["Informazioni sulla configurazione del client LDAP."](#)

- b. Per confermare ldap è una delle sorgenti configurate per nsswitch passwd database, inserire:

```
vserver services name-service ns-switch show
```

["Scopri di più sulla configurazione di nsswitch."](#)

4. Assicurarsi che gli utenti admin stiano autenticando con nsswitch e che l'autenticazione LDAP fast bind sia attivata nei propri account.

- Per gli utenti esistenti, immettere `security login modify` e verificare le seguenti impostazioni dei parametri:

```
-authentication-method nsswitch
```

```
-is-ldap-fastbind true
```

- Per i nuovi utenti admin, vedere ["Abilitare l'accesso all'account LDAP o NIS."](#)

## Visualizzare le statistiche LDAP

A partire da ONTAP 9.2, è possibile visualizzare le statistiche LDAP per le macchine virtuali di storage (SVM) su un sistema storage per monitorare le performance e diagnosticare i problemi.

### Di cosa hai bisogno

- È necessario aver configurato un client LDAP su SVM.
- Gli oggetti LDAP da cui è possibile visualizzare i dati devono essere stati identificati.

### Fase

1. Visualizzare i dati delle performance per gli oggetti del contatore:

```
statistics show
```

### Esempi

Nell'esempio riportato di seguito vengono illustrati i dati relativi alle prestazioni per l'oggetto `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"
```

Object: secd\_external\_service\_op

Instance: vserverName:LDAP (NIS & Name

Mapping):GetUserInfoFromName:1.1.1.1

Start-time: 4/13/2016 22:15:38

End-time: 4/13/2016 22:15:38

Scope: vserverName

Counter	Value
instance_name	vserverName:LDAP (NIS & Name Mapping):GetUserInfoFromName: 1.1.1.1
last_modified_time	1460610787
node_name	nodeName
num_not_found_responses	1
num_request_failures	1
num_requests_sent	1
num_responses_received	1
num_successful_responses	0
num_timeouts	0
operation	GetUserInfoFromName
process_name	secd
request_latency	52131us

## Configurare le mappature dei nomi

### Panoramica sulla configurazione delle mappature dei nomi

ONTAP utilizza la mappatura dei nomi per mappare le identità SMB alle identità UNIX, le identità Kerberos alle identità UNIX e le identità UNIX alle identità SMB. Queste informazioni sono necessarie per ottenere le credenziali dell'utente e fornire l'accesso corretto ai file, indipendentemente dal fatto che si stia connettendo da un client NFS o SMB.

Esistono due eccezioni per le quali non è necessario utilizzare la mappatura dei nomi:

- Si configura un ambiente UNIX puro e non si prevede di utilizzare l'accesso SMB o lo stile di sicurezza NTFS sui volumi.
- Viene configurato l'utente predefinito da utilizzare.

In questo scenario, la mappatura dei nomi non è necessaria perché, invece di mappare ogni singola credenziale client, tutte le credenziali client vengono mappate allo stesso utente predefinito.



Si noti che è possibile utilizzare la mappatura dei nomi solo per gli utenti, non per i gruppi.

Tuttavia, è possibile mappare un gruppo di singoli utenti a un utente specifico. Ad esempio, è possibile mappare tutti gli utenti ad che iniziano o terminano con la parola SALES a un utente UNIX specifico e all'UID dell'utente.

#### **Come funziona la mappatura dei nomi**

Quando ONTAP deve mappare le credenziali per un utente, controlla innanzitutto il database di mappatura dei nomi locali e il server LDAP per verificare la presenza di una mappatura esistente. Se controlla uno o entrambi e in quale ordine viene determinato dalla configurazione del servizio di nomi della SVM.

- Per la mappatura da Windows a UNIX

Se non viene trovata alcuna mappatura, ONTAP verifica se il nome utente Windows minuscolo è un nome utente valido nel dominio UNIX. Se non funziona, utilizza l'utente UNIX predefinito, a condizione che sia configurato. Se l'utente UNIX predefinito non è configurato e ONTAP non può ottenere un mapping in questo modo, il mapping non riesce e viene restituito un errore.

- Per la mappatura da UNIX a Windows

Se non viene trovata alcuna mappatura, ONTAP tenta di trovare un account Windows che corrisponda al nome UNIX nel dominio SMB. Se non funziona, utilizza l'utente SMB predefinito, a condizione che sia configurato. Se l'utente SMB predefinito non è configurato e ONTAP non può ottenere un mapping in questo modo, il mapping non riesce e viene restituito un errore.

Per impostazione predefinita, gli account del computer vengono mappati all'utente UNIX predefinito specificato. Se non viene specificato alcun utente UNIX predefinito, il mapping degli account del computer non riesce.

- A partire da ONTAP 9.5, è possibile mappare gli account dei computer a utenti diversi da quelli predefiniti.
- In ONTAP 9.4 e versioni precedenti, non è possibile mappare gli account dei computer ad altri utenti.

Anche se vengono definite le mappature dei nomi per gli account macchina, le mappature vengono ignorate.

#### **Multidominio ricerca le mappature dei nomi utente da UNIX a Windows**

ONTAP supporta le ricerche su più domini durante la mappatura degli utenti UNIX agli utenti Windows. In tutti i domini attendibili rilevati vengono ricercate le corrispondenze del modello di sostituzione fino a quando non viene restituito un risultato corrispondente. In alternativa, è possibile configurare un elenco di domini attendibili preferiti, che viene utilizzato al posto dell'elenco di domini attendibili rilevati e che viene ricercato in ordine fino a quando non viene restituito un risultato corrispondente.

#### **Il modo in cui i trust di dominio influiscono sulle ricerche di mappatura dei nomi utente da UNIX a Windows**

Per comprendere il funzionamento della mappatura dei nomi utente multidominio, è necessario comprendere il funzionamento dei trust di dominio con ONTAP. Le relazioni di trust di Active Directory con il dominio principale del server SMB possono essere un trust bidirezionale o uno dei due tipi di trust unidirezionali, un trust in

entrata o un trust in uscita. Il dominio principale è il dominio a cui appartiene il server SMB sulla SVM.

- *Fiducia bidirezionale*

Con trust bidirezionali, entrambi i domini si fidano l'uno dell'altro. Se il dominio principale del server SMB ha un trust bidirezionale con un altro dominio, il dominio principale può autenticare e autorizzare un utente appartenente al dominio attendibile e viceversa.

Le ricerche di associazione dei nomi utente da UNIX a Windows possono essere eseguite solo su domini con trust bidirezionali tra il dominio principale e l'altro dominio.

- *Fiducia in uscita*

Con un trust in uscita, il dominio principale considera attendibile l'altro dominio. In questo caso, il dominio principale può autenticare e autorizzare un utente appartenente al dominio trusted in uscita.

Un dominio con un trust in uscita con il dominio principale viene *not* ricercato quando si eseguono ricerche di mappatura da utente UNIX a nome utente Windows.

- *Fiducia in entrata*


Con un trust inbound, l'altro dominio considera attendibile il dominio principale del server SMB. In questo caso, il dominio principale non può autenticare o autorizzare un utente appartenente al dominio trusted in entrata.

Un dominio con un trust in entrata con il dominio principale viene *not* ricercato quando si eseguono ricerche di associazione tra utenti UNIX e nomi utente Windows.

**Modalità di utilizzo dei caratteri jolly (\*) per configurare le ricerche su più domini per la mappatura dei nomi**

Le ricerche di mappatura dei nomi multidominio sono facilitate dall'utilizzo di caratteri jolly nella sezione dominio del nome utente di Windows. Nella tabella seguente viene illustrato come utilizzare i caratteri jolly nella parte di dominio di una voce di mappatura dei nomi per abilitare le ricerche su più domini:

Schema	Sostituzione	Risultato
root	amministratore di *\\	L'utente UNIX "root" viene mappato all'utente "Administrator". Tutti i domini attendibili vengono ricercati in ordine fino a quando non viene trovato il primo utente corrispondente "Administrator".

Schema	Sostituzione	Risultato
*	*\\*	<p>Gli utenti UNIX validi vengono mappati ai corrispondenti utenti Windows. Tutti i domini attendibili vengono ricercati in ordine fino a quando non viene trovato il primo utente corrispondente a tale nome.</p> <div>  <p>Il modello {asterisco}\\{asterisco} è valido solo per la mappatura dei nomi da UNIX a Windows, non viceversa.</p> </div>

### Come vengono eseguite le ricerche di nomi multidominio

È possibile scegliere uno dei due metodi per determinare l'elenco di domini attendibili utilizzati per la ricerca di nomi di più domini:

- Utilizzare l'elenco di attendibilità bidirezionale rilevato automaticamente compilato da ONTAP
- Utilizzare l'elenco di domini attendibili preferito compilato

Se un utente UNIX viene mappato a un utente Windows con un carattere jolly utilizzato per la sezione di dominio del nome utente, l'utente Windows viene ricercato in tutti i domini attendibili nel modo seguente:

- Se viene configurato un elenco di domini attendibili preferito, l'utente Windows mappato viene ricercato solo in questo elenco di ricerca, in ordine.
- Se un elenco preferito di domini attendibili non è configurato, l'utente Windows viene ricercato in tutti i domini attendibili bidirezionali del dominio principale.
- Se non esistono domini trusted bidirezionalmente per il dominio principale, l'utente viene ricercato nel dominio principale.

Se un utente UNIX viene mappato a un utente Windows senza una sezione di dominio nel nome utente, l'utente Windows viene ricercato nel dominio principale.

### Regole di conversione del mapping dei nomi

Un sistema ONTAP mantiene una serie di regole di conversione per ogni SVM. Ogni regola è composta da due parti: Un *pattern* e un *replacement*. Le conversioni iniziano all'inizio dell'elenco appropriato ed eseguono una sostituzione in base alla prima regola di corrispondenza. Il modello è un'espressione regolare in stile UNIX. La sostituzione è una stringa contenente sequenze di escape che rappresentano sottoespressioni del modello, come in UNIX `sed` programma.

### Creare una mappatura dei nomi

È possibile utilizzare `vserver name-mapping create` per creare una mappatura dei

nomi. Si utilizzano le mappature dei nomi per consentire agli utenti Windows di accedere ai volumi di sicurezza UNIX e viceversa.

### A proposito di questa attività

Per ogni SVM, ONTAP supporta fino a 12,500 mappature di nomi per ciascuna direzione.

### Fase

1. Creazione di una mappatura dei nomi:

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text
```



Il `-pattern` e `-replacement` le dichiarazioni possono essere formulate come espressioni regolari. È inoltre possibile utilizzare `-replacement` per negare esplicitamente un mapping all'utente utilizzando la stringa di sostituzione nulla " " (il carattere dello spazio). Vedere `vserver name-mapping create` pagina man per i dettagli.

Quando vengono create mappature da Windows a UNIX, tutti i client SMB che hanno connessioni aperte al sistema ONTAP al momento della creazione delle nuove mappature devono disconnettersi e riconnettersi per visualizzare le nuove mappature.

### Esempi

Il seguente comando crea un mapping dei nomi sulla SVM denominata vs1. Il mapping è un mapping da UNIX a Windows nella posizione 1 nell'elenco delle priorità. Il mapping associa l'utente UNIX Johnd all'utente Windows ENG/JohnDoe.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win  
-position 1 -pattern johnd  
-replacement "ENG\\JohnDoe"
```

Il seguente comando crea un'altra mappatura dei nomi sulla SVM denominata vs1. Il mapping è un mapping da Windows a UNIX nella posizione 1 nell'elenco delle priorità. Qui il modello e la sostituzione includono espressioni regolari. Il mapping associa ogni utente CIFS nel dominio ENG agli utenti nel dominio LDAP associato alla SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix  
-position 1 -pattern "ENG\\(.+)"  
-replacement "\\1"
```

Il seguente comando crea un'altra mappatura dei nomi sulla SVM denominata vs1. Qui il modello include "" come elemento nel nome utente di Windows che deve essere escapato. La mappatura mappa l'utente Windows ENG all'utente UNIX john\_Ops.

```
vs1::> vserver name-mapping create -direction win-unix -position 1  
-pattern ENG\\john$ops  
-replacement john_ops
```

## Configurare l'utente predefinito

È possibile configurare un utente predefinito da utilizzare se tutti gli altri tentativi di mappatura non riescono per un utente o se non si desidera mappare singoli utenti tra UNIX e Windows. In alternativa, se si desidera che l'autenticazione degli utenti non mappati non venga eseguita correttamente, non è necessario configurare un utente predefinito.

### A proposito di questa attività

Per l'autenticazione CIFS, se non si desidera associare ciascun utente Windows a un singolo utente UNIX, è possibile specificare un utente UNIX predefinito.

Per l'autenticazione NFS, se non si desidera associare ciascun utente UNIX a un singolo utente Windows, è possibile specificare un utente Windows predefinito.

### Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Configurare l'utente UNIX predefinito	<code>vserver cifs options modify -default-unix-user user_name</code>
Configurare l'utente Windows predefinito	<code>vserver nfs modify -default-win-user user_name</code>

## Comandi per la gestione delle mappature dei nomi

Esistono comandi ONTAP specifici per la gestione delle mappature dei nomi.

Se si desidera...	Utilizzare questo comando...
Creare una mappatura dei nomi	<code>vserver name-mapping create</code>
Inserire una mappatura dei nomi in una posizione specifica	<code>vserver name-mapping insert</code>
Visualizza mappature dei nomi	<code>vserver name-mapping show</code>
Scambiare la posizione di due mappature dei nomi NOTA: Non è consentito eseguire uno swap quando la mappatura dei nomi è configurata con una voce di qualificatore ip.	<code>vserver name-mapping swap</code>
Modificare una mappatura dei nomi	<code>vserver name-mapping modify</code>

Eliminare una mappatura dei nomi	<code>vserver name-mapping delete</code>
Convalidare la corretta mappatura dei nomi	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Abilitare l'accesso per i client NFS di Windows

ONTAP supporta l'accesso ai file dai client NFSv3 di Windows. Ciò significa che i client che eseguono sistemi operativi Windows con supporto NFSv3 possono accedere ai file delle esportazioni NFSv3 nel cluster. Per utilizzare correttamente questa funzionalità, è necessario configurare correttamente la macchina virtuale di storage (SVM) ed essere consapevoli di determinati requisiti e limitazioni.

#### A proposito di questa attività

Per impostazione predefinita, il supporto del client Windows NFSv3 è disattivato.

#### Prima di iniziare

NFSv3 deve essere attivato su SVM.

#### Fasi

1. Abilitare il supporto del client Windows NFSv3:

```
vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
```

2. Su tutti gli SVM che supportano i client Windows NFSv3, disattivare `-enable-ejukebox` e `-v3 -connection-drop` parametri:

```
vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled
```

I client Windows NFSv3 possono ora montare le esportazioni sul sistema storage.

3. Assicurarsi che ogni client Windows NFSv3 utilizzi i supporti rigidi specificando `-o mtype=hard` opzione.

Questo è necessario per garantire montaggi affidabili.

```
mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
```

### Abilitare la visualizzazione delle esportazioni NFS sui client NFS

I client NFS possono utilizzare `showmount -e` Per visualizzare un elenco delle esportazioni disponibili da un server NFS ONTAP. In questo modo, gli utenti possono identificare il file system che desiderano montare.

A partire da ONTAP 9.2, ONTAP consente ai client NFS di visualizzare l'elenco di esportazione per

impostazione predefinita. Nelle versioni precedenti, il `showmount` opzione di `vserver nfs modify` il comando deve essere attivato in modo esplicito. Per visualizzare l'elenco di esportazione, è necessario attivare NFSv3 su SVM.

**Esempio**

Il seguente comando mostra la funzione `showmount` sulla SVM denominata `vs1`:

```
cluster1 : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
-----
vs1      enabled
```

Il seguente comando eseguito su un client NFS visualizza l'elenco delle esportazioni su un server NFS con l'indirizzo IP 10.63.21.9:

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix      (everyone)
/unix/unix1 (everyone)
/unix/unix2 (everyone)
/          (everyone)
```

**Gestire l'accesso ai file con NFS**

**Attivare o disattivare NFSv3**

È possibile attivare o disattivare NFSv3 modificando il `-v3` opzione. Ciò consente l'accesso ai file per i client che utilizzano il protocollo NFSv3. Per impostazione predefinita, NFSv3 è attivato.

**Fase**

- 1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Abilitare NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 enabled</code>
Disattiva NFSv3	<code>vserver nfs modify -vserver vserver_name -v3 disabled</code>

**Attivare o disattivare NFSv4.0**

È possibile attivare o disattivare NFSv4.0 modificando il `-v4.0` opzione. Questo consente l'accesso al file per i client che utilizzano il protocollo NFSv4.0. In ONTAP 9.9.1, NFSv4.0 è attivato per impostazione predefinita; nelle versioni precedenti, è disattivato per impostazione predefinita.

## Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare NFSv4.0	<pre>vserver nfs modify -vserver vserver_name -v4.0 enabled</pre>
Disattiva NFSv4.0	<pre>vserver nfs modify -vserver vserver_name -v4.0 disabled</pre>

## Attivare o disattivare NFSv4.1

È possibile attivare o disattivare NFSv4.1 modificando il `-v4.1` opzione. Ciò consente l'accesso ai file per i client che utilizzano il protocollo NFSv4.1. In ONTAP 9.9.1, NFSv4.1 è attivato per impostazione predefinita; nelle versioni precedenti, è disattivato per impostazione predefinita.

## Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare NFSv4.1	<pre>vserver nfs modify -vserver vserver_name -v4.1 enabled</pre>
Disattiva NFSv4.1	<pre>vserver nfs modify -vserver vserver_name -v4.1 disabled</pre>

## Gestire i limiti dello storepool di NFSv4

A partire da ONTAP 9.13, gli amministratori possono consentire ai server NFSv4 di negare le risorse ai client NFSv4 quando raggiungono i limiti di risorse dello storepool per client. Quando i client consumano troppe risorse dello storepool NFSv4, questo può causare il blocco di altri client NFSv4 a causa della mancata disponibilità delle risorse dello storepool NFSv4.

L'attivazione di questa funzionalità consente inoltre ai clienti di visualizzare il consumo attivo delle risorse dello storepool da parte di ciascun client. Ciò semplifica l'identificazione dei client che esauriscono le risorse di sistema e consente di imporre limiti di risorse per client.

## Visualizza le risorse dello storepool consumate

Il `vserver nfs storepool show` comando mostra il numero di risorse dello storepool utilizzate. Uno storepool è un pool di risorse utilizzate dai client NFSv4.

## Fase



1. In qualità di amministratore, eseguire `vserver nfs storepool show` Per visualizzare le informazioni sullo storepool dei client NFSv4.

**Esempio**

In questo esempio vengono visualizzate le informazioni sullo storepool dei client NFSv4.

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-IP: 10.0.1.1

Client-IP Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount
-----
10.0.2.1      nfs4.1      true      2 1 0 4
10.0.2.2      nfs4.2      true      2 1 0 4

2 entries were displayed.
```

**Attiva o disattiva i controlli dei limiti dello storepool**

Gli amministratori possono utilizzare i seguenti comandi per attivare o disattivare i controlli dei limiti dello storepool.

**Fase**

1. In qualità di amministratore, eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare i controlli dei limiti dello storepool	<code>vserver nfs storepool config modify -limit-enforce enabled</code>
Disattiva i controlli dei limiti di storepool	<code>vserver nfs storepool config modify -limit-enforce disabled</code>

**Visualizzare un elenco di client bloccati**

Se il limite di storepool è attivato, gli amministratori possono vedere quali client sono stati bloccati al raggiungimento della soglia di risorse per client. Gli amministratori possono utilizzare il seguente comando per vedere quali client sono stati contrassegnati come client bloccati.

**Fasi**

1. Utilizzare `vserver nfs storepool blocked-client show` Per visualizzare l'elenco dei client NFSv4 bloccati.

#### Rimuovere un client dall'elenco dei client bloccati

I client che raggiungono la soglia per client verranno disconnessi e aggiunti alla cache del client a blocchi. Gli amministratori possono utilizzare il seguente comando per rimuovere il client dalla cache del client a blocchi. In questo modo, il client potrà connettersi al server NFSV4 di ONTAP.

#### Fasi

1. Utilizzare `vserver nfs storepool blocked-client flush -client-ip <ip address>` comando per svuotare la cache del client bloccato nello storepool.
2. Utilizzare `vserver nfs storepool blocked-client show` comando per verificare che il client sia stato rimosso dalla cache del client a blocchi.

#### Esempio

In questo esempio viene visualizzato un client bloccato con l'indirizzo IP "10.2.1.1" che viene liberato da tutti i nodi.

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
-----
10.1.1.1

1 entries were displayed.
```

#### Abilitare o disabilitare pNFS

PNFS migliora le performance consentendo ai client NFS di eseguire operazioni di lettura/scrittura direttamente e in parallelo sui dispositivi di storage, ignorando il server NFS come potenziale collo di bottiglia. Per attivare o disattivare pNFS (Parallel NFS), è possibile modificare `-v4.1-pnfs` opzione.

Se la versione di ONTAP è...	Il valore predefinito di pNFS è...
9.8 o versione successiva	disattivato
9.7 o versioni precedenti	attivato

#### Di cosa hai bisogno

Il supporto di NFSv4.1 è necessario per poter utilizzare pNFS.

Se si desidera attivare pNFS, è necessario prima disattivare i riferimenti NFS. Non è possibile abilitare entrambi contemporaneamente.

Se si utilizza pNFS con Kerberos su SVM, è necessario attivare Kerberos su ogni LIF su SVM.

## Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Abilitare pNFS	<pre>vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled</pre>
Disattiva pNFS	<pre>vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled</pre>

## Informazioni correlate

- [Panoramica del trunking NFS](#)

## Controlla l'accesso NFS su TCP e UDP

È possibile attivare o disattivare l'accesso NFS alle macchine virtuali di storage (SVM) su TCP e UDP modificando il `-tcp` e `-udp` parametri, rispettivamente. In questo modo è possibile controllare se i client NFS possono accedere ai dati tramite TCP o UDP nel proprio ambiente.

## A proposito di questa attività

Questi parametri si applicano solo a NFS. Non influiscono sui protocolli ausiliari. Ad esempio, se NFS su TCP è disattivato, le operazioni di montaggio su TCP continuano a avere successo. Per bloccare completamente il traffico TCP o UDP, è possibile utilizzare le regole dei criteri di esportazione.



È necessario disattivare SnapDiff RPC Server prima di disattivare TCP per NFS per evitare un errore di comando non riuscito. È possibile disattivare il protocollo TCP utilizzando il comando `vserver snapdiff-rpc-server off -vserver vserver_name`.

## Fase

1. Eseguire una delle seguenti operazioni:

Se vuoi che l'accesso NFS sia...	Immettere il comando...
Abilitato su TCP	<pre>vserver nfs modify -vserver vserver_name -tcp enabled</pre>
Disattivato su TCP	<pre>vserver nfs modify -vserver vserver_name -tcp disabled</pre>
Abilitato su UDP	<pre>vserver nfs modify -vserver vserver_name -udp enabled</pre>
Disattivato su UDP	<pre>vserver nfs modify -vserver vserver_name -udp disabled</pre>

## Controllo delle richieste NFS da porte non riservate

È possibile rifiutare le richieste di montaggio NFS da porte non riservate attivando `-mount-rootonly` opzione. Per rifiutare tutte le richieste NFS da porte non riservate, è possibile attivare `-nfs-rootonly` opzione.

### A proposito di questa attività

Per impostazione predefinita, l'opzione `-mount-rootonly` è enabled.

Per impostazione predefinita, l'opzione `-nfs-rootonly` è disabled.

Queste opzioni non si applicano alla procedura NULL.

### Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Consenti richieste di montaggio NFS da porte non riservate	<code>vserver nfs modify -vserver vserver_name -mount -rootonly disabled</code>
Rifiutare le richieste di montaggio NFS da porte non riservate	<code>vserver nfs modify -vserver vserver_name -mount -rootonly enabled</code>
Consenti tutte le richieste NFS da porte non riservate	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly disabled</code>
Rifiutare tutte le richieste NFS da porte non riservate	<code>vserver nfs modify -vserver vserver_name -nfs -rootonly enabled</code>

## Gestire l'accesso NFS a volumi NTFS o qtree per utenti UNIX sconosciuti

Se ONTAP non riesce a identificare gli utenti UNIX che tentano di connettersi a volumi o qtree con lo stile di protezione NTFS, non può quindi mappare esplicitamente l'utente a un utente Windows. È possibile configurare ONTAP in modo che neghi l'accesso a tali utenti per una protezione più rigorosa oppure mapparli a un utente Windows predefinito per garantire un livello minimo di accesso a tutti gli utenti.

### Di cosa hai bisogno

Se si desidera attivare questa opzione, è necessario configurare un utente Windows predefinito.

### A proposito di questa attività

Se un utente UNIX tenta di accedere a volumi o qtree con uno stile di protezione NTFS, l'utente UNIX deve prima essere mappato a un utente Windows in modo che ONTAP possa valutare correttamente le autorizzazioni NTFS. Tuttavia, se ONTAP non riesce a cercare il nome dell'utente UNIX nelle origini del servizio nome informazioni utente configurate, non può eseguire il mapping esplicito dell'utente UNIX a un utente Windows specifico. È possibile decidere come gestire tali utenti UNIX sconosciuti nei seguenti modi:

- Negare l'accesso a utenti UNIX sconosciuti.

In questo modo viene garantita una sicurezza più rigorosa, richiedendo il mapping esplicito per tutti gli utenti UNIX per ottenere l'accesso ai volumi NTFS o ai qtree.

- Associare utenti UNIX sconosciuti a un utente Windows predefinito.

In questo modo si ottiene meno sicurezza, ma maggiore praticità, garantendo a tutti gli utenti un livello minimo di accesso ai volumi NTFS o ai qtree tramite un utente Windows predefinito.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera utilizzare l'utente Windows predefinito per utenti UNIX sconosciuti...	Immettere il comando...
Attivato	<code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled</code>
Disattivato	<code>vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled</code>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Considerazioni per i client che montano le esportazioni NFS utilizzando una porta non riservata

Il `-mount-rootonly` L'opzione deve essere disattivata su un sistema storage che deve supportare i client che montano le esportazioni NFS utilizzando una porta non riservata anche quando l'utente è connesso come root. Tali client includono i client Hummingbird e i client NFS/IPv6 di Solaris.

Se il `-mount-rootonly` ONTAP non consente ai client NFS che utilizzano porte non riservate, ovvero porte con numeri superiori a 1,023, di montare le esportazioni NFS.

## Eseguire un controllo degli accessi più rigoroso per i netgroup verificando i domini

Per impostazione predefinita, ONTAP esegue un'ulteriore verifica quando valuta l'accesso client per un netgroup. Il controllo aggiuntivo garantisce che il dominio del client corrisponda alla configurazione di dominio della macchina virtuale di storage (SVM). In caso contrario, ONTAP nega l'accesso al client.

## A proposito di questa attività

Quando ONTAP valuta le regole dei criteri di esportazione per l'accesso client e una regola dei criteri di esportazione contiene un netgroup, ONTAP deve determinare se l'indirizzo IP di un client appartiene al netgroup. A tale scopo, ONTAP converte l'indirizzo IP del client in un nome host utilizzando DNS e ottiene un nome di dominio completo (FQDN).

Se il file netgroup elenca solo un nome breve per l'host e il nome breve per l'host esiste in più domini, è possibile che un client di un dominio diverso ottenga l'accesso senza questo controllo.

Per evitare che ciò accada, ONTAP confronta il dominio restituito dal DNS per l'host con l'elenco dei nomi di dominio DNS configurati per la SVM. Se corrisponde, l'accesso è consentito. Se non corrisponde, l'accesso viene negato.

Questa verifica è attivata per impostazione predefinita. È possibile gestirlo modificando il `-netgroup-dns-domain-search` che è disponibile al livello di privilegio avanzato.

**Fasi**

- 1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- 2. Eseguire l'azione desiderata:

Se si desidera che la verifica del dominio per i netgroup sia...	Inserisci...
Attivato	<code>vserver nfs modify -vserver vserver_name -netgroup-dns-domain-search enabled</code>
Disattivato	<code>vserver nfs modify -vserver vserver_name -netgroup-dns-domain-search disabled</code>

- 3. Impostare il livello di privilegio su admin:

```
set -privilege admin
```

**Modificare le porte utilizzate per i servizi NFSv3**

Il server NFS sul sistema di storage utilizza servizi come mount daemon e Network Lock Manager per comunicare con i client NFS su porte di rete predefinite specifiche. Nella maggior parte degli ambienti NFS, le porte predefinite funzionano correttamente e non richiedono modifiche, ma se si desidera utilizzare diverse porte di rete NFS nell'ambiente NFSv3, è possibile farlo.

**Di cosa hai bisogno**

La modifica delle porte NFS sul sistema di storage richiede che tutti i client NFS si riconnettano al sistema, pertanto è necessario comunicare queste informazioni agli utenti prima di apportare la modifica.

**A proposito di questa attività**

È possibile impostare le porte utilizzate dai servizi NFS mount daemon, Network Lock Manager, Network

Status Monitor e NFS quota daemon per ciascuna macchina virtuale di storage (SVM). La modifica del numero di porta influisce sull'accesso dei client NFS ai dati sia su TCP che su UDP.

Le porte per NFSv4 e NFSv4.1 non possono essere modificate.

**Fasi**

- 1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- 2. Disattivare l'accesso a NFS:

```
vserver nfs modify -vserver vserver_name -access false
```

- 3. Impostare la porta NFS per il servizio NFS specifico:

```
vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
```

Parametro della porta NFS	Descrizione	Porta predefinita
-mountd-port	Daemon di montaggio NFS	635
-nlm-port	Network Lock Manager	4045
-nsm-port	Network Status Monitor (Monitor di stato della rete)	4046
-rquotad-port	Daemon quota NFS	4049

Oltre alla porta predefinita, l'intervallo consentito di numeri di porta è compreso tra 1024 e 65535. Ogni servizio NFS deve utilizzare una porta univoca.

- 4. Abilitare l'accesso a NFS:

```
vserver nfs modify -vserver vserver_name -access true
```

- 5. Utilizzare `network connections listening show` per verificare che il numero di porta cambi.

- 6. Tornare al livello di privilegio admin:

```
set -privilege admin
```

**Esempio**

I seguenti comandi impostano la porta NFS Mount Daemon su 1113 sulla SVM denominata vs1:

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name      Interface Name:Local Port      Protocol/Service
-----
Node: cluster1-01
Cluster           cluster1-01_clus_1:7700        TCP/ctlopccp
vs1               data1:4046                    TCP/sm
vs1               data1:4046                    UDP/sm
vs1               data1:4045                    TCP/nlm-v4
vs1               data1:4045                    UDP/nlm-v4
vs1               data1:1113                    TCP/mount
vs1               data1:1113                    UDP/mount
...
vs1::*> set -privilege admin


```

## Comandi per la gestione dei server NFS

Esistono comandi ONTAP specifici per la gestione dei server NFS.

Se si desidera...	Utilizzare questo comando...
Creare un server NFS	<code>vserver nfs create</code>
Visualizzare i server NFS	<code>vserver nfs show</code>
Modificare un server NFS	<code>vserver nfs modify</code>
Eliminare un server NFS	<code>vserver nfs delete</code>



<p>Nascondere <code>.snapshot</code> Elenco di directory sotto i punti di montaggio NFSv3</p> <div>  <p>Accesso esplicito a <code>.snapshot</code> la directory sarà comunque consentita anche se l'opzione è attivata.</p> </div>	<p><code>vserver nfs</code> comandi con <code>-v3-hide-snapshot</code> opzione attivata</p>
---	---

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Risolvere i problemi di name service

Quando i client riscontrano errori di accesso dovuti a problemi di name service, è possibile utilizzare `vserver services name-service getxxbyyy` famiglia di comandi per eseguire manualmente varie ricerche dei name service ed esaminare i dettagli e i risultati della ricerca per agevolare la risoluzione dei problemi.

### A proposito di questa attività

- Per ciascun comando, è possibile specificare quanto segue:
  - Nome del nodo o della SVM (Storage Virtual Machine) su cui eseguire la ricerca.

In questo modo è possibile verificare le ricerche name service per un nodo o una SVM specifico per limitare la ricerca di un potenziale problema di configurazione del name service.

- Se visualizzare l'origine utilizzata per la ricerca.

In questo modo è possibile verificare se è stata utilizzata la sorgente corretta.

- ONTAP seleziona il servizio per l'esecuzione della ricerca in base all'ordine di switch name service configurato.
- Questi comandi sono disponibili a livello di privilegio avanzato.

### Fasi

1. Eseguire una delle seguenti operazioni:

Per recuperare...	Utilizzare il comando...
Indirizzo IP di un nome host	<code>vserver services name-service getxxbyyy getaddrinfo vserver services name-service getxxbyyy gethostbyname</code> (Solo indirizzi IPv4)
Membri di un gruppo per ID gruppo	<code>vserver services name-service getxxbyyy getgrbygid</code>

Membri di un gruppo in base al nome del gruppo	<code>vserver services name-service getxxbyyy getgrbyname</code>
Elenco dei gruppi a cui appartiene un utente	<code>vserver services name-service getxxbyyy getgrlist</code>
Nome host di un indirizzo IP	<code>vserver services name-service getxxbyyy getnameinfo</code> <code>vserver services name-service getxxbyyy gethostbyaddr</code> (Solo indirizzi IPv4)
Informazioni utente per nome utente	<code>vserver services name-service getxxbyyy getpwbyname</code> È possibile verificare la risoluzione dei nomi degli utenti RBAC specificando <code>-use-rbac</code> parametro <code>as true</code> .
Informazioni utente per ID utente	<code>vserver services name-service getxxbyyy getpwbyuid</code> È possibile verificare la risoluzione dei nomi degli utenti RBAC specificando <code>-use-rbac</code> parametro <code>as true</code> .
Appartenenza a netgroup di un client	<code>vserver services name-service getxxbyyy netgrp</code>
Appartenenza a netgroup di un client mediante la ricerca netgroup-by-host	<code>vserver services name-service getxxbyyy netgrpbyhost</code>

L'esempio seguente mostra un test di ricerca DNS per SVM vs1 tentando di ottenere l'indirizzo IP per l'host `acast1.eng.example.com`:

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

L'esempio seguente mostra un test di ricerca NIS per SVM vs1 tentando di recuperare le informazioni utente per un utente con UID 501768:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvC2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

L'esempio seguente mostra un test di ricerca LDAP per SVM vs1 tentando di recuperare le informazioni utente per un utente con il nome ldap1:

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

L'esempio seguente mostra un test di ricerca di netgroup per SVM vs1 cercando di scoprire se il client dnshost0 è un membro del netgroup lnetgroup136:

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. Analizzare i risultati del test eseguito e intraprendere le azioni necessarie.

Se...	Controllare...
La ricerca del nome host o dell'indirizzo IP non è riuscita o ha dato risultati errati	Configurazione DNS
La ricerca ha richiesto un'origine errata	Configurazione dello switch name service

Se...	Controllare...
La ricerca di utenti o gruppi non è riuscita o ha prodotto risultati errati	<ul style="list-style-type: none"> <li>• Configurazione dello switch name service</li> <li>• Configurazione di origine (file locali, dominio NIS, client LDAP)</li> <li>• Configurazione di rete (ad esempio, LIF e route)</li> </ul>
Ricerca nome host non riuscita o scaduta e il server DNS non risolve i nomi brevi DNS (ad esempio, host1)	Configurazione DNS per query TLD (Top-Level Domain). È possibile disattivare le query TLD utilizzando <code>-is-tld-query-enabled false</code> al <code>vserver services name-service dns modify</code> comando.

### Informazioni correlate

["Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"](#)

### Verificare le connessioni name service

A partire da ONTAP 9.2, è possibile controllare i server dei nomi DNS e LDAP per verificare che siano connessi a ONTAP. Questi comandi sono disponibili a livello di privilegi di amministratore.

#### A proposito di questa attività

È possibile verificare la presenza di una configurazione DNS o LDAP name service valida in base alle necessità utilizzando il controllo della configurazione del name service. Questo controllo di convalida può essere avviato dalla riga di comando o in System Manager.

Per le configurazioni DNS, tutti i server sono testati e devono funzionare perché la configurazione sia considerata valida. Per le configurazioni LDAP, se un server è attivo, la configurazione è valida. I comandi name service applicano il controllo della configurazione, a meno che non lo sia `skip-config-validation` il campo è `true` (il valore predefinito è `false`).

### Fase

1. Utilizzare il comando appropriato per controllare la configurazione di un name service. L'interfaccia utente visualizza lo stato dei server configurati.

Per verificare...	Utilizzare questo comando...
Stato della configurazione DNS	<code>vserver services name-service dns check</code>
Stato della configurazione LDAP	<code>vserver services name-service ldap check</code>

```
cluster1::> vserver services name-service dns check -vserver vs0
```

Vserver	Name Server	Status	Status Details
vs0	10.11.12.13	up	Response time (msec): 55
vs0	10.11.12.14	up	Response time (msec): 70
vs0	10.11.12.15	down	Connection refused.

```
cluster1::> vserver services name-service ldap check -vserver vs0
```

```
| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
"10.11.12.13". |
```

La convalida della configurazione ha esito positivo se almeno uno dei server configurati (name-server/ldap-server) è raggiungibile e fornisce il servizio. Se alcuni server non sono raggiungibili, viene visualizzato un avviso.

## Comandi per la gestione delle voci di switch name service

È possibile gestire le voci di name service switch creandole, visualizzandole, modificandole ed eliminandole.

Se si desidera...	Utilizzare questo comando...
Creare una voce name service switch	<code>vserver services name-service ns-switch create</code>
Nome visualizzato voci switch servizio	<code>vserver services name-service ns-switch show</code>
Modificare una voce di name service switch	<code>vserver services name-service ns-switch modify</code>
Consente di eliminare una voce di switch name service	<code>vserver services name-service ns-switch delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Informazioni correlate

["Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"](#)

## Comandi per la gestione della cache del name service

È possibile gestire la cache del name service modificando il valore TTL (Time To Live). Il valore TTL determina per quanto tempo le informazioni del servizio dei nomi sono persistenti nella cache.

Se si desidera modificare il valore TTL per...	Utilizzare questo comando...
Utenti UNIX	<code>vserver services name-service cache unix-user settings</code>
Gruppi UNIX	<code>vserver services name-service cache unix-group settings</code>
Netgroup UNIX	<code>vserver services name-service cache netgroups settings</code>
Host	<code>vserver services name-service cache hosts settings</code>
Appartenenza al gruppo	<code>vserver services name-service cache group-membership settings</code>

### Informazioni correlate

["Comandi di ONTAP 9"](#)

## Comandi per la gestione delle mappature dei nomi

Esistono comandi ONTAP specifici per la gestione delle mappature dei nomi.

Se si desidera...	Utilizzare questo comando...
Creare una mappatura dei nomi	<code>vserver name-mapping create</code>
Inserire una mappatura dei nomi in una posizione specifica	<code>vserver name-mapping insert</code>
Visualizza mappature dei nomi	<code>vserver name-mapping show</code>
Scambiare la posizione di due mappature dei nomi NOTA: Non è consentito eseguire uno swap quando la mappatura dei nomi è configurata con una voce di qualificatore ip.	<code>vserver name-mapping swap</code>
Modificare una mappatura dei nomi	<code>vserver name-mapping modify</code>

Eliminare una mappatura dei nomi	<code>vserver name-mapping delete</code>
Convalidare la corretta mappatura dei nomi	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione degli utenti UNIX locali

Esistono comandi ONTAP specifici per la gestione degli utenti UNIX locali.

Se si desidera...	Utilizzare questo comando...
Creare un utente UNIX locale	<code>vserver services name-service unix-user create</code>
Caricare utenti UNIX locali da un URI	<code>vserver services name-service unix-user load-from-uri</code>
Visualizzare gli utenti UNIX locali	<code>vserver services name-service unix-user show</code>
Modificare un utente UNIX locale	<code>vserver services name-service unix-user modify</code>
Eliminare un utente UNIX locale	<code>vserver services name-service unix-user delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione di gruppi UNIX locali

Esistono comandi ONTAP specifici per la gestione dei gruppi UNIX locali.

Se si desidera...	Utilizzare questo comando...
Creare un gruppo UNIX locale	<code>vserver services name-service unix-group create</code>
Aggiungere un utente a un gruppo UNIX locale	<code>vserver services name-service unix-group adduser</code>
Caricare i gruppi UNIX locali da un URI	<code>vserver services name-service unix-group load-from-uri</code>
Visualizzare i gruppi UNIX locali	<code>vserver services name-service unix-group show</code>
Modificare un gruppo UNIX locale	<code>vserver services name-service unix-group modify</code>

Eliminare un utente da un gruppo UNIX locale	<code>vserver services name-service unix-group deluser</code>
Eliminare un gruppo UNIX locale	<code>vserver services name-service unix-group delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Limiti per utenti UNIX locali, gruppi e membri del gruppo

ONTAP ha introdotto limiti per il numero massimo di utenti e gruppi UNIX nel cluster e comandi per gestire questi limiti. Questi limiti possono aiutare a evitare problemi di performance impedendo agli amministratori di creare troppi utenti e gruppi UNIX locali nel cluster.

Esiste un limite per il numero combinato di gruppi di utenti UNIX locali e di membri del gruppo. Esiste un limite separato per gli utenti UNIX locali. I limiti sono a livello di cluster. Ciascuno di questi nuovi limiti viene impostato su un valore predefinito che è possibile modificare fino a un limite massimo preassegnato.

Database	Limite predefinito	Limite massimo
Utenti UNIX locali	32,768	65,536
Gruppi UNIX locali e membri del gruppo	32,768	65,536

### Gestire i limiti per utenti e gruppi UNIX locali

Esistono comandi ONTAP specifici per la gestione dei limiti per utenti e gruppi UNIX locali. Gli amministratori dei cluster possono utilizzare questi comandi per risolvere i problemi di performance nel cluster che si ritiene siano correlati a un numero eccessivo di utenti e gruppi UNIX locali.

#### A proposito di questa attività

Questi comandi sono disponibili per l'amministratore del cluster a livello di privilegi avanzati.

#### Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Utilizzare il comando...
Visualizza informazioni sui limiti utente UNIX locali	<code>vserver services unix-user max-limit show</code>
Visualizza informazioni sui limiti dei gruppi UNIX locali	<code>vserver services unix-group max-limit show</code>



Se si desidera...	Utilizzare il comando...
Modificare i limiti utente UNIX locali	<code>vserver services unix-user max-limit modify</code>
Modificare i limiti dei gruppi UNIX locali	<code>vserver services unix-group max-limit modify</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione dei netgroup locali

È possibile gestire i netgroup locali caricandoli da un URI, verificandone lo stato tra i nodi, visualizzandoli ed eliminandoli.

Se si desidera...	Utilizzare il comando...
Caricare i netgroup da un URI	<code>vserver services name-service netgroup load</code>
Verificare lo stato dei netgroup nei nodi	<code>vserver services name-service netgroup status</code> Disponibile a un livello di privilegio avanzato e superiore.
Visualizzare i netgroup locali	<code>vserver services name-service netgroup file show</code>
Eliminare un netgroup locale	<code>vserver services name-service netgroup file delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione delle configurazioni di dominio NIS

Esistono comandi ONTAP specifici per la gestione delle configurazioni di dominio NIS.

Se si desidera...	Utilizzare questo comando...
Creare una configurazione di dominio NIS	<code>vserver services name-service nis-domain create</code>
Visualizzare le configurazioni di dominio NIS	<code>vserver services name-service nis-domain show</code>
Visualizza lo stato di binding di una configurazione di dominio NIS	<code>vserver services name-service nis-domain show-bound</code>
Visualizzare le statistiche NIS	<code>vserver services name-service nis-domain show-statistics</code> Disponibile a un livello di privilegio avanzato e superiore.

Cancellare le statistiche NIS	<code>vserver services name-service nis-domain clear-statistics</code> Disponibile a un livello di privilegio avanzato e superiore.
Modificare una configurazione di dominio NIS	<code>vserver services name-service nis-domain modify</code>
Eliminare una configurazione di dominio NIS	<code>vserver services name-service nis-domain delete</code>
Abilitare il caching per le ricerche netgroup-by-host	<code>vserver services name-service nis-domain netgroup-database config modify</code> Disponibile a un livello di privilegio avanzato e superiore.

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione delle configurazioni del client LDAP

Esistono comandi ONTAP specifici per la gestione delle configurazioni del client LDAP.



Gli amministratori SVM non possono modificare o eliminare le configurazioni client LDAP create dagli amministratori del cluster.

Se si desidera...	Utilizzare questo comando...
Creare una configurazione del client LDAP	<code>vserver services name-service ldap client create</code>
Visualizzare le configurazioni del client LDAP	<code>vserver services name-service ldap client show</code>
Modificare una configurazione del client LDAP	<code>vserver services name-service ldap client modify</code>
Modificare la password BIND del client LDAP	<code>vserver services name-service ldap client modify-bind-password</code>
Eliminare una configurazione del client LDAP	<code>vserver services name-service ldap client delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione delle configurazioni LDAP

Esistono comandi ONTAP specifici per la gestione delle configurazioni LDAP.

Se si desidera...	Utilizzare questo comando...
-------------------	------------------------------

Creare una configurazione LDAP	<code>vserver services name-service ldap create</code>
Visualizzare le configurazioni LDAP	<code>vserver services name-service ldap show</code>
Modificare una configurazione LDAP	<code>vserver services name-service ldap modify</code>
Eliminare una configurazione LDAP	<code>vserver services name-service ldap delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione dei modelli di schema del client LDAP

Esistono comandi ONTAP specifici per la gestione dei modelli di schema del client LDAP.



Gli amministratori di SVM non possono modificare o eliminare gli schemi client LDAP creati dagli amministratori del cluster.

Se si desidera...	Utilizzare questo comando...
Copiare un modello di schema LDAP esistente	<code>vserver services name-service ldap client schema copy</code> Disponibile a un livello di privilegio avanzato e superiore.
Visualizzare i modelli di schema LDAP	<code>vserver services name-service ldap client schema show</code>
Modificare un modello di schema LDAP	<code>vserver services name-service ldap client schema modify</code> Disponibile a un livello di privilegio avanzato e superiore.
Eliminare un modello di schema LDAP	<code>vserver services name-service ldap client schema delete</code> Disponibile a un livello di privilegio avanzato e superiore.

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione delle configurazioni dell'interfaccia Kerberos NFS

Esistono comandi ONTAP specifici per la gestione delle configurazioni dell'interfaccia Kerberos NFS.

Se si desidera...	Utilizzare questo comando...
Abilitare NFS Kerberos su una LIF	<code>vserver nfs kerberos interface enable</code>
Visualizzare le configurazioni dell'interfaccia Kerberos NFS	<code>vserver nfs kerberos interface show</code>

Modificare una configurazione dell'interfaccia Kerberos NFS	<code>vserver nfs kerberos interface modify</code>
Disattiva NFS Kerberos su LIF	<code>vserver nfs kerberos interface disable</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione delle configurazioni del realm Kerberos NFS

Esistono comandi ONTAP specifici per la gestione delle configurazioni di autenticazione Kerberos NFS.

Se si desidera...	Utilizzare questo comando...
Creare una configurazione di autenticazione Kerberos NFS	<code>vserver nfs kerberos realm create</code>
Visualizzare le configurazioni del realm Kerberos NFS	<code>vserver nfs kerberos realm show</code>
Modificare la configurazione di un realm Kerberos NFS	<code>vserver nfs kerberos realm modify</code>
Eliminare una configurazione di autenticazione Kerberos NFS	<code>vserver nfs kerberos realm delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Comandi per la gestione delle policy di esportazione

Esistono comandi ONTAP specifici per la gestione delle policy di esportazione.

Se si desidera...	Utilizzare questo comando...
Visualizza informazioni sui criteri di esportazione	<code>vserver export-policy show</code>
Rinominare un criterio di esportazione	<code>vserver export-policy rename</code>
Copiare una policy di esportazione	<code>vserver export-policy copy</code>
Eliminare una policy di esportazione	<code>vserver export-policy delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Comandi per la gestione delle regole di esportazione

Esistono comandi ONTAP specifici per la gestione delle regole di esportazione.

Se si desidera...	Utilizzare questo comando...
Creare una regola di esportazione	<code>vserver export-policy rule create</code>
Visualizza le informazioni sulle regole di esportazione	<code>vserver export-policy rule show</code>
Modificare una regola di esportazione	<code>vserver export-policy rule modify</code>
Eliminare una regola di esportazione	<code>vserver export-policy rule delete</code>



Se sono state configurate più regole di esportazione identiche corrispondenti a client diversi, assicurarsi di mantenerle sincronizzate durante la gestione delle regole di esportazione.

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Configurare la cache delle credenziali NFS

### Motivi per modificare il time-to-live della cache delle credenziali NFS

ONTAP utilizza una cache delle credenziali per memorizzare le informazioni necessarie per l'autenticazione dell'utente per l'accesso all'esportazione NFS, in modo da fornire un accesso più rapido e migliorare le performance. È possibile configurare per quanto tempo le informazioni vengono memorizzate nella cache delle credenziali per personalizzarle in base all'ambiente in uso.

La modifica del TTL (Time-to-live) della cache delle credenziali NFS può aiutare a risolvere i problemi in diversi scenari. È necessario comprendere quali sono questi scenari e le conseguenze di tali modifiche.

### Motivi

Modificare il TTL predefinito nei seguenti casi:

Problema	Azione correttiva
I name server nel tuo ambiente stanno riscontrando un peggioramento delle performance dovuto a un elevato carico di richieste da parte di ONTAP.	Aumentare il TTL per le credenziali positive e negative memorizzate nella cache per ridurre il numero di richieste da ONTAP ai server dei nomi.
L'amministratore del name server ha apportato delle modifiche per consentire l'accesso agli utenti NFS precedentemente rifiutati.	Ridurre il TTL per le credenziali negative memorizzate nella cache per ridurre il tempo di attesa che gli utenti NFS debbano attendere che ONTAP richieda nuove credenziali ai server dei nomi esterni in modo che possano accedervi.

Problema	Azione correttiva
L'amministratore del name server ha apportato delle modifiche per negare l'accesso agli utenti NFS precedentemente autorizzati.	Riduci il TTL per le credenziali positive memorizzate nella cache per ridurre il tempo prima che ONTAP richieda nuove credenziali ai server dei nomi esterni, in modo che gli utenti NFS non possano accedere.

## Conseguenze

È possibile modificare la durata del tempo singolarmente per il caching delle credenziali positive e negative. Tuttavia, è necessario essere consapevoli dei vantaggi e degli svantaggi di tale operazione.

Se...	Il vantaggio è...	Lo svantaggio è...
Aumentare il tempo di cache delle credenziali positive	ONTAP invia le richieste di credenziali ai server dei nomi con minore frequenza, riducendo il carico sui server dei nomi.	Ci vuole più tempo per negare l'accesso agli utenti NFS a cui in precedenza era consentito l'accesso ma che non sono più disponibili.
Ridurre il tempo di cache delle credenziali positive	È necessario meno tempo per negare l'accesso agli utenti NFS a cui in precedenza era consentito l'accesso ma che non sono più disponibili.	ONTAP invia più frequentemente richieste di credenziali ai server dei nomi, aumentando il carico sui server dei nomi.
Aumentare il tempo di cache delle credenziali negative	ONTAP invia le richieste di credenziali ai server dei nomi con minore frequenza, riducendo il carico sui server dei nomi.	Occorre più tempo per concedere l'accesso agli utenti NFS che in precedenza non avevano accesso, ma che ora lo sono.
Ridurre il tempo di cache delle credenziali negative	Occorrono meno tempo per concedere l'accesso agli utenti NFS che in precedenza non avevano accesso, ma che ora lo sono.	ONTAP invia più frequentemente richieste di credenziali ai server dei nomi, aumentando il carico sui server dei nomi.

## Configurare il time-to-live per le credenziali utente NFS memorizzate nella cache

È possibile configurare il periodo di tempo in cui ONTAP memorizza le credenziali degli utenti NFS nella cache interna (time-to-live o TTL) modificando il server NFS della macchina virtuale di storage (SVM). In questo modo è possibile ridurre alcuni problemi legati all'elevato carico sui server dei nomi o alle modifiche delle credenziali che influiscono sull'accesso degli utenti NFS.

### A proposito di questa attività

Questi parametri sono disponibili a livello di privilegio avanzato.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

## 2. Eseguire l'azione desiderata:

Se si desidera modificare il TTL per la cache...	Utilizzare il comando...
Credenziali positive	<pre>vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live</pre> <p>Il TTL viene misurato in millisecondi. A partire da ONTAP 9.10.1 e versioni successive, il valore predefinito è 1 ora (3.600.000 millisecondi). In ONTAP 9.9.1 e versioni precedenti, il valore predefinito è 24 ore (86.400.000 millisecondi). L'intervallo consentito per questo valore è compreso tra 1 minuto (60000 millisecondi) e 7 giorni (604,800,000 millisecondi).</p>
Credenziali negative	<pre>vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live</pre> <p>Il TTL viene misurato in millisecondi. L'impostazione predefinita è 2 ore (7,200,000 millisecondi). L'intervallo consentito per questo valore è compreso tra 1 minuto (60000 millisecondi) e 7 giorni (604,800,000 millisecondi).</p>

## 3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Gestire le cache delle policy di esportazione

### Svuotare le cache delle policy di esportazione

ONTAP utilizza diverse cache delle policy di esportazione per memorizzare le informazioni relative alle policy di esportazione per un accesso più rapido. L'operazione di cancellazione della policy di esportazione viene eseguita manualmente nella cache (`vserver export-policy cache flush`) Rimuove le informazioni potenzialmente obsolete e costringe ONTAP a recuperare le informazioni correnti dalle risorse esterne appropriate. Questo può aiutare a risolvere una serie di problemi relativi all'accesso client alle esportazioni NFS.

### A proposito di questa attività

Le informazioni della cache delle policy di esportazione potrebbero essere obsolete a causa dei seguenti motivi:

- Una recente modifica alle regole dei criteri di esportazione
- Una recente modifica ai record dei nomi host nei server dei nomi
- Una recente modifica alle voci di netgroup nei server dei nomi
- Ripristino da un'interruzione di rete che ha impedito il caricamento completo dei netgroup

## Fasi

1. Se la cache del servizio nomi non è attivata, eseguire una delle seguenti operazioni in modalità privilegio avanzato:

Se si desidera eseguire il lavaggio...	Immettere il comando...
Tutte le cache delle policy di esportazione (ad eccezione di showmount)	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name</code>
La policy di esportazione regola l'accesso alla cache	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache access</code> È possibile includere il opzionale <code>-node</code> parametro per specificare il nodo su cui si desidera svuotare la cache di accesso.
La cache dei nomi host	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache host</code>
La cache del netgroup	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache netgroup</code> L'elaborazione dei netgroup richiede un uso intensivo delle risorse. È necessario svuotare la cache del netgroup solo se si tenta di risolvere un problema di accesso client causato da un netgroup obsoleto.
La cache di showmount	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache showmount</code>

2. Se la cache del name service è attivata, eseguire una delle seguenti operazioni:

Se si desidera eseguire il lavaggio...	Immettere il comando...
La policy di esportazione regola l'accesso alla cache	<code>vserver export-policy cache flush</code> <code>-vserver vserver_name -cache access</code> È possibile includere il opzionale <code>-node</code> parametro per specificare il nodo su cui si desidera svuotare la cache di accesso.
La cache dei nomi host	<code>vserver services name-service cache</code> <code>hosts forward-lookup delete-all</code>



Se si desidera eseguire il lavaggio...	Immettere il comando...
La cache del netgroup	<pre>vserver services name-service cache netgroups ip-to-netgroup delete-all vserver services name-service cache netgroups members delete-all</pre> <p>L'elaborazione dei netgroup richiede un uso intensivo delle risorse. È necessario svuotare la cache del netgroup solo se si tenta di risolvere un problema di accesso client causato da un netgroup obsoleto.</p>
La cache di showmount	<pre>vserver export-policy cache flush -vserver vserver_name -cache showmount</pre>

#### Visualizza la coda e la cache del netgroup dei criteri di esportazione

ONTAP utilizza la coda netgroup per importare e risolvere i netgroup e la cache netgroup per memorizzare le informazioni risultanti. Durante la risoluzione dei problemi relativi ai netgroup di policy di esportazione, è possibile utilizzare `vserver export-policy netgroup queue show` e `vserver export-policy netgroup cache show` comandi per visualizzare lo stato della coda netgroup e il contenuto della cache netgroup.

#### Fase

1. Eseguire una delle seguenti operazioni:

Per visualizzare il netgroup dei criteri di esportazione...	Immettere il comando...
Coda	<code>vserver export-policy netgroup queue show</code>
Cache	<code>vserver export-policy netgroup cache show -vserver vserver_name</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

#### Verificare se un indirizzo IP del client è membro di un netgroup

Durante la risoluzione dei problemi di accesso al client NFS relativi ai netgroup, è possibile utilizzare `vserver export-policy netgroup check-membership` Per determinare se un IP client è membro di un determinato netgroup.

#### A proposito di questa attività

La verifica dell'appartenenza a netgroup consente di determinare se ONTAP è consapevole che un client è o meno membro di un netgroup. Consente inoltre di sapere se la cache del netgroup ONTAP si trova in uno stato transitorio durante l'aggiornamento delle informazioni del netgroup. Queste informazioni possono aiutarti a capire perché a un client potrebbe essere concesso o negato l'accesso in modo imprevisto.

## Fase

1. Verificare l'appartenenza al netgroup di un indirizzo IP client: `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

Il comando può restituire i seguenti risultati:

- Il client è membro del netgroup.

Ciò è stato confermato mediante una ricerca inversa o una ricerca netgroup-by-host.

- Il client è membro del netgroup.

È stato trovato nella cache del netgroup di ONTAP.

- Il client non è membro del netgroup.

- L'appartenenza del client non può ancora essere determinata perché ONTAP sta aggiornando la cache del netgroup.

Fino a quando ciò non viene fatto, l'appartenenza non può essere esplicitamente esclusa o esclusa. Utilizzare `vserver export-policy netgroup queue show` comando per monitorare il caricamento del netgroup e riprovare il controllo al termine.

## Esempio

Nell'esempio seguente viene verificato se un client con l'indirizzo IP 172.17.16.72 è membro del netgroup Mercury su SVM vs1:

```
cluster1::> vserver export-policy netgroup check-membership -vserver vs1  
-netgroup mercury -client-ip 172.17.16.72
```

## Ottimizza le performance della cache di accesso

È possibile configurare diversi parametri per ottimizzare la cache di accesso e trovare il giusto equilibrio tra le prestazioni e la corrente delle informazioni memorizzate nella cache di accesso.

### A proposito di questa attività

Quando si configurano i periodi di aggiornamento della cache di accesso, tenere presente quanto segue:

- Valori più elevati significano che le voci rimangono più lunghe nella cache di accesso.

Il vantaggio è rappresentato dalle performance migliori, in quanto ONTAP spende meno risorse per il refresh delle voci della cache di accesso. Lo svantaggio è che se le regole dei criteri di esportazione cambiano e le voci della cache di accesso diventano obsolete, l'aggiornamento richiede più tempo. Di conseguenza, i client che dovrebbero ottenere l'accesso potrebbero essere rifiutati e i client che dovrebbero ottenere l'accesso potrebbero ottenere l'accesso.

- Valori più bassi significano che ONTAP aggiorna più spesso le voci della cache di accesso.

Il vantaggio è che le voci sono più aggiornate e i client hanno maggiori probabilità di ottenere o negare l'accesso correttamente. Lo svantaggio è una diminuzione delle performance perché ONTAP spende più

risorse per aggiornare le voci della cache di accesso.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire l'azione desiderata:

Per modificare...	Inserisci...
Periodo di refresh per voci positive	<pre>vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value</pre>
Periodo di refresh per le voci negative	<pre>vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value</pre>
Periodo di timeout per le voci precedenti	<pre>vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value</pre>

3. Verificare le nuove impostazioni dei parametri:

```
vserver export-policy access-cache config show-all-vservers
```

4. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Gestire i blocchi dei file

### Informazioni sul blocco dei file tra protocolli

Il blocco dei file è un metodo utilizzato dalle applicazioni client per impedire a un utente di accedere a un file precedentemente aperto da un altro utente. Il modo in cui ONTAP blocca i file dipende dal protocollo del client.

Se il client è un client NFS, i blocchi sono avvisi; se il client è un client SMB, i blocchi sono obbligatori.

A causa delle differenze tra i blocchi di file NFS e SMB, un client NFS potrebbe non riuscire ad accedere a un file precedentemente aperto da un'applicazione SMB.

Quando un client NFS tenta di accedere a un file bloccato da un'applicazione SMB, si verifica quanto segue:

- In volumi misti o NTFS, operazioni di manipolazione dei file come `rm`, `rmdir`, e. `mv` Può causare il malfunzionamento dell'applicazione NFS.
- Le operazioni di lettura e scrittura NFS sono negate rispettivamente dalle modalità aperta di negazione-lettura e di negazione-scrittura di SMB.

- Le operazioni di scrittura NFS non riescono quando l'intervallo scritto del file è bloccato con un esclusivo bytelock SMB.

Nei volumi UNIX di sicurezza, le operazioni di sconnessione e ridenominazione NFS ignorano lo stato di blocco SMB e consentono l'accesso al file. Tutte le altre operazioni NFS sui volumi UNIX di sicurezza rispettano lo stato di blocco SMB.

#### Come ONTAP tratta i bit di sola lettura

Il bit di sola lettura viene impostato file per file per indicare se un file è scrivibile (disattivato) o di sola lettura (abilitato).

I client SMB che utilizzano Windows possono impostare un bit di sola lettura per ogni file. I client NFS non impostano un bit di sola lettura per ogni file perché i client NFS non eseguono operazioni di protocollo che utilizzano un bit di sola lettura per ogni file.

ONTAP può impostare un bit di sola lettura su un file quando un client SMB che utilizza Windows crea tale file. ONTAP può anche impostare un bit di sola lettura quando un file viene condiviso tra client NFS e client SMB. Alcuni software, se utilizzati dai client NFS e dai client SMB, richiedono l'abilitazione del bit di sola lettura.

Affinché ONTAP mantenga le autorizzazioni di lettura e scrittura appropriate su un file condiviso tra client NFS e client SMB, tratta il bit di sola lettura in base alle seguenti regole:

- NFS considera qualsiasi file con il bit di sola lettura abilitato come se non abbia alcun bit di permesso di scrittura abilitato.
- Se un client NFS disattiva tutti i bit di permesso di scrittura e almeno uno di questi bit era stato precedentemente attivato, ONTAP attiva il bit di sola lettura per quel file.
- Se un client NFS attiva qualsiasi bit di autorizzazione di scrittura, ONTAP disattiva il bit di sola lettura per quel file.
- Se il bit di sola lettura per un file è attivato e un client NFS tenta di rilevare le autorizzazioni per il file, i bit di autorizzazione per il file non vengono inviati al client NFS; invece, ONTAP invia i bit di autorizzazione al client NFS con i bit di autorizzazione di scrittura mascherati.
- Se il bit di sola lettura per un file è attivato e un client SMB disattiva il bit di sola lettura, ONTAP attiva il bit di autorizzazione di scrittura del proprietario per il file.
- I file con il bit di sola lettura abilitato sono scrivibili solo da root.



Le modifiche alle autorizzazioni dei file hanno effetto immediato sui client SMB, ma potrebbero non avere effetto immediato sui client NFS se il client NFS attiva il caching degli attributi.

#### In che modo ONTAP si differenzia da Windows per la gestione dei blocchi sui componenti del percorso di condivisione

A differenza di Windows, ONTAP non blocca ogni componente del percorso di un file aperto mentre il file è aperto. Questo comportamento influisce anche sui percorsi di condivisione SMB.

Poiché ONTAP non blocca ogni componente del percorso, è possibile rinominare un componente del percorso sopra il file aperto o la condivisione, che può causare problemi per alcune applicazioni o causare l'invalidità del percorso di condivisione nella configurazione SMB. Questo può rendere la condivisione inaccessibile.

Per evitare problemi causati dalla ridenominazione dei componenti del percorso, è possibile applicare le impostazioni di protezione dell'elenco di controllo di accesso Windows (ACL) che impediscono agli utenti o alle

applicazioni di rinominare le directory critiche.

Scopri di più ["Come impedire che le directory vengano rinominate mentre i client le accedono"](#).

### Visualizza informazioni sui blocchi

È possibile visualizzare informazioni sui blocchi di file correnti, inclusi i tipi di blocchi che vengono conservati e lo stato di blocco, i dettagli sui blocchi dell'intervallo di byte, le modalità sharelock, i blocchi di delega e i blocchi opportunistici e se i blocchi vengono aperti con handle durevoli o persistenti.

### A proposito di questa attività

L'indirizzo IP del client non può essere visualizzato per i blocchi stabiliti tramite NFSv4 o NFSv4.1.

Per impostazione predefinita, il comando visualizza le informazioni relative a tutti i blocchi. È possibile utilizzare i parametri dei comandi per visualizzare informazioni sui blocchi di una specifica macchina virtuale di storage (SVM) o per filtrare l'output del comando in base ad altri criteri.

Il `vserver locks show` il comando visualizza informazioni su quattro tipi di blocchi:

- Blocchi byte-range, che bloccano solo una parte di un file.
- Blocchi di condivisione che bloccano i file aperti.
- Blocchi opportunistici, che controllano il caching lato client su SMB.
- Deleghe, che controllano il caching lato client su NFSv4.x.

Specificando i parametri opzionali, è possibile determinare informazioni importanti su ciascun tipo di blocco. Per ulteriori informazioni, vedere la pagina man per il comando.

### Fase

1. Visualizzare le informazioni sui blocchi utilizzando `vserver locks show` comando.

### Esempi

Nell'esempio riportato di seguito vengono visualizzate informazioni riepilogative per un blocco NFSv4 su un file con il percorso `/vol1/file1`. La modalità di accesso sharelock è `write-deny_none` e il blocco è stato concesso con delega di scrittura:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1                    lif1         nfsv4     share-level -
                                     Sharelock Mode: write-deny_none
                                     delegation  -
                                     Delegation Type: write
```

Nell'esempio riportato di seguito vengono visualizzate informazioni dettagliate sull'oplock e sullo sharlock

relative al blocco SMB in un file con il percorso /data2/data2\_2/intro.pptx. Un handle durevole viene concesso sul file con una modalità di accesso con blocco della condivisione write-deny\_none a un client con un indirizzo IP 10.3.1.3. Un oplock di leasing viene concesso con un livello di oplock batch:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
    Volume: data2_2
  Logical Interface: lif2
    Object Path: /data2/data2_2/intro.pptx
    Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
    Lock Protocol: cifs
    Lock Type: share-level
  Node Holding Lock State: node3
    Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: -
  Shared Lock Access Mode: write-deny_none
    Shared Lock is Soft: false
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: durable
    SMB Connect State: connected
  SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

```

    Vserver: vs1
    Volume: data2_2
  Logical Interface: lif2
    Object Path: /data2/data2_2/test.pptx
    Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
    Lock Protocol: cifs
    Lock Type: op-lock
  Node Holding Lock State: node3
    Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
```

```
Bytelock is Soft: -
Oplock Level: batch
Shared Lock Access Mode: -
Shared Lock is Soft: -
Delegation Type: -
Client Address: 10.3.1.3
SMB Open Type: -
SMB Connect State: connected
SMB Expiration Time (Secs): -
SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

## Blocchi di rottura

Quando i blocchi di file impediscono l'accesso dei client ai file, è possibile visualizzare le informazioni sui blocchi attualmente in attesa e quindi interrompere blocchi specifici. Esempi di scenari in cui potrebbe essere necessario interrompere i blocchi includono il debug delle applicazioni.

### A proposito di questa attività

Il `vserver locks break` il comando è disponibile solo a un livello di privilegio avanzato e superiore. La pagina man del comando contiene informazioni dettagliate.

### Fasi

1. Per trovare le informazioni necessarie per interrompere un blocco, utilizzare `vserver locks show` comando.

La pagina man del comando contiene informazioni dettagliate.

2. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

3. Eseguire una delle seguenti operazioni:

Se si desidera interrompere un blocco specificando...	Immettere il comando...
Il nome SVM, il nome del volume, il nome LIF e il percorso del file	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
L'ID blocco	<code>vserver locks break -lockid UUID</code>

4. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Come funzionano i filtri FPolicy first-Read e first-write con NFS

I client NFS sperimentano tempi di risposta elevati durante il traffico elevato delle richieste di lettura/scrittura quando FPolicy viene abilitato utilizzando un server FPolicy esterno con operazioni di lettura/scrittura come eventi monitorati. Per i client NFS, l'utilizzo di filtri di prima lettura e prima scrittura in FPolicy riduce il numero di notifiche FPolicy e migliora le performance.

In NFS, il client esegue l'i/o su un file mediante il recupero dell'handle. Questo handle potrebbe rimanere valido per i riavvii del server e del client. Pertanto, il client è libero di memorizzare nella cache l'handle e di inviarne le richieste senza dover recuperare nuovamente gli handle. In una sessione regolare, molte richieste di lettura/scrittura vengono inviate al file server. Se vengono generate notifiche per tutte queste richieste, potrebbero verificarsi i seguenti problemi:

- Un carico maggiore grazie all'elaborazione aggiuntiva delle notifiche e a tempi di risposta più elevati.
- Un gran numero di notifiche inviate al server FPolicy anche se il server non è interessato da tutte le notifiche.

Dopo aver ricevuto la prima richiesta di lettura/scrittura da un client per un determinato file, viene creata una voce della cache e il conteggio di lettura/scrittura viene incrementato. Questa richiesta viene contrassegnata come prima operazione di lettura/scrittura e viene generato un evento FPolicy. Prima di pianificare e creare i filtri FPolicy per un client NFS, è necessario comprendere le nozioni di base sul funzionamento dei filtri FPolicy.

- First-Read (prima lettura): Filtra le richieste di lettura del client per la prima lettura.

Quando questo filtro viene utilizzato per gli eventi NFS, il `-file-session-io-grouping-count` e `-file-session-io-grouping-duration` Le impostazioni determinano la richiesta di prima lettura per la quale viene elaborato FPolicy.

- First-write: Filtra le richieste di scrittura del client per la first-write.

Quando questo filtro viene utilizzato per gli eventi NFS, il `-file-session-io-grouping-count` e `-file-session-io-grouping-duration` Le impostazioni determinano la richiesta di prima scrittura per la quale FPolicy ha elaborato.

Le seguenti opzioni vengono aggiunte nel database dei server NFS.

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

## Modificare l'ID di implementazione del server NFSv4.1

Il protocollo NFSv4.1 include un ID di implementazione del server che documenta il dominio, il nome e la data del server. È possibile modificare i valori predefiniti dell'ID di implementazione del server. La modifica dei valori predefiniti può essere utile, ad



esempio, per la raccolta di statistiche di utilizzo o la risoluzione dei problemi di interoperabilità. Per ulteriori informazioni, vedere RFC 5661.

### A proposito di questa attività

I valori predefiniti per le tre opzioni sono i seguenti:

Opzione	Nome dell'opzione	Valore predefinito
Dominio ID implementazione NFSv4.1	<code>-v4.1-implementation</code> <code>-domain</code>	netapp.com
Nome ID implementazione NFSv4.1	<code>-v4.1-implementation-name</code>	Nome della versione del cluster
Data ID implementazione NFSv4.1	<code>-v4.1-implementation-date</code>	Data di versione del cluster

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera modificare l'ID di implementazione NFSv4.1...	Immettere il comando...
Dominio	<code>vserver nfs modify -v4.1</code> <code>-implementation-domain domain</code>
Nome	<code>vserver nfs modify -v4.1</code> <code>-implementation-name name</code>
Data	<code>vserver nfs modify -v4.1</code> <code>-implementation-date date</code>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

### Gestire gli ACL NFSv4

#### Vantaggi dell'abilitazione degli ACL NFSv4

L'abilitazione degli ACL NFSv4 offre numerosi vantaggi.

I vantaggi derivanti dall'abilitazione degli ACL NFSv4 includono:

- Controllo più dettagliato dell'accesso degli utenti per file e directory

- Maggiore sicurezza NFS
- Maggiore interoperabilità con CIFS
- Rimozione del limite NFS di 16 gruppi per utente

#### Come funzionano gli ACL NFSv4

Un client che utilizza ACL NFSv4 può impostare e visualizzare ACL su file e directory del sistema. Quando viene creato un nuovo file o sottodirectory in una directory che dispone di un ACL, il nuovo file o sottodirectory eredita tutte le voci ACL (ACL) nell'ACL contrassegnate con gli indicatori di ereditarietà appropriati.

Quando viene creato un file o una directory come risultato di una richiesta NFSv4, l'ACL del file o della directory risultante dipende dal fatto che la richiesta di creazione del file includa un ACL o solo permessi di accesso ai file UNIX standard e se la directory principale dispone di un ACL:

- Se la richiesta include un ACL, viene utilizzato tale ACL.
- Se la richiesta include solo autorizzazioni di accesso ai file UNIX standard ma la directory principale dispone di un ACL, le ACE nell'ACL della directory principale vengono ereditate dal nuovo file o directory, purché le ACE siano state contrassegnate con gli indicatori di ereditarietà appropriati.



Un ACL padre viene ereditato anche se `-v4.0-acl` è impostato su `off`.

- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale non dispone di un ACL, la modalità file client viene utilizzata per impostare le autorizzazioni di accesso ai file UNIX standard.
- Se la richiesta include solo le autorizzazioni di accesso ai file UNIX standard e la directory principale dispone di un ACL non ereditabile, il nuovo oggetto viene creato solo con i bit di modalità.



Se il `-chown-mode` il parametro è stato impostato su `restricted` con i comandi in `vserver nfs` oppure `vserver export-policy rule Famiglie`, la proprietà del file può essere modificata solo dal superutente, anche se le autorizzazioni su disco impostate con gli ACL NFSv4 consentono a un utente non root di modificare la proprietà del file. Per ulteriori informazioni, consulta le relative pagine man.

#### Attiva o disattiva la modifica degli ACL NFSv4

Quando ONTAP riceve un `chmod` Per un file o una directory con un ACL, per impostazione predefinita l'ACL viene conservato e modificato per riflettere la modifica del bit di modalità. È possibile disattivare `-v4-acl-preserve` Parametro per modificare il comportamento se si desidera che l'ACL venga eliminato.

#### A proposito di questa attività

Quando si utilizza uno stile di sicurezza unificato, questo parametro specifica anche se le autorizzazioni del file NTFS vengono mantenute o interrotte quando un client invia un comando `chmod`, `chgroup` o `chown` per un file o una directory.

L'impostazione predefinita per questo parametro è `Enabled` (attivato).

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Attiva conservazione e modifica degli ACL NFSv4 esistenti (impostazione predefinita)	<pre>vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled</pre>
Disattiva la conservazione e disattiva gli ACL NFSv4 quando si modificano i bit di modalità	<pre>vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled</pre>

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

#### Come ONTAP utilizza gli ACL NFSv4 per determinare se è in grado di eliminare un file

Per determinare se è possibile eliminare un file, ONTAP utilizza una combinazione del bit DELETE del file e del bit DELETE\_CHILD della directory contenente. Per ulteriori informazioni, vedere NFS 4.1 RFC 5661.

#### Attivare o disattivare gli ACL NFSv4

Per attivare o disattivare gli ACL NFSv4, è possibile modificare `-v4.0-acl` e `-v4.1-acl` opzioni. Queste opzioni sono disattivate per impostazione predefinita.

#### A proposito di questa attività

Il `-v4.0-acl` oppure `-v4.1-acl` L'opzione controlla l'impostazione e la visualizzazione degli ACL NFSv4; non controlla l'applicazione di questi ACL per il controllo degli accessi.

#### Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Quindi...
Abilitare gli ACL NFSv4.0	Immettere il seguente comando:  <pre>vserver nfs modify -vserver vserver_name -v4.0-acl enabled</pre>
Disattivare gli ACL NFSv4.0	Immettere il seguente comando:  <pre>vserver nfs modify -vserver vserver_name -v4.0-acl disabled</pre>

Abilitare gli ACL NFSv4.1	Immettere il seguente comando:  <code>vserver nfs modify -vserver vserver_name -v4.1-acl enabled</code>
Disattivare gli ACL NFSv4.1	Immettere il seguente comando:  <code>vserver nfs modify -vserver vserver_name -v4.1-acl disabled</code>

#### Modificare il limite massimo ACE per gli ACL NFSv4

È possibile modificare il numero massimo di ACE consentiti per ogni ACL NFSv4 modificando il parametro `-v4-acl-max-aces`. Per impostazione predefinita, il limite è impostato su 400 ACE per ogni ACL. L'aumento di questo limite può contribuire a garantire una migrazione corretta dei dati con ACL contenenti oltre 400 ACE nei sistemi storage che eseguono ONTAP.

#### A proposito di questa attività

L'aumento di questo limite potrebbe influire sulle performance dei client che accedono ai file con ACL NFSv4.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Modificare il limite massimo ACE per gli ACL NFSv4:

```
vserver nfs modify -v4-acl-max-aces max_ace_limit
```

L'intervallo valido di

`max_ace_limit` è 192 a. 1024.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

#### Gestire le deleghe dei file NFSv4

##### Attivare o disattivare le deleghe dei file di lettura NFSv4

Per attivare o disattivare le deleghe dei file di lettura NFSv4, è possibile modificare `-v4.0-read-delegation` oppure opzione. Attivando le deleghe dei file di lettura, è possibile eliminare gran parte dell'overhead dei messaggi associato all'apertura e alla chiusura dei file.

#### A proposito di questa attività

Per impostazione predefinita, le deleghe dei file di lettura sono disattivate.

Lo svantaggio dell'abilitazione delle deleghe dei file in lettura consiste nel fatto che il server e i suoi client devono ripristinare le deleghe dopo il riavvio o il riavvio del server, il riavvio o il riavvio di un client o la creazione di una partizione di rete.

## Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Quindi...
Abilitare le deleghe dei file di lettura NFSv4	Immettere il seguente comando:  <pre>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled</pre>
Abilitare le deleghe dei file di lettura NFSv4.1	Immettere il seguente comando:  + <pre>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled</pre>
Disattiva le deleghe dei file di lettura NFSv4	Immettere il seguente comando:  <pre>vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled</pre>
Disattiva le deleghe dei file di lettura NFSv4.1	Immettere il seguente comando:  <pre>vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled</pre>

## Risultato

Le opzioni di delega dei file diventano effettive non appena vengono modificate. Non è necessario riavviare NFS.

### Attivare o disattivare le deleghe dei file di scrittura NFSv4

Per attivare o disattivare le deleghe dei file di scrittura, è possibile modificare `-v4.0 -write-delegation` oppure opzione. Attivando le deleghe di scrittura dei file, è possibile eliminare gran parte dell'overhead dei messaggi associato al blocco di file e record, oltre all'apertura e alla chiusura dei file.

### A proposito di questa attività

Per impostazione predefinita, le deleghe dei file di scrittura sono disattivate.

Lo svantaggio di abilitare le deleghe dei file di scrittura è che il server e i relativi client devono eseguire attività aggiuntive per ripristinare le deleghe dopo il riavvio o il riavvio del server, il riavvio o il riavvio di un client o la creazione di una partizione di rete.

## Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Quindi...
Abilitare le deleghe dei file di scrittura NFSv4	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation enabled</code>
Abilitare le deleghe dei file di scrittura NFSv4.1	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation enabled</code>
Disattiva le deleghe dei file di scrittura NFSv4	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.0 -write-delegation disabled</code>
Disattivare le deleghe dei file di scrittura NFSv4.1	Immettere il seguente comando: <code>vserver nfs modify -vserver vserver_name -v4.1 -write-delegation disabled</code>

## Risultato

Le opzioni di delega dei file diventano effettive non appena vengono modificate. Non è necessario riavviare NFS.

## Configurare il blocco di file e record NFSv4

### Informazioni sul blocco di file e record NFSv4

Per i client NFSv4, ONTAP supporta il meccanismo di blocco dei file NFSv4, mantenendo lo stato di tutti i blocchi dei file in un modello basato sul lease.

["Report tecnico di NetApp 3580: Guida ai miglioramenti e alle Best practice di NFSv4 per l'implementazione di Data ONTAP"](#)

### Specificare il periodo di lease di blocco NFSv4

Per specificare il periodo di leasing di blocco NFSv4 (ovvero, il periodo di tempo in cui ONTAP concede irrevocabilmente un blocco a un client), è possibile modificare `-v4 -lease-seconds` opzione. I periodi di leasing più brevi accelerano il ripristino dei server, mentre i periodi di leasing più lunghi sono vantaggiosi per i server che gestiscono un numero molto elevato di client.

### A proposito di questa attività

Per impostazione predefinita, questa opzione è impostata su 30. Il valore minimo per questa opzione è 10. Il valore massimo per questa opzione è il periodo di tolleranza di blocco, che è possibile impostare con `locking.lease_seconds` opzione.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Immettere il seguente comando:

```
vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
```

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

#### **Specificare il periodo di tolleranza del blocco NFSv4**

Per specificare il periodo di tolleranza del blocco NFSv4 (ovvero il periodo di tempo in cui i client tentano di recuperare il proprio stato di blocco da ONTAP durante il ripristino del server), è possibile modificare `-v4-grace-seconds` opzione.

#### **A proposito di questa attività**

Per impostazione predefinita, questa opzione è impostata su 45.

#### **Fasi**

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Immettere il seguente comando:

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

#### **Come funzionano i referral NFSv4**

Quando si abilitano i riferimenti NFSv4, ONTAP fornisce i riferimenti “intra-SVM” ai client NFSv4. Il riferimento intra-SVM avviene quando un nodo del cluster che riceve la richiesta NFSv4 fa riferimento al client NFSv4 a un'altra interfaccia logica (LIF) sulla macchina virtuale di storage (SVM).

Il client NFSv4 deve accedere al percorso che ha ricevuto il riferimento alla LIF di destinazione da quel momento in poi. Il nodo del cluster originale fornisce tale riferimento quando determina l'esistenza di una LIF nella SVM residente sul nodo del cluster su cui risiede il volume di dati, consentendo ai client un accesso più rapido ai dati ed evitando comunicazioni del cluster aggiuntive.

#### **Attiva o disattiva i riferimenti NFSv4**

È possibile attivare i riferimenti NFSv4 sulle macchine virtuali di storage (SVM) attivando le opzioni `-v4-fsid-change` e `-v4.0-referrals` oppure. L'attivazione dei riferimenti

NFSV4 può accelerare l'accesso ai dati per i client NFSv4 che supportano questa funzionalità.

**Di cosa hai bisogno**

Se si desidera attivare i riferimenti NFS, è necessario prima disattivare Parallel NFS. Non è possibile attivare entrambi contemporaneamente.

**Fasi**

- 1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- 2. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Abilitare i riferimenti NFSv4	<code>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled</code>
Disattiva i riferimenti NFSv4	<code>vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled</code>
Abilitare i riferimenti NFSv4.1	<code>vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled</code>
Disattiva i riferimenti NFSv4.1	<code>vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled</code>

- 3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

**Visualizzare le statistiche NFS**

È possibile visualizzare le statistiche NFS per le macchine virtuali di storage (SVM) sul sistema storage per monitorare le performance e diagnosticare i problemi.

**Fasi**

- 1. Utilizzare `statistics catalog object show` Per identificare gli oggetti NFS da cui è possibile visualizzare i dati.  
  
`statistics catalog object show -object nfs*`
- 2. Utilizzare `statistics start` e opzionale `statistics stop` comandi per raccogliere un campione di dati da uno o più oggetti.
- 3. Utilizzare `statistics show` per visualizzare i dati di esempio.



### Esempio: Monitoraggio delle performance di NFSv3

L'esempio seguente mostra i dati relativi alle prestazioni per il protocollo NFSv3.

Il seguente comando avvia la raccolta dati per un nuovo campione:

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

Il comando seguente mostra i dati dell'esempio specificando i contatori che mostrano il numero di richieste di lettura e scrittura riuscite rispetto al numero totale di richieste di lettura e scrittura:

```
vs1::> statistics show -sample-id nfs_sample -counter  
read_total|write_total|read_success|write_success
```

Object: nfsv3

Instance: vs1

Start-time: 2/11/2013 15:38:29

End-time: 2/11/2013 15:38:41

Cluster: cluster1

Counter	Value
read_success	40042
read_total	40042
write_success	1492052
write_total	1492052

### Informazioni correlate

["Configurazione del monitoraggio delle performance"](#)

### Visualizzare le statistiche DNS

È possibile visualizzare le statistiche DNS per le macchine virtuali di storage (SVM) sul sistema di storage per monitorare le performance e diagnosticare i problemi.

#### Fasi

1. Utilizzare `statistics catalog object show` Per identificare gli oggetti DNS da cui è possibile visualizzare i dati.

```
statistics catalog object show -object external_service_op*
```

2. Utilizzare `statistics start` e `statistics stop` comandi per raccogliere un campione di dati da uno o più oggetti.
3. Utilizzare `statistics show` per visualizzare i dati di esempio.

## Monitoraggio delle statistiche DNS

I seguenti esempi mostrano i dati relativi alle prestazioni per le query DNS. I seguenti comandi avviano la raccolta di dati per un nuovo campione:

```
vs1::*> statistics start -object external_service_op -sample-id  
dns_sample1  
vs1::*> statistics start -object external_service_op_error -sample-id  
dns_sample2
```

Il seguente comando visualizza i dati dell'esempio specificando i contatori che visualizzano il numero di query DNS inviate rispetto al numero di query DNS ricevute, non riuscite o in timeout:

```
vs1::*> statistics show -sample-id dns_sample1 -counter  
num_requests_sent|num_responses_received|num_successful_responses|num_time  
outs|num_request_failures|num_not_found_responses
```

```
Object: external_service_op  
Instance: vs1:DNS:Query:10.72.219.109  
Start-time: 3/8/2016 11:15:21  
End-time: 3/8/2016 11:16:52  
Elapsed-time: 91s  
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	0
num_requests_sent	1
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

Il seguente comando visualizza i dati dell'esempio specificando i contatori che visualizzano il numero di volte in cui è stato ricevuto un errore specifico per una query DNS sul server specifico:

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count
```

Object: external\_service\_op\_error

Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109

Start-time: 3/8/2016 11:23:21

End-time: 3/8/2016 11:24:25

Elapsed-time: 64s

Scope: vs1

Counter	Value
count	1
error_string	NXDOMAIN
server_ip_address	10.72.219.109

3 entries were displayed.

## Informazioni correlate

["Configurazione del monitoraggio delle performance"](#)

## Visualizzare le statistiche NIS

È possibile visualizzare le statistiche NIS per le macchine virtuali di storage (SVM) sul sistema storage per monitorare le performance e diagnosticare i problemi.

### Fasi

1. Utilizzare `statistics catalog object show` Per identificare gli oggetti NIS da cui è possibile visualizzare i dati.

```
statistics catalog object show -object external_service_op*
```

2. Utilizzare `statistics start` e `statistics stop` comandi per raccogliere un campione di dati da uno o più oggetti.
3. Utilizzare `statistics show` per visualizzare i dati di esempio.

## Monitoraggio delle statistiche NIS

I seguenti esempi mostrano i dati relativi alle prestazioni per le query NIS. I seguenti comandi avviano la raccolta di dati per un nuovo campione:

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

Il seguente comando visualizza i dati dell'esempio specificando i contatori che mostrano il numero di query NIS

inviata rispetto al numero di query NIS ricevute, non riuscite o in timeout:

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses
```

```
Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1
```

Counter	Value
num_not_found_responses	0
num_request_failures	1
num_requests_sent	2
num_responses_received	1
num_successful_responses	1
num_timeouts	0

6 entries were displayed.

Il seguente comando visualizza i dati dell'esempio specificando i contatori che indicano il numero di volte in cui è stato ricevuto un errore specifico per una query NIS sul server specifico:

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count
```

```
Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1
```

Counter	Value
count	1
error_string	YP_NOTFOUND
server_ip_address	10.227.13.221

3 entries were displayed.

## Informazioni correlate

["Configurazione del monitoraggio delle performance"](#)

## Supporto per VMware vStorage su NFS

ONTAP supporta alcune API vStorage VMware per l'integrazione degli array (VAAI) in un ambiente NFS.

### Funzionalità supportate

Sono supportate le seguenti funzioni:

- Offload delle copie

Consente a un host ESXi di copiare macchine virtuali o dischi di macchine virtuali (VMDK) direttamente tra la posizione dell'archivio dati di origine e di destinazione senza coinvolgere l'host. In questo modo si preservano i cicli della CPU host ESXi e la larghezza di banda della rete. L'offload delle copie preserva l'efficienza dello spazio se il volume di origine è sparso.

- Prenotazione di spazio

Garantisce lo spazio di storage per un file VMDK riservando spazio all'IT.

### Limitazioni

VMware vStorage su NFS presenta le seguenti limitazioni:

- Le operazioni di offload della copia possono avere esito negativo nei seguenti scenari:
  - Durante l'esecuzione di wafiron sul volume di origine o di destinazione, in quanto il volume viene temporaneamente disattivato
  - Durante lo spostamento del volume di origine o di destinazione
  - Durante lo spostamento della LIF di origine o di destinazione
  - Durante l'esecuzione di operazioni di Takeover o giveback
  - Durante le operazioni di switchover o switchback
- La copia lato server potrebbe non riuscire a causa delle differenze di formato del file handle nel seguente scenario:

Si tenta di copiare i dati dalle SVM che hanno attualmente o precedentemente esportato qtree in SVM che non hanno mai esportato qtree. Per aggirare questo limite, è possibile esportare almeno un qtree sulla SVM di destinazione.

### Informazioni correlate

["Quali operazioni VAAI offloaded sono supportate da Data ONTAP?"](#)

### Abilitare o disabilitare VMware vStorage su NFS

È possibile attivare o disattivare il supporto per VMware vStorage su NFS su macchine virtuali di storage (SVM) utilizzando `vserver nfs modify` comando.

### A proposito di questa attività

Per impostazione predefinita, il supporto di VMware vStorage su NFS è disattivato.

### Fasi

1. Visualizzare lo stato corrente del supporto vStorage per le SVM:

```
vserver nfs show -vserver vserver_name -instance
```

2. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare il supporto di VMware vStorage	<pre>vserver nfs modify -vserver vserver_name -vstorage enabled</pre>
Disattivare il supporto di VMware vStorage	<pre>vserver nfs modify -vserver vserver_name -vstorage disabled</pre>

### Al termine

Prima di utilizzare questa funzionalità, è necessario installare il plug-in NFS per VMware VAAI. Per ulteriori informazioni, consulta la sezione *Installazione del plug-in NetApp NFS per VMware VAAI*.

### Informazioni correlate

["Documentazione NetApp: Plug-in NetApp NFS per VMware VAAI"](#)

### Attiva o disattiva il supporto rquota

ONTAP supporta il protocollo di quota remota versione 1 (rquota v1). Il protocollo rquota consente ai client NFS di ottenere informazioni sulle quote per gli utenti da un computer remoto. È possibile attivare rquota su macchine virtuali storage (SVM) utilizzando `vserver nfs modify` comando.

### A proposito di questa attività

Per impostazione predefinita, rquota è disattivato.

### Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Abilitare il supporto rquota per le SVM	<pre>vserver nfs modify -vserver vserver_name -rquota enable</pre>
Disattiva il supporto rquota per le SVM	<pre>vserver nfs modify -vserver vserver_name -rquota disable</pre>

Per ulteriori informazioni sulle quote, vedere ["Gestione dello storage logico"](#).

### Miglioramento delle performance di NFSv3 e NFSv4 modificando le dimensioni del trasferimento TCP

È possibile migliorare le prestazioni dei client NFSv3 e NFSv4 che si connettono ai sistemi storage su una rete ad alta latenza modificando le dimensioni massime di

## trasferimento TCP.

Quando i client accedono ai sistemi storage su una rete ad alta latenza, ad esempio WAN (Wide Area Network) o MAN (Metro Area Network) con una latenza superiore a 10 millisecondi, è possibile migliorare le prestazioni di connessione modificando le dimensioni massime di trasferimento TCP. I client che accedono a sistemi storage in una rete a bassa latenza, come una LAN (Local Area Network), possono aspettarsi pochi benefici dalla modifica di questi parametri. Se il miglioramento del throughput non supera l'impatto della latenza, non utilizzare questi parametri.

Per determinare se il tuo ambiente di storage potrebbe trarre beneficio dalla modifica di questi parametri, devi prima eseguire una valutazione completa delle performance di un client NFS dalle performance scarse. Verificare se le performance ridotte sono dovute a un'eccessiva latenza di round trip e a una piccola richiesta sul client. In queste condizioni, il client e il server non possono utilizzare completamente la larghezza di banda disponibile perché trascorrono la maggior parte dei loro cicli di lavoro in attesa di piccole richieste e risposte da trasmettere sulla connessione.

Aumentando le dimensioni delle richieste NFSv3 e NFSv4, il client e il server possono utilizzare la larghezza di banda disponibile in modo più efficace per spostare più dati per unità di tempo, aumentando quindi l'efficienza complessiva della connessione.

Tenere presente che la configurazione tra il sistema storage e il client potrebbe variare. Il sistema storage e il client supportano una dimensione massima di 1 MB per le operazioni di trasferimento. Tuttavia, se si configura il sistema di storage in modo che supporti le dimensioni massime di trasferimento di 1 MB ma il client supporta solo 64 KB, la dimensione di trasferimento del mount è limitata a 64 KB o meno.

Prima di modificare questi parametri, è necessario tenere presente che questo comporta un consumo di memoria aggiuntivo nel sistema di storage per il periodo di tempo necessario per assemblare e trasmettere una risposta elevata. Maggiore è la latenza elevata delle connessioni al sistema storage, maggiore è il consumo di memoria aggiuntivo. I sistemi storage con elevata capacità di memoria potrebbero avere un effetto molto ridotto da questo cambiamento. I sistemi storage con capacità di memoria bassa potrebbero riscontrare un notevole peggioramento delle performance.

Il corretto utilizzo di questi parametri dipende dalla capacità di recuperare i dati da più nodi di un cluster. La latenza intrinseca della rete del cluster potrebbe aumentare la latenza complessiva della risposta. La latenza complessiva tende ad aumentare quando si utilizzano questi parametri. Di conseguenza, i carichi di lavoro sensibili alla latenza potrebbero avere un impatto negativo.

### Modificare le dimensioni massime di trasferimento TCP NFSv3 e NFSv4

È possibile modificare `-tcp-max-xfer-size` Opzione per configurare le dimensioni massime di trasferimento per tutte le connessioni TCP utilizzando i protocolli NFSv3 e NFSv4.x.

#### A proposito di questa attività

È possibile modificare queste opzioni singolarmente per ciascuna macchina virtuale di storage (SVM).

A partire da ONTAP 9 `v3-tcp-max-read-size` e `v3-tcp-max-write-size` le opzioni sono obsolete. È necessario utilizzare `-tcp-max-xfer-size` invece.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Modificare le dimensioni massime di trasferimento TCP NFSv3 o NFSv4	<pre>vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size</pre>

Opzione	Raggio d'azione	Predefinito
-tcp-max-xfer-size	da 8192 a 1048576 byte	65536 byte



La dimensione massima di trasferimento immessa deve essere un multiplo di 4 KB (4096 byte). Le richieste non allineate correttamente influiscono negativamente sulle performance.

3. Utilizzare `vserver nfs show -fields tcp-max-xfer-size` per verificare le modifiche.
4. Se alcuni client utilizzano i mount statici, smontare e rimontare per rendere effettive le nuove dimensioni dei parametri.

### Esempio

Il seguente comando imposta le dimensioni massime di trasferimento TCP NFSv3 e NFSv4.x su 1048576 byte sulla SVM denominata vs1:

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

### Configurare il numero di ID di gruppo consentiti per gli utenti NFS

Per impostazione predefinita, ONTAP supporta fino a 32 ID di gruppo quando gestisce le credenziali utente NFS utilizzando l'autenticazione Kerberos (RPCSEC\_GSS). Quando si utilizza l'autenticazione AUTH\_SYS, il numero massimo predefinito di ID gruppo è 16, come definito in RFC 5531. È possibile aumentare il numero massimo fino a 1,024 se si dispone di utenti che fanno parte di un numero di gruppi superiore a quello predefinito.

#### A proposito di questa attività

Se un utente dispone di un numero di ID di gruppo superiore a quello predefinito nelle proprie credenziali, gli ID di gruppo rimanenti vengono troncati e l'utente potrebbe ricevere errori quando tenta di accedere ai file dal sistema di storage. Impostare il numero massimo di gruppi, per SVM, su un numero che rappresenta il numero massimo di gruppi nell'ambiente.

La seguente tabella mostra i due parametri di `vserver nfs modify` Comando che determina il numero massimo di ID di gruppo in tre configurazioni di esempio:

Parametri	Impostazioni	Limite ID gruppo risultante
-----------	--------------	-----------------------------



-extended-groups-limit	32	RPCSEC_GSS: 32
-auth-sys-extended-groups	disabled	AUTH_SYS: 16
Queste sono le impostazioni predefinite.		
-extended-groups-limit	256	RPCSEC_GSS: 256
-auth-sys-extended-groups	disabled	AUTH_SYS: 16
-extended-groups-limit	512	RPCSEC_GSS: 512
-auth-sys-extended-groups	enabled	AUTH_SYS: 512

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire l'azione desiderata:

Se si desidera impostare il numero massimo di gruppi ausiliari consentiti...	Immettere il comando...
Solo per RPCSEC_GSS e lasciare AUTH_SYS impostato sul valore predefinito 16	<pre>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled</pre>
Per RPCSEC_GSS e AUTH_SYS	<pre>vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled</pre>

3. Verificare -extended-groups-limit Valutare e verificare se AUTH\_SYS utilizza gruppi estesi:

```
vserver nfs show -vserver vserver_name -fields auth-sys-extended-  
groups,extended-groups-limit
```

4. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Esempio

Nell'esempio riportato di seguito vengono abiliti i gruppi estesi per l'autenticazione AUTH\_SYS e viene impostato il numero massimo di gruppi estesi su 512 per l'autenticazione AUTH\_SYS e RPCSEC\_GSS. Queste modifiche vengono apportate solo ai client che accedono alla SVM denominata vs1:

```

vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
        them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
-----
vs1      enabled                      512

vs1::*> set -privilege admin

```

## Controllare l'accesso dell'utente root ai dati di sicurezza NTFS

È possibile configurare ONTAP per consentire ai client NFS di accedere ai dati di sicurezza NTFS e ai client NTFS per accedere ai dati di sicurezza NFS. Quando si utilizza lo stile di sicurezza NTFS su un archivio dati NFS, è necessario decidere come trattare l'accesso da parte dell'utente root e configurare di conseguenza la macchina virtuale di storage (SVM).

### A proposito di questa attività

Quando un utente root accede ai dati di sicurezza NTFS, sono disponibili due opzioni:

- Mappare l'utente root a un utente Windows come qualsiasi altro utente NFS e gestire l'accesso in base agli ACL NTFS.
- Ignorare gli ACL NTFS e fornire l'accesso completo all'utente root.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire l'azione desiderata:

Se si desidera che l'utente root...	Immettere il comando...
Essere mappato a un utente Windows	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled</code>
Ignorare il controllo dell'ACL NT	<code>vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled</code>

Per impostazione predefinita, questo parametro è disattivato.

Se questo parametro è attivato ma non esiste alcuna mappatura dei nomi per l'utente root, ONTAP utilizza una credenziale di amministratore SMB predefinita per il controllo.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Versioni e client NFS supportati

### Panoramica delle versioni e dei client NFS supportati

Prima di poter utilizzare NFS nella rete, è necessario conoscere le versioni e i client NFS supportati da ONTAP.

Questa tabella indica quando le versioni principali e minori dei protocolli NFS sono supportate per impostazione predefinita in ONTAP. Il supporto predefinito non indica che si tratta della prima versione di ONTAP che supporta tale protocollo NFS.

Versione	Attivato per impostazione predefinita
NFSv3	Sì
NFSv4.0	Sì, a partire da ONTAP 9.9.1
NFSv4.1	Sì, a partire da ONTAP 9.9.1
NFSv4.2	Sì, a partire da ONTAP 9.9.1
PNFS	No

Per informazioni aggiornate sui client NFS supportati da ONTAP, consulta la matrice di interoperabilità.

["Tool di matrice di interoperabilità NetApp"](#)

### Funzionalità NFSv4.0 supportata da ONTAP

ONTAP supporta tutte le funzionalità obbligatorie di NFSv4.0, ad eccezione dei meccanismi di sicurezza SPKM3 e LIPKEY.

Sono supportate le seguenti funzionalità DI NFSV4:

- **COMPOSTO**

Consente a un client di richiedere più operazioni di file in una singola richiesta RPC (Remote procedure Call).

- **Delega del file**

Consente al server di delegare il controllo del file ad alcuni tipi di client per l'accesso in lettura e scrittura.

- **Pseudo-fs**

Utilizzato dai server NFSv4 per determinare i punti di montaggio sul sistema storage. NFSv4 non contiene alcun protocollo di montaggio.

- **Blocco**

Basato sul leasing. Non esistono protocolli NLM (Network Lock Manager) o NSM (Network Status Monitor) separati in NFSv4.

Per ulteriori informazioni sul protocollo NFSv4.0, vedere RFC 3530.

## **Limitazioni del supporto ONTAP per NFSv4**

È necessario conoscere diverse limitazioni del supporto ONTAP per NFSv4.

- La funzione di delega non è supportata da ogni tipo di client.
- In ONTAP 9.4 e versioni precedenti, i nomi con caratteri non ASCII su volumi diversi da UTF8 vengono rifiutati dal sistema di storage.

In ONTAP 9.5 e versioni successive, i volumi creati con l'impostazione del linguaggio utf8mb4 e montati utilizzando NFS v4 non sono più soggetti a questa restrizione.

- Tutti gli handle di file sono persistenti; il server non fornisce handle di file volatili.
- Migrazione e replica non sono supportate.
- I client NFSv4 non sono supportati con mirror di sola lettura per la condivisione del carico.

ONTAP indirizza i client NFSv4 all'origine del mirror di condivisione del carico per l'accesso diretto in lettura e scrittura.

- Gli attributi denominati non sono supportati.
- Sono supportati tutti gli attributi consigliati, ad eccezione di:

- archive
- hidden
- homogeneous
- mimetype
- quota\_avail\_hard
- quota\_avail\_soft
- quota\_used
- system
- time\_backup



Anche se non supporta quota\* ONTAP supporta le quote utente e di gruppo tramite il protocollo RQUOTA Side Band.

## Supporto ONTAP per NFSv4.1

A partire da ONTAP 9.8, la funzionalità `nconnect` è disponibile per impostazione predefinita quando NFSv4.1 è attivato.

Le implementazioni dei client NFS precedenti utilizzano solo una singola connessione TCP con un mount. In ONTAP, una singola connessione TCP può diventare un collo di bottiglia con un aumento degli IOPS. Tuttavia, un client abilitato a `nconnect` può avere più connessioni TCP (fino a 16) associate a un singolo montaggio NFS. Un client NFS di questo tipo moltiplica le operazioni di file su più connessioni TCP in modo round-robin e ottiene così un throughput più elevato dalla larghezza di banda di rete disponibile. `NConnect` è consigliato solo per i supporti NFSv3 e NFSv4.1.

Consultare la documentazione del client NFS per verificare se `nconnect` è supportato nella versione del client.

NFSv4.1 è attivato per impostazione predefinita in ONTAP 9.9.1 e versioni successive. Nelle versioni precedenti, è possibile attivarlo specificando `-v4.1` e impostarlo su `enabled` Quando si crea un server NFS sulla macchina virtuale di storage (SVM).

ONTAP non supporta le deleghe a livello di file e directory NFSv4.1.

## Supporto ONTAP per NFSv4.2

A partire da ONTAP 9.8, ONTAP supporta il protocollo NFSv4.2 per consentire l'accesso a client abilitati per NFSv4.2.

NFSv4.2 è attivato per impostazione predefinita in ONTAP 9.9.1 e versioni successive. In ONTAP 9.8, è necessario attivare manualmente `v4.2` specificando il `-v4.1` e impostarlo su `enabled` Quando si crea un server NFS sulla macchina virtuale di storage (SVM). L'abilitazione di NFSv4.1 consente inoltre ai client di utilizzare le funzionalità di NFSv4.1 mentre sono montati come `v4.2`.

Le successive versioni di ONTAP ampliano il supporto per NFSv4.2 funzioni opzionali.

A partire da...	NFSv4.2 caratteristiche opzionali includono ...
ONTAP 9.12.1	<ul style="list-style-type: none"><li>• Attributi estesi NFS</li><li>• File sparse</li><li>• Prenotazioni di spazio</li></ul>
ONTAP 9.9.1	Obbligatorio Access Control (MAC) con etichetta NFS

### Etichette di sicurezza NFS v4.2

A partire da ONTAP 9.9.1, è possibile attivare le etichette di sicurezza NFS. Sono disattivati per impostazione predefinita.

Con le etichette di sicurezza NFS v4.2, i server NFS ONTAP sono compatibili con il controllo di accesso obbligatorio (MAC), memorizzando e recuperando gli attributi `sec_label` inviati dai client.

Per ulteriori informazioni, vedere ["RFC 7240"](#).

A partire da ONTAP 9.12.1, le etichette di sicurezza NFS v4.2 sono supportate per le operazioni di dump NDMP. Se vengono rilevate etichette di sicurezza su file o directory nelle release precedenti, il dump non riesce.

## Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Abilitare le etichette di sicurezza:

```
vserver nfs modify -vserver _svm_name_ -v4.2-seclabel enabled
```

## Attributi estesi NFS

A partire da ONTAP 9.12.1, gli attributi estesi NFS (xattrs) sono attivati per impostazione predefinita.

Gli attributi estesi sono attributi NFS standard definiti da ["RFC 8276"](#) E abilitato nei moderni client NFS. Possono essere utilizzate per collegare metadati definiti dall'utente a oggetti del file system e sono interessanti per implementazioni di sicurezza avanzate.

Gli attributi estesi NFS non sono attualmente supportati per le operazioni di dump NDMP. Se vengono rilevati attributi estesi su file o directory, il dump procede ma non esegue il backup degli attributi estesi su tali file o directory.

Se è necessario disattivare gli attributi estesi, utilizzare `vserver nfs modify -v4.2-xattrs disabled` comando.

## Supporto ONTAP per NFS parallelo

ONTAP supporta NFS paralleli (pNFS). Il protocollo pNFS offre miglioramenti delle performance offrendo ai client l'accesso diretto ai dati di un set di file distribuiti su più nodi di un cluster. Aiuta i clienti a individuare il percorso ottimale per un volume.

## Utilizzo di supporti rigidi

Durante la risoluzione dei problemi di montaggio, assicurarsi di utilizzare il tipo di montaggio corretto. NFS supporta due tipi di montaggio: Supporti morbidi e hard mount. Per motivi di affidabilità, utilizzare solo supporti rigidi.

Non si consiglia di utilizzare supporti soft, soprattutto quando è possibile che si verificano frequenti timeout NFS. Le condizioni di gara possono verificarsi in seguito a questi timeout, che possono portare alla corruzione dei dati.

## Dipendenze di nomi di file e directory NFS e SMB

### Panoramica delle dipendenze di nomi di file e directory NFS e SMB

Le convenzioni di denominazione di file e directory dipendono dai sistemi operativi dei client di rete e dai protocolli di condivisione file, oltre alle impostazioni della lingua del cluster e dei client ONTAP.

Il sistema operativo e i protocolli di condivisione file determinano quanto segue:

- Caratteri che possono essere utilizzati da un nome file
- Distinzione tra maiuscole e minuscole per un nome file

ONTAP supporta caratteri multi-byte nei nomi di file, directory e qtree, a seconda della versione di ONTAP.

### **Caratteri che possono essere utilizzati da un nome di file o di directory**

Se si accede a un file o a una directory da client con sistemi operativi diversi, utilizzare caratteri validi in entrambi i sistemi operativi.

Ad esempio, se si utilizza UNIX per creare un file o una directory, non utilizzare i due punti (:) nel nome perché i due punti non sono consentiti nei nomi di file o directory MS-DOS. Poiché le restrizioni sui caratteri validi variano da un sistema operativo all'altro, consultare la documentazione del sistema operativo client per ulteriori informazioni sui caratteri non consentiti.

### **Distinzione tra maiuscole e minuscole dei nomi di file e directory in un ambiente multiprotocollo**

I nomi di file e directory sono sensibili al maiuscolo/minuscolo per i client NFS e non al maiuscolo/minuscolo ma conservano il maiuscolo/minuscolo per i client SMB. È necessario comprendere le implicazioni di un ambiente multiprotocollo e le azioni da intraprendere quando si specifica il percorso durante la creazione di condivisioni SMB e quando si accede ai dati all'interno delle condivisioni.

Se un client SMB crea una directory denominata `testdir`, Sia i client SMB che NFS visualizzano il nome del file come `testdir`. Tuttavia, se un utente SMB tenta in seguito di creare un nome di directory `TESTDIR`, il nome non è consentito perché, per il client SMB, tale nome esiste attualmente. Se un utente NFS successivamente crea una directory denominata `TESTDIR` il client , NFS e SMB visualizzano il nome della directory in modo diverso, come segue:

- Sui client NFS, ad esempio, vengono visualizzati entrambi i nomi di directory così come sono stati creati `testdir` e `TESTDIR`, perché i nomi delle directory sono sensibili al maiuscolo/minuscolo.
- I client SMB utilizzano i nomi 8.3 per distinguere le due directory. Una directory ha il nome del file di base. Alle directory aggiuntive viene assegnato un nome file 8.3.
  - Sui client SMB, viene visualizzato `testdir` e `TESTDI~1`.
  - ONTAP crea il `TESTDI~1` nome della directory per differenziare le due directory.

In questo caso, è necessario utilizzare il nome 8.3 quando si specifica un percorso di condivisione durante la creazione o la modifica di una condivisione su una macchina virtuale di storage (SVM).

Analogamente per i file, se viene creato un client SMB `test.txt`, Sia i client SMB che NFS visualizzano il nome del file come `test.txt`. Tuttavia, se un utente SMB tenta di creare in un secondo momento `Test.txt`, il nome non è consentito perché, per il client SMB, tale nome esiste attualmente. Se un utente NFS successivamente crea un file denominato `Test.txt` il client , NFS e SMB visualizzano il nome del file in modo diverso, come segue:

- Sui client NFS, vengono visualizzati entrambi i nomi dei file così come sono stati creati, `test.txt` e `Test.txt`, perché i nomi dei file sono sensibili al maiuscolo/minuscolo.

- I client SMB utilizzano i nomi 8.3 per distinguere i due file. Un file ha il nome del file di base. Ai file aggiuntivi viene assegnato un nome file 8.3.
  - Sui client SMB, viene visualizzato `test.txt` e `TEST~1.TXT`.
  - ONTAP crea il `TEST~1.TXT` nome del file per differenziare i due file.



Se è stata creata una mappatura dei caratteri utilizzando i comandi di mappatura dei caratteri CIFS di Vserver, una ricerca di Windows che normalmente non fa distinzione tra maiuscole e minuscole può diventare sensibile al maiuscolo/minuscolo. Ciò significa che le ricerche dei nomi file distinguono tra maiuscole e minuscole solo se la mappatura dei caratteri è stata creata e il nome del file sta utilizzando la mappatura dei caratteri.

## Come ONTAP crea i nomi di file e directory

ONTAP crea e mantiene due nomi per i file o le directory in qualsiasi directory che ha accesso da un client SMB: Il nome lungo originale e un nome in formato 8.3.

Per i nomi di file o directory che superano il nome di otto caratteri o il limite di estensione di tre caratteri (per i file), ONTAP genera un nome in formato 8.3 come segue:

- Il nome del file o della directory originale viene troncato a sei caratteri, se il nome supera i sei caratteri.
- Aggiunge una tilde (~) e un numero, da uno a cinque, ai nomi di file o directory che non sono più univoci dopo essere stati troncati.

Se esaurisce i numeri perché ci sono più di cinque nomi simili, crea un nome unico che non ha alcuna relazione con il nome originale.

- Nel caso dei file, l'estensione del nome del file viene troncata a tre caratteri.

Ad esempio, se un client NFS crea un file denominato `specifications.html`, il nome del file di formato 8.3 creato da ONTAP è `specif~1.htm`. Se questo nome esiste già, ONTAP utilizza un numero diverso alla fine del nome del file. Ad esempio, se un client NFS crea un altro file denominato `specifications_new.html`, il formato 8.3 di `specifications_new.html` è `specif~2.htm`.

## Come ONTAP gestisce i nomi di file, directory e qtree multi-byte

A partire da ONTAP 9.5, il supporto per i nomi codificati UTF-8 a 4 byte consente la creazione e la visualizzazione di nomi di file, directory e albero che includono caratteri aggiuntivi Unicode al di fuori del piano multilingua di base (BMP). Nelle versioni precedenti, questi caratteri supplementari non erano visualizzati correttamente negli ambienti multiprotocollo.

Per abilitare il supporto per i nomi codificati UTF-8 a 4 byte, è disponibile un nuovo codice lingua *utf8mb4* per *vserver* e *volume* famiglie di comandi.

- È necessario creare un nuovo volume in uno dei seguenti modi:
- Impostazione del volume `-language` opzione esplicitamente:

```
volume create -language utf8mb4 {...}
```

- Ereditare il volume `-language` Opzione da una SVM creata con o modificata per l'opzione:



```
vserver [create|modify] -language utf8mb4 {...}``volume create {...}
```

- Se si utilizza ONTAP 9.6 e versioni precedenti, non è possibile modificare i volumi esistenti per il supporto di utf8mb4; è necessario creare un nuovo volume utf8mb4-ready e quindi migrare i dati utilizzando strumenti di copia basati su client.

Se si utilizza ONTAP 9.7P1 o versione successiva, è possibile modificare i volumi esistenti per utf8mb4 con una richiesta di supporto. Per ulteriori informazioni, vedere "[È possibile modificare la lingua del volume dopo la creazione in ONTAP?](#)".

È possibile aggiornare le SVM per il supporto di utf8mb4, ma i volumi esistenti conservano i codici lingua originali.



I nomi LUN con caratteri UTF-8 a 4 byte non sono attualmente supportati.

- I dati dei caratteri Unicode sono generalmente rappresentati nelle applicazioni di file system Windows che utilizzano il formato di trasformazione Unicode a 16 bit (UTF-16) e nei file system NFS che utilizzano il formato di trasformazione Unicode a 8 bit (UTF-8).

Nelle release precedenti a ONTAP 9.5, i nomi, inclusi i caratteri supplementari UTF-16 creati dai client Windows, venivano visualizzati correttamente su altri client Windows ma non sono stati tradotti correttamente in UTF-8 per i client NFS. Analogamente, i nomi con caratteri supplementari UTF-8 creati dai client NFS non sono stati tradotti correttamente in UTF-16 per i client Windows.

- Quando si creano nomi di file su sistemi con ONTAP 9.4 o versioni precedenti che contengono caratteri supplementari validi o non validi, ONTAP rifiuta il nome del file e restituisce un errore di nome del file non valido.

Per evitare questo problema, utilizzare solo caratteri BMP nei nomi dei file ed evitare di utilizzare caratteri supplementari oppure eseguire l'aggiornamento a ONTAP 9.5 o versioni successive.

I caratteri Unicode sono consentiti nei nomi qtree.

- È possibile utilizzare il `volume qtree` Command Family o System Manager per impostare o modificare i nomi di qtree.
- I nomi qtree possono includere caratteri multi-byte in formato Unicode, ad esempio caratteri giapponesi e cinesi.
- Nelle versioni precedenti a ONTAP 9.5, erano supportati solo i caratteri BMP (ovvero quelli che potevano essere rappresentati in 3 byte).



Nelle release precedenti a ONTAP 9.5, il percorso di giunzione del volume padre del qtree può contenere nomi di qtree e directory con caratteri Unicode. Il `volume show` Il comando visualizza correttamente questi nomi quando il volume d'origine dispone di un'impostazione della lingua UTF-8. Tuttavia, se la lingua del volume padre non è una delle impostazioni della lingua UTF-8, alcune parti del percorso di giunzione vengono visualizzate utilizzando un nome alternativo NFS numerico.

- Nella versione 9.5 e successive, i caratteri a 4 byte sono supportati nei nomi qtree, a condizione che il qtree si trovi in un volume abilitato per utf8mb4.

## Configurare la mappatura dei caratteri per la conversione dei nomi file SMB sui volumi

I client NFS possono creare nomi di file che contengono caratteri non validi per i client SMB e alcune applicazioni Windows. È possibile configurare la mappatura dei caratteri per la conversione dei nomi file sui volumi per consentire ai client SMB di accedere ai file con nomi NFS che altrimenti non sarebbero validi.

### A proposito di questa attività

Quando i client SMB accedono ai file creati dai client NFS, ONTAP esamina il nome del file. Se il nome non è un nome file SMB valido (ad esempio, se ha un carattere ":" incorporato), ONTAP restituisce il nome file 8.3 che viene mantenuto per ciascun file. Tuttavia, questo causa problemi per le applicazioni che codificano informazioni importanti in nomi di file lunghi.

Pertanto, se si condivide un file tra client su sistemi operativi diversi, è necessario utilizzare caratteri nei nomi dei file validi in entrambi i sistemi operativi.

Tuttavia, se si dispone di client NFS che creano nomi file contenenti caratteri non validi per i client SMB, è possibile definire una mappa che converte i caratteri NFS non validi in caratteri Unicode accettati sia da SMB che da alcune applicazioni Windows. Ad esempio, questa funzionalità supporta le applicazioni CATIA MCAD e Mathematica e altre applicazioni che richiedono questo requisito.

È possibile configurare la mappatura dei caratteri volume per volume.

Quando si configura la mappatura dei caratteri su un volume, è necessario tenere presente quanto segue:

- La mappatura dei caratteri non viene applicata tra i punti di giunzione.

È necessario configurare esplicitamente la mappatura dei caratteri per ciascun volume di giunzione.

- È necessario assicurarsi che i caratteri Unicode utilizzati per rappresentare caratteri non validi o non validi siano caratteri che normalmente non vengono visualizzati nei nomi dei file; in caso contrario, si verificano mappature indesiderate.

Ad esempio, se si tenta di mappare i due punti (:) a un trattino (-) ma il trattino (-) è stato utilizzato correttamente nel nome del file, un client Windows che tenta di accedere a un file denominato "a-b" avrebbe la sua richiesta mappata al nome NFS "a:b" (non il risultato desiderato).

- Dopo aver applicato la mappatura dei caratteri, se la mappatura contiene ancora un carattere Windows non valido, ONTAP torna ai nomi file di Windows 8.3.
- Nelle notifiche FPolicy, nei registri di controllo NAS e nei messaggi di traccia di sicurezza, vengono visualizzati i nomi dei file mappati.
- Quando viene creata una relazione SnapMirror di tipo DP, la mappatura dei caratteri del volume di origine non viene replicata sul volume DP di destinazione.
- Distinzione tra maiuscole e minuscole: Poiché i nomi Windows mappati diventano nomi NFS, la ricerca dei nomi segue la semantica NFS. Ciò include il fatto che le ricerche NFS sono sensibili al maiuscolo/minuscolo. Ciò significa che le applicazioni che accedono alle condivisioni mappate non devono fare affidamento sul comportamento di Windows senza distinzione tra maiuscole e minuscole. Tuttavia, il nome 8.3 è disponibile, senza distinzione tra maiuscole e minuscole.
- Mappature parziali o non valide: Dopo aver mappato un nome da restituire ai client che eseguono l'enumerazione della directory ("dir"), il nome Unicode risultante viene controllato per la validità di Windows. Se il nome contiene ancora caratteri non validi o se non è valido per Windows (ad esempio, termina con "." o vuoto) viene restituito il nome 8.3 invece del nome non valido.

## Fase

### 1. Configurare la mappatura dei caratteri:

```
vserver cifs character-mapping create -vserver vserver_name -volume  
volume_name -mapping mapping_text, ...
```

Il mapping è costituito da un elenco di coppie di caratteri origine-destinazione separate da “:”. I caratteri sono caratteri Unicode immessi utilizzando cifre esadecimali. Ad esempio: 3C:E03C.

Il primo valore di ciascuno `mapping_text` La coppia separata dai due punti è il valore esadecimale del carattere NFS che si desidera convertire, mentre il secondo valore è il valore Unicode utilizzato da SMB. Le coppie di mappatura devono essere univoche (deve esistere una mappatura uno a uno).

#### ◦ Mappatura di origine

La tabella seguente mostra il set di caratteri Unicode consentito per il mapping di origine:

Carattere Unicode	Carattere stampato	Descrizione
0x01-0x19	Non applicabile	Caratteri di controllo non stampabili
0x5C	.	Barra rovesciata
0x3A	:	Due punti
0x2A	*	Asterisco
0x3F	?	Punto interrogativo
0x22	"	Virgoletta
0x3C	<	Inferiore a.
0x3E	>	Maggiore di
0x7C		
Linea verticale	0xB1	±

#### ◦ Mappatura di destinazione

È possibile specificare i caratteri di destinazione nella “Private Use Area” di Unicode nel seguente intervallo: U+E0000...U+F8FF.

## Esempio

Il seguente comando crea un mapping di caratteri per un volume denominato “data” su storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	data	3c:e17c, 3e:f17d, 2a:f745

## Comandi per la gestione delle mappature dei caratteri per la conversione dei nomi file SMB

È possibile gestire la mappatura dei caratteri creando, modificando, visualizzando o eliminando le mappature dei caratteri dei file utilizzate per la conversione dei nomi dei file SMB sui volumi FlexVol.

Se si desidera...	Utilizzare questo comando...
Creare nuove mappature dei caratteri del file	<code>vserver cifs character-mapping create</code>
Visualizza le informazioni sulle mappature dei caratteri del file	<code>vserver cifs character-mapping show</code>
Modificare le mappature dei caratteri del file esistente	<code>vserver cifs character-mapping modify</code>
Eliminare le mappature dei caratteri del file	<code>vserver cifs character-mapping delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Gestire il trunking NFS

### Panoramica del trunking NFS

A partire da ONTAP 9.14.1, i client NFSv4,1 possono sfruttare il trunking di sessione per aprire più connessioni a diverse LIF sul server NFS, aumentando in tal modo la velocità di trasferimento dei dati e fornendo resilienza tramite multipathing.

Il trunking è vantaggioso per l'esportazione di volumi FlexVol in client compatibili con il trunking, in particolare client VMware e Linux, o per NFS su RDMA, TCP o pNFS.

In ONTAP 9.14.1, il trunking è limitato alle LIF in un singolo nodo; il trunking non può estendersi a LIF in più nodi.

I volumi FlexGroup sono supportati per il trunking. Anche se in questo modo è possibile ottenere performance migliori, l'accesso multipath a un volume FlexGroup può essere configurato solo su un singolo nodo.

In questa versione, è supportato solo il trunking di sessione per il multipathing.

## Come utilizzare il trunking

Per sfruttare i vantaggi del multipathing offerti dal trunking, è necessario disporre di una serie di LIF, definite *gruppo trunking*, associate alla SVM contenente un server NFS abilitato al trunking. Le LIF in un gruppo trunking devono avere porte home sullo stesso nodo del cluster e devono risiedere in tali porte home. È consigliabile che tutte le LIF in un gruppo trunking siano membri dello stesso gruppo di failover.

ONTAP supporta fino a 16 connessioni trunked per nodo da un determinato client.

Quando un client esegue l'esportazione da un server abilitato al trunking, specifica un numero di indirizzi IP per le LIF in un gruppo trunking. Una volta che il client si connette alla prima LIF, le LIF aggiuntive vengono aggiunte alla sessione NFSv4,1 e utilizzate per il trunking se conformi ai requisiti del gruppo di trunking. Il client distribuisce quindi le operazioni NFS su più connessioni in base al proprio algoritmo (ad esempio round-robin).

Per ottenere performance ottimali, è necessario configurare il trunking in una SVM dedicata all'esportazione multipath, non all'esportazione single-path. In altre parole, è necessario abilitare il trunking su un server NFS in una SVM le cui esportazioni vengono fornite solo ai client abilitati al trunking.

## Client supportati

Il server ONTAP NFSv4,1 supporta il trunking con qualsiasi client in grado di utilizzare il trunking di sessione NFSv4,1.

I seguenti client sono stati testati con ONTAP 9.14.1:

- VMware - ESXi 7.0U3F e versioni successive
- Linux - Red Hat Enterprise Linux (RHEL) 8,8 e 9,3



Quando il trunking è abilitato su un server NFS, gli utenti che accedono a condivisioni esportate su client NFS che non supportano il trunking potrebbero riscontrare un calo delle prestazioni. Questo perché viene utilizzata solo una connessione TCP per diversi mount delle LIF dati SVM.

## Differenza tra NFS trunking e nconnect

A partire da ONTAP 9.8, la funzionalità nconnect è disponibile per impostazione predefinita quando NFSv4.1 è attivato. Nei client nConnect-capable, un singolo montaggio NFS può avere più connessioni TCP (fino a 16 Gbps) su una singola LIF.

Al contrario, il trunking è la funzionalità *multipathing*, che fornisce più connessioni TCP su LIF multiple. Se si dispone della possibilità di utilizzare schede NIC aggiuntive nell'ambiente, il trunking offre un parallelismo e prestazioni superiori rispetto alle funzionalità di nconnect.

Scopri di più "[nconnettiti](#)."

## Configurare un nuovo server NFS ed esportare per il trunking

### Creare un server NFS abilitato al trunking

A partire da ONTAP 9.14.1, il trunking può essere abilitato sui server NFS. NFSv4,1 è attivato per impostazione predefinita quando vengono creati i server NFS.

## Prima di iniziare

La SVM deve essere:

- supportato da uno storage sufficiente per i requisiti dei dati dei client.
- Abilitato per NFS.
- Dedicato al trunking NFS. Nessun altro client deve essere configurato su di esso.

## Fasi

1. Se non esiste una SVM idonea, creane una:

```
vserver create -vserver svm_name -rootvolume root_volume_name -aggregate  
aggregate_name -rootvolume-security-style unix -language C.UTF-8
```

2. Verificare la configurazione e lo stato della SVM appena creata:

```
vserver show -vserver svm_name
```

Scopri di più ["Creazione di una SVM."](#)

3. Creare il server NFS:

```
vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled  
-v4.1-trunking enabled -v4-id-domain my_domain.com
```

4. Verificare che NFS sia in esecuzione:

```
vserver nfs status -vserver svm_name
```

5. Verificare che NFS sia configurato come desiderato:

```
vserver nfs show -vserver svm_name
```

Scopri di più ["Configurazione del server NFS."](#)

## Al termine

Configurare i seguenti servizi in base alle esigenze:

- ["DNS"](#)
- ["LDAP"](#)
- ["Kerberos"](#)

## Preparare la rete per il trunking

Per sfruttare il trunking NFSv4,1, le LIF di un gruppo trunking devono risiedere sullo stesso nodo e disporre di porte home sullo stesso nodo. Le LIF devono essere configurate in un gruppo di failover sullo stesso nodo.

## A proposito di questa attività

Una mappatura uno a uno di LIF e NIC consente di ottenere il massimo guadagno in termini di prestazioni, ma non è necessaria per abilitare il trunking. L'installazione di almeno due NIC può offrire vantaggi in termini di prestazioni, ma non è necessaria.

È possibile disporre di più gruppi di failover, ma il gruppo di failover per il trunking deve includere solo i file LIFS nel gruppo trunking.

È necessario regolare il gruppo di failover trunking ogni volta che si aggiungono o rimuovono connessioni (e NIC sottostanti) da un gruppo di failover.

### Prima di iniziare

- Se si desidera creare un gruppo di failover, è necessario conoscere i nomi delle porte associate alle schede NIC.
- Le porte devono essere tutte sullo stesso nodo.

### Fasi

1. Verificare i nomi e lo stato delle porte di rete che si intende utilizzare:

```
network port status
```

2. Creare il gruppo di failover:

```
network interface failover-groups create -vserver svm_name -failover-group  
failover_group_name -targets ports_list
```



Non è un requisito per avere un gruppo di failover, ma è vivamente consigliato.

- *svm\_name* È il nome della SVM che contiene il server NFS.
- *ports\_list* è l'elenco delle porte che verranno aggiunte al gruppo di failover.

Le porte vengono aggiunte nel formato *node\_name:port\_number*, ad esempio, *node1:e0c*.

Questo comando crea il gruppo di failover FG3 per SVM VS1 e aggiunge tre porte:

```
network interface failover-groups create -vserver vs1 -failover-group fg3  
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Scopri di più ["gruppi di failover."](#)

3. Se necessario, creare LIF per i membri del gruppo trunking:

```
network interface create -vserver svm_name -lif lif_name -home-node node_name  
-home-port port_name -address IP_address -netmask IP_address [-service-policy  
policy] [-auto-revert {true|false}]
```

- *-home-node* - Il nodo da cui la LIF ritorna quando il comando di revert dell'interfaccia di rete viene eseguito sulla LIF.

È inoltre possibile specificare se il LIF deve ripristinare automaticamente il nodo home e la porta home con *-auto-revert* opzione.

- *-home-port* Indica la porta fisica o logica alla quale la LIF ritorna quando il comando di indirizzamento dell'interfaccia di rete viene eseguito sulla LIF.
- È possibile specificare un indirizzo IP con *-address* e *-netmask* opzioni, non con *-subnet* opzione.

- Quando si assegnano gli indirizzi IP, potrebbe essere necessario configurare un percorso predefinito per un gateway se ci sono client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- `-service-policy` - La politica di servizio per la LIF. Se non viene specificato alcun criterio, viene assegnato automaticamente un criterio predefinito. Utilizzare `network interface service-policy show` per esaminare le politiche di servizio disponibili.
- `-auto-revert` - Consente di specificare se un data LIF viene automaticamente riportato al suo nodo principale in circostanze come l'avvio, modifiche allo stato del database di gestione o quando viene effettuata la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarla su `true` in base ai criteri di gestione della rete nell'ambiente.

Ripetere questo passaggio per ogni LIF nel gruppo trunking.

Viene creato il seguente comando `lif-A` Per SVM `vs1`, sulla porta `e0c` del nodo `cluster1_01`:

```
network interface create -vserver vs1 -lif lif-A -service-policy ??? -home
-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Scopri di più ["Creazione LIF."](#)

4. Verificare che la LIF sia stata creata:

```
network interface show
```

5. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

## Esportare i dati per l'accesso client

Per fornire al client l'accesso alle condivisioni di dati, è necessario creare uno o più volumi e il volume deve disporre di policy di esportazione con almeno una regola.

Requisiti di esportazione client:

- I client Linux devono avere un mount separato e un mount point separato per ogni connessione trunking (vale a dire, per ogni LIF).
- I client VMware richiedono solo un punto di montaggio singolo per un volume esportato, con diverse LIF specificate.

I client VMware richiedono l'accesso root nel criterio di esportazione.

## Fasi

1. Creare una policy di esportazione:

```
vserver export-policy create -vserver svm_name -policyname policy_name
```



Il nome del criterio può contenere fino a 256 caratteri.

2. Verificare che il criterio di esportazione sia stato creato:

```
vserver export-policy show -policyname policy_name
```

### Esempio

I seguenti comandi creano e verificano la creazione di una policy di esportazione denominata exp1 sulla SVM denominata vs1:

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1
```

3. Creare una regola di esportazione e aggiungerla a un criterio di esportazione esistente:

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

Il `-clientmatch` Il parametro deve identificare i client Linux o VMware che supportano il trunking che montano l'esportazione.

Scopri di più ["creazione di regole di esportazione."](#)

4. Creare il volume con un punto di giunzione:

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

Scopri di più ["creazione di volumi."](#)

5. Verificare che il volume sia stato creato con il punto di giunzione desiderato:

```
volume show -vserver svm_name -volume volume_name -junction-path
```

## Creare montaggi client

I client Linux e VMware che supportano il trunking possono montare volumi o condivisioni di dati da un server ONTAP NFSv4,1 abilitato per il trunking.

Quando si immettono i comandi mount sui client, è necessario immettere gli indirizzi IP per ogni LIF nel gruppo trunking.

Scopri di più ["client supportati"](#).

### Requisiti del client Linux

È necessario un punto di montaggio separato per ciascuna connessione nel gruppo trunking.

Montare i volumi esportati con comandi simili ai seguenti:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=16
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=16
```

La versione (`vers`) il valore deve essere 4.1 o versioni successive.

Il `max_connect` il valore corrisponde al numero di connessioni nel gruppo trunking.

### Requisiti del client VMware

È necessaria un'istruzione mount che includa un indirizzo IP per ciascuna connessione nel gruppo trunking.

Montare il datastore esportato con un comando simile al seguente:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Il `-H` i valori corrispondono alle connessioni nel gruppo trunking.

## Adattare le esportazioni NFS esistenti per il trunking

### Adattamento della panoramica delle esportazioni a percorso singolo

È possibile adattare un'esportazione NFSv4,1 a percorso singolo (non trunked) esistente per utilizzare il trunking. I client con funzionalità trunking possono trarre vantaggio da prestazioni migliorate non appena il trunking viene abilitato sul server, a condizione che i prerequisiti del server e del client siano soddisfatti.

L'adattamento di un'esportazione a percorso singolo per il trunking consente di mantenere i set di dati esportati in volumi e SVM esistenti. A tale scopo, è necessario abilitare il trunking sul server NFS, aggiornare la configurazione di rete ed esportarla e rimontare la condivisione esportata sui client.

L'attivazione del trunking ha l'effetto di riavviare il server. I client VMware devono quindi rimontare i datastore esportati, mentre i client Linux devono rimontare i volumi esportati con `max_connect` opzione.

### Abilitare il trunking sul server NFS

Il trunking deve essere esplicitamente attivato sui server NFS. NFSv4,1 è attivato per impostazione predefinita quando vengono creati i server NFS.

Dopo aver attivato il trunking, verificare che i seguenti servizi siano configurati come necessario.

- "DNS"
- "LDAP"
- "Kerberos"

## Fasi

1. Abilitare il trunking e assicurarsi che NFSv4,1 sia abilitato:

```
vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
```

2. Verificare che NFS sia in esecuzione:

```
vserver nfs status -vserver svm_name
```

3. Verificare che NFS sia configurato come desiderato:

```
vserver nfs show -vserver svm_name
```

Scopri di più ["Configurazione del server NFS."](#)

.. Se fornisci client Windows da questa SVM, sposta le condivisioni ed elimina il server.

```
vserver cifs show -vserver svm_name
```

+

```
vserver cifs delete -vserver svm_name
```

## Aggiornare la rete per il trunking

Il trunking NFSv4,1 richiede che le LIF di un gruppo trunking risiedano sullo stesso nodo e dispongano di porte home sullo stesso nodo. Tutte le LIF devono essere configurate in un gruppo di failover sullo stesso nodo.

### A proposito di questa attività

Una mappatura uno a uno di LIF e NIC consente di ottenere il massimo guadagno in termini di prestazioni, ma non è necessaria per abilitare il trunking.

È possibile disporre di più gruppi di failover, ma il gruppo di failover per il trunking deve includere solo questi LIFS nel gruppo trunking.

È necessario regolare il gruppo di failover trunking ogni volta che si aggiungono o rimuovono connessioni (e NIC sottostanti) da un gruppo di failover.

### Prima di iniziare

- Per creare un gruppo di failover, è necessario conoscere i nomi delle porte associate alle schede NIC.
- Le porte devono essere tutte sullo stesso nodo.

## Fasi

1. Verificare i nomi e lo stato delle porte di rete che si intende utilizzare:

```
network port show
```

2. Creare un gruppo di failover trunking o modificarne uno esistente per il trunking:

```
network interface failover-groups create -vserver svm_name -failover-group failover_group_name -targets ports_list
```

```
network interface failover-groups modify -vserver svm_name -failover-group failover_group_name -targets ports_list
```



Non è un requisito per avere un gruppo di failover, ma è vivamente consigliato.

- *svm\_name* È il nome della SVM che contiene il server NFS.
- *ports\_list* è l'elenco delle porte che verranno aggiunte al gruppo di failover.

Le porte vengono aggiunte nel formato *node\_name:port\_number*, ad esempio, *node1:e0c*.

Il comando seguente crea un gruppo di failover *fg3* Per SVM *VS1* e aggiunge tre porte:

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

Scopri di più ["gruppi di failover."](#)

### 3. Creare LIF aggiuntive per i membri del gruppo trunking, se necessario:

```
network interface create -vserver svm_name -lif lif_name -home-node node_name
-home-port port_name -address IP_address -netmask IP_address [-service-policy
policy] [-auto-revert {true|false}]
```

- *-home-node* - Il nodo da cui la LIF ritorna quando il comando di revert dell'interfaccia di rete viene eseguito sulla LIF.

Puoi specificare se la LIF deve tornare automaticamente al nodo home e alla porta home con il *-auto-revert* opzione.

- *-home-port* Indica la porta fisica o logica alla quale la LIF ritorna quando il comando di indirizzamento dell'interfaccia di rete viene eseguito sulla LIF.
- È possibile specificare un indirizzo IP con *-address* e. *-netmask* opzioni.
- Quando si assegnano gli indirizzi IP manualmente (senza usare una subnet), potrebbe essere necessario configurare un percorso predefinito per un gateway se ci sono client o controller di dominio su una subnet IP diversa. La pagina man di creazione di percorsi di rete contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- *-service-policy* - La politica di servizio per la LIF. Se non viene specificato alcun criterio, viene assegnato automaticamente un criterio predefinito. Utilizzare `network interface service-policy show` per esaminare le politiche di servizio disponibili.
- *-auto-revert* - Consente di specificare se un data LIF viene automaticamente riportato al suo nodo principale in circostanze come l'avvio, modifiche allo stato del database di gestione o quando viene effettuata la connessione di rete. **L'impostazione predefinita è false**, ma è possibile impostarla su *true* in base ai criteri di gestione della rete nel proprio ambiente.

Ripetere questo passaggio per ogni LIF aggiuntivo necessario nel gruppo di trunking.

Il seguente comando crea *lif-A* per la SVM *VS1*, sulla porta *e0c* del nodo *cluster1\_01*:

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

Scopri di più ["Creazione LIF."](#)

4. Verificare che la LIF sia stata creata:

```
network interface show
```

5. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

## Modificare l'esportazione dei dati per l'accesso client

Per consentire ai client di sfruttare il trunking per le condivisioni di dati esistenti, potrebbe essere necessario modificare i criteri e le regole di esportazione e i volumi a cui sono collegati. Esistono diversi requisiti di esportazione per i client Linux e i datastore VMware.

Requisiti di esportazione client:

- I client Linux devono avere un mount separato e un mount point separato per ogni connessione trunking (vale a dire, per ogni LIF).

Se si esegue l'aggiornamento a ONTAP 9.14.1 ed è già stato esportato un volume, è possibile continuare a utilizzare tale volume in un gruppo trunking.

- I client VMware richiedono solo un punto di montaggio singolo per un volume esportato, con diverse LIF specificate.

I client VMware richiedono l'accesso root nel criterio di esportazione.

## Fasi

1. Verificare che sia in vigore un criterio di esportazione esistente:

```
vserver export-policy show
```

2. Verificare che le regole dei criteri di esportazione esistenti siano appropriate per la configurazione trunking:

```
vserver export-policy rule show -policyname policy_name
```

In particolare, verificare che `-clientmatch` Parametro identifica correttamente i client Linux o VMware che supportano il trunking che montano l'esportazione.

Se sono necessarie regolazioni, modificare la regola utilizzando `vserver export-policy rule modify` o creare una nuova regola:

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,..." }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

Scopri di più ["creazione di regole di esportazione."](#)

3. Verificare che i volumi esportati esistenti siano online:

```
volume show -vserver svm_name
```

### Ristabilire i montaggi dei client

Per convertire le connessioni client non trunked in connessioni trunked, i mount esistenti sui client Linux e VMware devono essere smontati e rimontati utilizzando le informazioni sulle LIF.

Quando si immettono i comandi mount sui client, è necessario immettere gli indirizzi IP per ogni LIF nel gruppo trunking.

Scopri di più ["client supportati"](#).



L'annullamento del montaggio dei client VMware provoca interruzioni per le macchine virtuali presenti nel datastore. Un'alternativa potrebbe essere creare un nuovo datastore abilitato per il trunking e utilizzare **storage vmotion** per spostare le macchine virtuali dal vecchio datastore al nuovo. Per ulteriori informazioni, consultare la documentazione VMware.

#### Requisiti del client Linux

È necessario un punto di montaggio separato per ciascuna connessione nel gruppo trunking.

Montare i volumi esportati con comandi simili ai seguenti:

```
mount lif1_ip:/vol-test /mnt/test1 -o vers=4.1,max_connect=2
```

```
mount lif2_ip:/vol-test /mnt/test2 -o vers=4.1,max_connect=2
```

Il `vers` il valore deve essere 4.1 o versioni successive.

Il `max_connect` il valore deve corrispondere al numero di connessioni nel gruppo trunking.

#### Requisiti del client VMware

È necessaria un'istruzione mount che includa un indirizzo IP per ciascuna connessione nel gruppo trunking.

Montare il datastore esportato con un comando simile al seguente:

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

Il `-H` i valori devono corrispondere alle connessioni nel gruppo trunking.

## Gestire NFS su RDMA

### NFS su RDMA

NFS su RDMA utilizza adattatori RDMA, che consentono di copiare i dati direttamente tra la memoria del sistema di storage e la memoria del sistema host, eludendo le interruzioni

della CPU e il sovraccarico.

Le configurazioni NFS su RDMA sono progettate per i clienti con carichi di lavoro sensibili alla latenza o a elevata larghezza di banda, come l'apprendimento automatico e l'analisi. NVIDIA ha esteso NFS su RDMA per abilitare GPU Direct Storage (GDS). GDS accelera ulteriormente i carichi di lavoro abilitati alla GPU bypassando la CPU e la memoria principale, utilizzando RDMA per trasferire i dati direttamente tra il sistema di storage e la memoria GPU.

A partire da ONTAP 9.14.1, le configurazioni NFS su RDMA sono supportate per il protocollo NFSv4,1.

A partire da ONTAP 9.10.1, le configurazioni NFS su RDMA sono supportate per il protocollo NFSv4,0 se utilizzato con l'adattatore Mellanox CX-5 o CX-6, che fornisce il supporto per RDMA utilizzando la versione 2 del protocollo RoCE. GDS è supportato solo utilizzando GPU NVIDIA Tesla e Ampere con schede NIC Mellanox e software MOFED.

Il supporto di NFS su RDMA è limitato solo al traffico locale del nodo. FlexVol standard o FlexGroup in cui tutti i componenti si trovano sullo stesso nodo sono supportati e devono essere accessibili da un LIF sullo stesso nodo. Le dimensioni del montaggio NFS superiori a 64k determinano performance instabili con configurazioni NFS su RDMA.

### Requisiti

- I sistemi di storage devono eseguire ONTAP 9.10.1 o versione successiva
  - È possibile configurare NFS su RDMA con Gestione di sistema a partire da ONTAP 9.12.1. In ONTAP 9.10.1 e 9.11.1, è necessario utilizzare la CLI per configurare NFS su RDMA.
- Entrambi i nodi della coppia ha devono essere della stessa versione.
- I controller del sistema storage devono disporre del supporto RDMA

Inizio a ONTAP...	I seguenti controller supportano RDMA...
9.10.1 e versioni successive	<ul style="list-style-type: none"><li>• R400</li><li>• R700</li><li>• R800</li></ul>
ONTAP 9.14.1 e versioni successive	<ul style="list-style-type: none"><li>• AFF C-Series</li><li>• R900</li></ul>

- Appliance di storage configurata con hardware supportato da RDMA (ad esempio Mellanox CX-5 o CX-6).
- Le LIF dei dati devono essere configurate per supportare RDMA.
- I client devono utilizzare schede NIC Mellanox RDMA e software di rete Mellanox OFED (MOFED).



I gruppi di interfacce non sono supportati con NFS su RDMA.

### Cosa succederà

- [Configurare le NIC per NFS su RDMA](#)
- [Configurare LIF per NFS su RDMA](#)
- [Impostazioni NFS per NFS su RDMA](#)

### Informazioni correlate

- ["RDMA"](#)
- [Panoramica del trunking NFS](#)
- ["RFC 7530: Protocollo NFS versione 4"](#)
- ["RFC 8166: Remote Direct Memory Access Transport for Remote procedure Call Version 1"](#)
- ["RFC 8167: Chiamata di procedura remota bidirezionale su porte RPC-over-RDMA"](#)
- ["RFC 8267: Associazione di livello superiore NFS a RPC-over-RDMA versione 1"](#)

## Configurare le NIC per NFS su RDMA

NFS su RDMA richiede la configurazione NIC sia per il sistema client che per la piattaforma di storage.

### Configurazione della piattaforma di storage

Sul server deve essere installato un adattatore RDMA X1148. Se si utilizza una configurazione ha, è necessario disporre di un adattatore X1148 corrispondente sul partner di failover in modo che il servizio RDMA possa continuare durante il failover. La NIC deve essere compatibile con ROCE.

A partire da ONTAP 9.10.1, è possibile visualizzare un elenco di protocolli di offload RDMA con il comando:

```
network port show -rdma-protocols roce
```

### Configurazione del sistema client

I client devono utilizzare schede NIC Mellanox RDMA (ad esempio X1148) e il software di rete Mellanox OFED. Consultare la documentazione di Mellanox per i modelli e le versioni supportate. Sebbene sia possibile collegare direttamente client e server, si consiglia di utilizzare gli switch a causa delle migliori prestazioni di failover con uno switch.

Il client, il server e gli switch e tutte le porte sugli switch devono essere configurati utilizzando frame Jumbo. Assicurarsi inoltre che il controllo di flusso prioritario sia attivo su qualsiasi switch.

Una volta confermata la configurazione, è possibile montare NFS.



## System Manager

È necessario utilizzare ONTAP 9.12.1 o versione successiva per configurare le interfacce di rete con NFS su RDMA utilizzando Gestione di sistema.

### Fasi

1. Controllare se RDMA è supportato. Accedere a **Network > Ethernet Ports** (rete > Porte Ethernet) e selezionare il nodo appropriato nella vista del gruppo. Quando si espande il nodo, osservare il campo **RDMA Protocol** (protocolli RDMA) per una data porta: Il valore **RoCE** indica che RDMA è supportato; un trattino (-) indica che non è supportato.
2. Per aggiungere una VLAN, selezionare **+ VLAN**. Selezionare il nodo appropriato. Nel menu a discesa **Port** (porta), le porte disponibili visualizzano il testo **RoCE Enabled** (abilitato RoCE) se supportano RDMA; se non supportano RDMA, non viene visualizzato alcun testo.
3. Seguire il flusso di lavoro in [Abilitare lo storage NAS per i server Linux utilizzando NFS](#) Per configurare un nuovo server NFS.

Quando si aggiungono interfacce di rete, è possibile selezionare **Usa porte RoCE**. Selezionare questa opzione per tutte le interfacce di rete che si desidera utilizzare NFS su RDMA.

### CLI

1. Controllare se l'accesso RDMA è attivato sul server NFS con il comando:

```
vserver nfs show-vserver SVM_name
```

Per impostazione predefinita, `-rdma` deve essere attivato. In caso contrario, abilitare l'accesso RDMA sul server NFS:

```
vserver nfs modify -vserver SVM_name -rdma enabled
```

2. Montare il client tramite NFSv4.0 su RDMA:
  - a. L'input per il parametro `proto` dipende dalla versione del protocollo IP del server. Se si tratta di IPv4, utilizzare `proto=rdma`. Se si tratta di IPv6, utilizzare `proto=rdma6`.
  - b. Specificare la porta di destinazione NFS come `port=20049` invece della porta standard 2049:

```
mount -o vers=4,minorversion=0,proto=rdma,port=20049 Server_IP_address  
:/volume_path mount_point
```

3. **OPZIONALE:** Se è necessario smontare il client, eseguire il comando `umount mount_path`

## Ulteriori informazioni

- [Creare un server NFS](#)
- [Abilitare lo storage NAS per i server Linux utilizzando NFS](#)

## Configurare LIF per NFS su RDMA

Per utilizzare NFS su RDMA, è necessario configurare le LIF (interfaccia di rete) in modo che siano compatibili con RDMA. Sia la LIF che la sua coppia di failover devono essere in grado di supportare RDMA.

## Creare una nuova LIF

### System Manager

Per creare un'interfaccia di rete per NFS su RDMA con Gestione di sistema, è necessario eseguire ONTAP 9.12.1 o versioni successive.

#### Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare **+ Add**.
3. Quando si seleziona **NFS,SMB/CIFS,S3**, si avrà la possibilità di **utilizzare porte RoCE**. Selezionare la casella di controllo **Usa porte RoCE**.
4. Selezionare la VM di storage e il nodo home. Assegnare un nome. Inserire l'indirizzo IP e la subnet mask.
5. Una volta immessi l'indirizzo IP e la subnet mask, System Manager filtra l'elenco dei domini di trasmissione in base a quelli che dispongono di porte compatibili con RoCE. Selezionare un dominio di trasmissione. È possibile aggiungere un gateway.
6. Selezionare **Salva**.

### CLI

#### Fasi

1. Creare una LIF:

```
network interface create -vserver SVM_name -lif lif_name -service-policy service_policy_name -home-node node_name -home-port port_name {-address IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall -policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

- La politica di servizio deve essere predefinita-data-file o una policy personalizzata che includa il servizio di interfaccia di rete Data-nfs.
- Il `-rdma-protocols` parameter accetta un elenco, che per impostazione predefinita è vuoto. Quando `roce` Viene aggiunto come valore, la LIF può essere configurata solo sulle porte che supportano l'offload RoCE, con conseguenze sulla migrazione e il failover di bot LIF.

## Modificare una LIF

## System Manager

Per creare un'interfaccia di rete per NFS su RDMA con Gestione di sistema, è necessario eseguire ONTAP 9.12.1 o versioni successive.

### Fasi

1. Selezionare **rete > Panoramica > interfacce di rete**.
2. Selezionare **:** > **Modifica** accanto all'interfaccia di rete che si desidera modificare.
3. Selezionare **Use RoCE Ports** (Usa porte RoCE) per attivare NFS su RDMA o deselezionare la casella per disattivarla. Se l'interfaccia di rete si trova su una porta compatibile con RoCE, viene visualizzata una casella di controllo accanto a **Usa porte RoCE**.
4. Modificare le altre impostazioni in base alle necessità.
5. Selezionare **Save** (Salva) per confermare le modifiche.

### CLI

1. È possibile controllare lo stato dei file LIF con `network interface show` comando. La politica di servizio deve includere il servizio di interfaccia di rete dati-nfs. Il `-rdma-protocols` l'elenco deve includere `roce`. Se una di queste condizioni non è vera, modificare la LIF.
2. Per modificare la LIF, eseguire:

```
network interface modify vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```



La modifica di una LIF per richiedere un protocollo di offload specifico quando la LIF non è attualmente assegnata a una porta che supporta tale protocollo genera un errore.

## Migrare una LIF

ONTAP consente inoltre di migrare le interfacce di rete (LIF) per utilizzare NFS su RDMA. Quando si esegue questa migrazione, è necessario assicurarsi che la porta di destinazione sia compatibile con RoCE. A partire da ONTAP 9.12.1, è possibile completare questa procedura in Gestore di sistema. Quando si seleziona una porta di destinazione per l'interfaccia di rete, System Manager stabilisce se le porte sono compatibili con RoCE.

È possibile migrare una LIF a una configurazione NFS su RDMA solo se:

- Si tratta di un'interfaccia di rete NFS RDMA (LIF) ospitata su una porta compatibile con RoCE.
- Si tratta di un'interfaccia di rete NFS TCP (LIF) ospitata su una porta compatibile con RoCE.
- Si tratta di un'interfaccia di rete NFS TCP (LIF) ospitata su una porta non compatibile con RoCE.

Per ulteriori informazioni sulla migrazione di un'interfaccia di rete, fare riferimento a [Migrare una LIF](#).

### Ulteriori informazioni

- [Creare una LIF](#)
- [Creare una LIF](#)

- [Modificare una LIF](#)
- [Migrare una LIF](#)

## Modificare la configurazione NFS

Nella maggior parte dei casi, non sarà necessario modificare la configurazione della VM di storage abilitata NFS per NFS su RDMA.

Tuttavia, se si affrontano problemi relativi ai chip Mellanox e alla migrazione LIF, è necessario aumentare il periodo di tolleranza di blocco NFSv4. Per impostazione predefinita, il periodo di tolleranza è impostato su 45 secondi. A partire da ONTAP 9.10.1, il periodo di tolleranza ha un valore massimo di 180 (secondi).

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Immettere il seguente comando:

```
vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
```

Per ulteriori informazioni su questa attività, vedere [Specifica del periodo di tolleranza del blocco NFSv4](#).

## Configurare SMB con la CLI

### Panoramica della configurazione SMB con la CLI

È possibile utilizzare i comandi CLI di ONTAP 9 per configurare l'accesso del client SMB ai file contenuti in un nuovo volume o qtree in una SVM nuova o esistente.



*SMB* (Server message Block) si riferisce ai dialetti moderni del protocollo CIFS (Common Internet file System). L'interfaccia della riga di comando (CLI) di ONTAP e i tool di gestione di OnCommand sono ancora visibili in *CIFS*.

Attenersi alle seguenti procedure se si desidera configurare l'accesso SMB a un volume o a un qtree nel modo seguente:

- Si desidera utilizzare SMB versione 2 o successiva.
- Si desidera servire solo client SMB, non client NFS (non una configurazione multiprotocollo).
- Per proteggere il nuovo volume verranno utilizzate le autorizzazioni NTFS.
- Si dispone di privilegi di amministratore del cluster, non di amministratore SVM.

Per creare SVM e LIF sono necessari i privilegi di amministratore del cluster. I privilegi di amministratore di SVM sono sufficienti per altre attività di configurazione SMB.

- Si desidera utilizzare la CLI, non System Manager o uno strumento di scripting automatico.

Per utilizzare System Manager per configurare l'accesso multiprotocollo NAS, vedere ["Provisioning dello storage NAS per Windows e Linux utilizzando sia NFS che SMB"](#).

- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.

I dettagli sulla sintassi dei comandi sono disponibili nelle pagine guida CLI e man ONTAP.

Per ulteriori informazioni sulla gamma di funzionalità del protocollo SMB ONTAP, consultare ["Panoramica di riferimento SMB"](#).

### Altri modi per farlo in ONTAP

Per eseguire queste attività con...	Fare riferimento a...
System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive)	<a href="#">"Provisioning dello storage NAS per i server Windows utilizzando SMB"</a>
System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)	<a href="#">"Panoramica della configurazione SMB"</a>

## Workflow di configurazione SMB

La configurazione di SMB implica la valutazione dei requisiti di storage fisico e di rete, quindi la scelta di un workflow specifico dell'obiettivo, la configurazione dell'accesso SMB a una SVM nuova o esistente o l'aggiunta di un volume o qtree a una SVM esistente già completamente configurata per l'accesso SMB.

## Preparazione

### Valutare i requisiti di storage fisico

Prima di eseguire il provisioning dello storage SMB per i client, è necessario assicurarsi che vi sia spazio sufficiente in un aggregato esistente per il nuovo volume. In caso contrario, è possibile aggiungere dischi a un aggregato esistente o creare un nuovo aggregato del tipo desiderato.

### Fasi

1. Visualizzare lo spazio disponibile negli aggregati esistenti: `storage aggregate show`

Se esiste un aggregato con spazio sufficiente, registrare il nome nel foglio di lavoro.

```
cluster::> storage aggregate show
Aggregate      Size Available Used% State  #Vols  Nodes  RAID Status
-----
aggr_0         239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_1         239.0GB   11.13GB   95% online    1 node1  raid_dp,
normal
aggr_2         239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_3         239.0GB   11.13GB   95% online    1 node2  raid_dp,
normal
aggr_4         239.0GB   238.9GB   95% online    5 node3  raid_dp,
normal
aggr_5         239.0GB   239.0GB   95% online    4 node4  raid_dp,
normal

6 entries were displayed.
```

2. Se non sono presenti aggregati con spazio sufficiente, aggiungere dischi a un aggregato esistente utilizzando `storage aggregate add-disks` oppure creare un nuovo aggregato utilizzando il comando `storage aggregate create` comando.

## Valutare i requisiti di rete

Prima di fornire storage SMB ai client, è necessario verificare che la rete sia configurata correttamente per soddisfare i requisiti di provisioning SMB.

### Prima di iniziare

È necessario configurare i seguenti oggetti di rete del cluster:

- Porte fisiche e logiche
- Domini di broadcast
- Subnet (se richieste)
- IPspaces (come richiesto, oltre all'IPSpace predefinito)
- Gruppi di failover (secondo necessità, oltre al gruppo di failover predefinito per ciascun dominio di broadcast)
- Firewall esterni

### Fasi

1. Visualizzare le porte fisiche e virtuali disponibili: `network port show`
  - Quando possibile, utilizzare la porta con la velocità massima per la rete dati.
  - Per ottenere le migliori prestazioni, tutti i componenti della rete dati devono avere la stessa impostazione MTU.
2. Se si intende utilizzare un nome di sottorete per assegnare l'indirizzo IP e il valore della maschera di rete per una LIF, verificare che la subnet esista e che gli indirizzi disponibili siano sufficienti: `network subnet show`

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Le subnet vengono create utilizzando `network subnet create` comando.

3. Visualizzare gli spazi IP disponibili: `network ipspace show`

È possibile utilizzare l'IPSpace predefinito o un IPspace personalizzato.

4. Se si desidera utilizzare gli indirizzi IPv6, verificare che IPv6 sia attivato sul cluster: `network options ipv6 show`

Se necessario, è possibile attivare IPv6 utilizzando `network options ipv6 modify` comando.

## Decidere dove eseguire il provisioning della nuova capacità di storage per PMI

Prima di creare un nuovo volume o qtree SMB, è necessario decidere se posizionarlo in una SVM nuova o esistente e la quantità di configurazione richiesta da SVM. Questa decisione determina il tuo flusso di lavoro.

### Scelte

- Se si desidera eseguire il provisioning di un volume o qtree su una nuova SVM o su una SVM esistente che ha SMB abilitato ma non configurato, completare la procedura descritta in “Configurazione dell'accesso SMB a una SVM” e “aggiunta di capacità di storage a una SVM abilitata per SMB”.

#### Configurazione dell'accesso SMB a una SVM

#### Configurazione dell'accesso del client SMB allo storage condiviso

È possibile scegliere di creare una nuova SVM se si verifica una delle seguenti condizioni:

- Si sta abilitando SMB su un cluster per la prima volta.
- Esistono SVM in un cluster in cui non si desidera abilitare il supporto SMB.
- Si dispone di una o più SVM abilitate per SMB in un cluster e si desidera una delle seguenti connessioni:
  - A una foresta o a un gruppo di lavoro Active Directory diverso.
  - A un server SMB in uno spazio dei nomi isolato (scenario multi-tenancy). È inoltre necessario scegliere questa opzione per eseguire il provisioning dello storage su una SVM esistente con SMB abilitato ma non configurato. Questo potrebbe verificarsi se è stata creata la SVM per l'accesso SAN o se non sono stati attivati protocolli al momento della creazione della SVM.

Dopo aver attivato SMB su SVM, procedere al provisioning di un volume o qtree.

- Se si desidera eseguire il provisioning di un volume o qtree su una SVM esistente completamente configurata per l'accesso SMB, completare la procedura descritta in “aggiunta di capacità di storage a una SVM abilitata per SMB”.

#### Configurazione dell'accesso del client SMB allo storage condiviso

## Foglio di lavoro per la raccolta delle informazioni di configurazione SMB

Il foglio di lavoro di configurazione SMB consente di raccogliere le informazioni necessarie per impostare l'accesso SMB per i client.

È necessario completare una o entrambe le sezioni del foglio di lavoro, a seconda della decisione presa su dove eseguire il provisioning dello storage:

- Se si configura l'accesso SMB a una SVM, completare entrambe le sezioni.

[Configurazione dell'accesso SMB a una SVM](#)

[Configurazione dell'accesso del client SMB allo storage condiviso](#)

- Se si aggiunge capacità di storage a una SVM abilitata per SMB, completare solo la seconda sezione.

[Configurazione dell'accesso del client SMB allo storage condiviso](#)

Le pagine man dei comandi contengono dettagli sui parametri.

### Configurazione dell'accesso SMB a una SVM

#### Parametri per la creazione di una SVM

Questi valori vengono forniti con `vserver create`. Se si sta creando una nuova SVM.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Un nome fornito per la nuova SVM che sia un nome di dominio completo (FQDN) o che segua un'altra convenzione che applica nomi SVM univoci in un cluster.	
<code>-aggregate</code>	Il nome di un aggregato nel cluster con spazio sufficiente per la nuova capacità di storage SMB.	
<code>-rootvolume</code>	Un nome univoco fornito per il volume root SVM.	
<code>-rootvolume-security-style</code>	Utilizzare lo stile di protezione NTFS per SVM.	<code>ntfs</code>
<code>-language</code>	Utilizzare l'impostazione della lingua predefinita in questo flusso di lavoro.	<code>C.UTF-8</code>
<code>ipspace</code>	Opzionale: Gli IPspaces sono spazi di indirizzi IP distinti in cui risiedono le SVM.	

#### Parametri per la creazione di una LIF

Questi valori vengono forniti con `network interface create`. Durante la creazione di LIF.



Campo	Descrizione	Il tuo valore
-lif	Un nome fornito per il nuovo LIF.	
-role	Utilizza il ruolo LIF dei dati in questo flusso di lavoro.	data
-data-protocol	Utilizzare solo il protocollo SMB in questo flusso di lavoro.	cifs
-home-node	Il nodo a cui la LIF restituisce quando <code>network interface revert</code> Viene eseguito sul LIF.	
-home-port	La porta o il gruppo di interfacce a cui LIF restituisce quando <code>network interface revert</code> Viene eseguito sul LIF.	
-address	L'indirizzo IPv4 o IPv6 del cluster che verrà utilizzato per l'accesso ai dati dal nuovo LIF.	
-netmask	La maschera di rete e il gateway per LIF.	
-subnet	Un pool di indirizzi IP. Utilizzato al posto di <code>-address</code> e <code>-netmask</code> per assegnare automaticamente indirizzi e netmask.	
-firewall-policy	Utilizzare la policy predefinita del firewall dati in questo flusso di lavoro.	data
-auto-revert	Facoltativo: Specifica se un LIF dei dati viene automaticamente riportato al nodo principale all'avvio o in altre circostanze. L'impostazione predefinita è <code>false</code> .	

## Parametri per la risoluzione del nome host DNS

Questi valori vengono forniti con `vserver services name-service dns create` Durante la configurazione del DNS.

Campo	Descrizione	Il tuo valore
<code>-domains</code>	Fino a cinque nomi di dominio DNS.	
<code>-name-servers</code>	Fino a tre indirizzi IP per ciascun server dei nomi DNS.	

### Configurazione di un server SMB in un dominio Active Directory

#### Parametri per la configurazione del servizio Time

Questi valori vengono forniti con `cluster time-service ntp server create` quando si configurano i servizi orari.

Campo	Descrizione	Il tuo valore
<code>-server</code>	Il nome host o l'indirizzo IP del server NTP per il dominio Active Directory.	

#### Parametri per la creazione di un server SMB in un dominio Active Directory

Questi valori vengono forniti con `vserver cifs create` Quando si crea un nuovo server SMB e si specificano le informazioni di dominio.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM su cui creare il server SMB.	
<code>-cifs-server</code>	Il nome del server SMB (fino a 15 caratteri).	
<code>-domain</code>	Il nome di dominio completo (FQDN) del dominio Active Directory da associare al server SMB.	
<code>-ou</code>	Facoltativo: L'unità organizzativa all'interno del dominio Active Directory da associare al server SMB. Per impostazione predefinita, questo parametro è impostato su CN=computer.	
<code>-netbios-aliases</code>	Facoltativo: Un elenco di alias NetBIOS, che sono nomi alternativi al nome del server SMB.	

Campo	Descrizione	Il tuo valore
<code>-comment</code>	Facoltativo: Un commento di testo per il server. I client Windows possono visualizzare questa descrizione del server SMB quando esplorano i server della rete.	

### Configurazione di un server SMB in un gruppo di lavoro

#### Parametri per la creazione di un server SMB in un gruppo di lavoro

Questi valori vengono forniti con `vserver cifs create` Quando si crea un nuovo server SMB e si specificano le versioni SMB supportate.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM su cui creare il server SMB.	
<code>-cifs-server</code>	Il nome del server SMB (fino a 15 caratteri).	
<code>-workgroup</code>	Il nome del gruppo di lavoro (fino a 15 caratteri).	
<code>-comment</code>	Facoltativo: Un commento di testo per il server. I client Windows possono visualizzare questa descrizione del server SMB quando esplorano i server della rete.	

#### Parametri per la creazione di utenti locali

Questi valori vengono forniti quando si creano utenti locali utilizzando `vserver cifs users-and-groups local-user create` comando. Sono richiesti per i server SMB nei gruppi di lavoro e opzionali nei domini ad.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della SVM su cui creare l'utente locale.	
<code>-user-name</code>	Il nome dell'utente locale (fino a 20 caratteri).	

Campo	Descrizione	Il tuo valore
-full-name	Facoltativo: Il nome completo dell'utente. Se il nome completo contiene uno spazio, racchiudere il nome completo tra virgolette doppie.	
-description	Facoltativo: Una descrizione per l'utente locale. Se la descrizione contiene uno spazio, racchiudere il parametro tra virgolette.	
-is-account-disabled	Facoltativo: Consente di specificare se l'account utente è attivato o disattivato. Se questo parametro non viene specificato, l'impostazione predefinita prevede l'attivazione dell'account utente.	

### Parametri per la creazione di gruppi locali

Questi valori vengono forniti quando si creano gruppi locali utilizzando `vserver cifs users-and-groups local-group create` comando. Sono opzionali per i server SMB nei domini e nei gruppi di lavoro ad.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM su cui creare il gruppo locale.	
-group-name	Il nome del gruppo locale (fino a 256 caratteri).	
-description	Facoltativo: Una descrizione per il gruppo locale. Se la descrizione contiene uno spazio, racchiudere il parametro tra virgolette.	

### Aggiunta di capacità di storage a una SVM abilitata per SMB

#### Parametri per la creazione di un volume

Questi valori vengono forniti con `volume create` se si sta creando un volume invece di un qtree.

Campo	Descrizione	Il tuo valore
-vserver	Il nome di una SVM nuova o esistente che ospiterà il nuovo volume.	

Campo	Descrizione	Il tuo valore
-volume	Un nome descrittivo univoco fornito per il nuovo volume.	
-aggregate	Il nome di un aggregato nel cluster con spazio sufficiente per il nuovo volume SMB.	
-size	Un numero intero fornito per le dimensioni del nuovo volume.	
-security-style	USA lo stile di sicurezza NTFS per questo flusso di lavoro.	ntfs
-junction-path	Posizione sotto root (/) dove deve essere montato il nuovo volume.	

### Parametri per la creazione di un qtree

Questi valori vengono forniti con `volume qtree create` se si sta creando un qtree invece di un volume.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM su cui risiede il volume contenente il qtree.	
-volume	Il nome del volume che conterrà il nuovo qtree.	
-qtree	Un nome descrittivo univoco fornito per il nuovo qtree, massimo 64 caratteri.	
-qtree-path	L'argomento del percorso qtree nel formato <code>/vol/volume_name/qtree_name\&gt;</code> può essere specificato invece di specificare volume e qtree come argomenti separati.	

### Parametri per la creazione di condivisioni SMB

Questi valori vengono forniti con `vserver cifs share create` comando.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM su cui creare la condivisione SMB.	

Campo	Descrizione	Il tuo valore
-share-name	Il nome della condivisione SMB che si desidera creare (fino a 256 caratteri).	
-path	Il nome del percorso della condivisione SMB (fino a 256 caratteri). Questo percorso deve esistere in un volume prima di creare la condivisione.	
-share-properties	Facoltativo: Un elenco delle proprietà di condivisione. Le impostazioni predefinite sono oplocks, browsable, changenotify, e. show-previous-versions.	
-comment	Facoltativo: Un commento di testo per il server (fino a 256 caratteri). I client Windows possono visualizzare questa descrizione della condivisione SMB durante la navigazione in rete.	

### Parametri per la creazione di elenchi di controllo degli accessi di condivisione SMB (ACL)

Questi valori vengono forniti con `vserver cifs share access-control create` comando.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della SVM su cui creare l'ACL SMB.	
-share	Il nome della condivisione SMB su cui creare.	
-user-group-type	Il tipo di utente o gruppo da aggiungere all'ACL della condivisione. Il tipo predefinito è windows	windows
-user-or-group	L'utente o il gruppo da aggiungere all'ACL della condivisione. Se si specifica il nome utente, è necessario includere il dominio dell'utente nel formato "'domain\' nomeutente'".	

Campo	Descrizione	Il tuo valore
-permission	Specifica le autorizzazioni per l'utente o il gruppo.	`[ No_access
Read	Change	Full_Control ]`

## Configurare l'accesso SMB a una SVM

### Configurare l'accesso SMB a una SVM

Se non si dispone già di una SVM configurata per l'accesso al client SMB, è necessario creare e configurare una nuova SVM o configurare una SVM esistente. La configurazione di SMB implica l'apertura dell'accesso al volume root SVM, la creazione di un server SMB, la creazione di una LIF, l'abilitazione della risoluzione dei nomi host, la configurazione dei servizi dei nomi e, se lo si desidera, Attivazione della sicurezza Kerberos.

### Creare una SVM

Se non si dispone già di almeno una SVM in un cluster per fornire l'accesso ai dati ai client SMB, è necessario crearne una.

#### Prima di iniziare

- A partire da ONTAP 9.13.1, è possibile impostare una capacità massima per una VM di storage. È inoltre possibile configurare gli avvisi quando SVM si avvicina a un livello di capacità di soglia. Per ulteriori informazioni, vedere [Gestire la capacità SVM](#).

#### Fasi

1. Creare una SVM: `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
  - Utilizzare l'impostazione NTFS per `-rootvolume-security-style` opzione.
  - Utilizzare il C.UTF-8 predefinito `-language` opzione.
  - Il `ipspace` l'impostazione è facoltativa.

2. Verificare la configurazione e lo stato della SVM appena creata: `vserver show -vserver vserver_name`

Il `Allowed Protocols` Il campo deve includere CIFS. È possibile modificare questo elenco in un secondo momento.

Il `Vserver Operational State` il campo deve visualizzare `running` stato. Se viene visualizzato il `initializing` indica che alcune operazioni intermedie, ad esempio la creazione del volume root, non sono riuscite ed è necessario eliminare la SVM e ricrearla.

### Esempi

Il seguente comando crea una SVM per l'accesso ai dati in IPspace `ipspaceA`:

```
cluster1::> vservers create -vservers vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA
```

```
[Job 2059] Job succeeded:
Vserver creation completed
```

Il seguente comando indica che è stata creata una SVM con un volume root di 1 GB, che è stata avviata automaticamente e si trova in `running` stato. Il volume root dispone di un criterio di esportazione predefinito che non include alcuna regola, pertanto il volume root non viene esportato al momento della creazione.

```
cluster1::> vservers show -vservers vs1.example.com
Vserver: vs1.example.com
Vserver Type: data
Vserver Subtype: default
Vserver UUID: b8375669-19b0-11e5-b9d1-00a0983d9736
Root Volume: root_vs1
Aggregate: aggr1
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: C.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
Disallowed Protocols: -
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspaceA
```



A partire da ONTAP 9.13.1, è possibile impostare un modello di gruppo di policy QoS adattivo, applicando un limite di throughput e di soffitto ai volumi nella SVM. È possibile applicare questo criterio solo dopo aver creato la SVM. Per ulteriori informazioni su questo processo, vedere [Impostare un modello di gruppo di criteri adattativi](#).

## Verificare che il protocollo SMB sia attivato su SVM

Prima di poter configurare e utilizzare SMB su SVM, è necessario verificare che il



protocollo sia attivato.

### A proposito di questa attività

Questa operazione viene generalmente eseguita durante l'installazione di SVM, ma se il protocollo non è stato attivato durante l'installazione, è possibile attivarlo in un secondo momento utilizzando `vserver add-protocols` comando.



Una volta creato, non è possibile aggiungere o rimuovere un protocollo da un LIF.

È inoltre possibile disattivare i protocolli sulle SVM utilizzando `vserver remove-protocols` comando.

### Fasi

1. Controllare quali protocolli sono attualmente attivati e disattivati per SVM: `vserver show -vserver vserver_name -protocols`

È inoltre possibile utilizzare `vserver show-protocols` Per visualizzare i protocolli attualmente abilitati su tutte le SVM nel cluster.

2. Se necessario, attivare o disattivare un protocollo:

- Per attivare il protocollo SMB: `vserver add-protocols -vserver vserver_name -protocols cifs`
- Per disattivare un protocollo: `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`

3. Verificare che i protocolli attivati e disattivati siano stati aggiornati correttamente: `vserver show -vserver vserver_name -protocols`

### Esempio

Il seguente comando visualizza i protocolli attualmente attivati e disattivati (consentiti e non consentiti) sulla SVM denominata vs1:

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols           Disallowed Protocols
-----
vs1.example.com   cifs                        nfs, fcp, iscsi, ndmp
```

Il seguente comando consente l'accesso tramite SMB aggiungendo `cifs` All'elenco dei protocolli abilitati sulla SVM denominato vs1:

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

### Aprire la policy di esportazione del volume root SVM

Il criterio di esportazione predefinito del volume root SVM deve includere una regola per consentire a tutti i client l'accesso aperto tramite SMB. Senza tale regola, a tutti i client SMB viene negato l'accesso a SVM e ai relativi volumi.

## A proposito di questa attività

Quando viene creata una nuova SVM, viene creata automaticamente una policy di esportazione predefinita (chiamata predefinita) per il volume root della SVM. È necessario creare una o più regole per il criterio di esportazione predefinito prima che i client possano accedere ai dati sulla SVM.

Verificare che tutti gli accessi SMB siano aperti nel criterio di esportazione predefinito e, in seguito, limitare l'accesso ai singoli volumi creando policy di esportazione personalizzate per singoli volumi o qtree.

## Fasi

1. Se si utilizza una SVM esistente, controllare il criterio di esportazione del volume root predefinito: `vserver export-policy rule show`

L'output del comando dovrebbe essere simile a quanto segue:

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                Vserver: vs1.example.com
                                Policy Name: default
                                Rule Index: 1
                                Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                                RO Access Rule: any
                                RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                                Superuser Security Types: any
                                Honor SetUID Bits in SETATTR: true
                                Allow Creation of Devices: true
```

Se esiste una regola di questo tipo che consente l'accesso aperto, questa attività è completa. In caso contrario, passare alla fase successiva.

2. Creare una regola di esportazione per il volume root SVM: `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. Verificare la creazione della regola utilizzando `vserver export-policy rule show` comando.

## Risultati

Qualsiasi client SMB può ora accedere a qualsiasi volume o qtree creato su SVM.

## Creare una LIF

LIF è un indirizzo IP associato a una porta fisica o logica. In caso di guasto di un componente, una LIF può eseguire il failover o essere migrata su una porta fisica diversa, continuando così a comunicare con la rete.

## Prima di iniziare

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore `up` stato.

- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando `network subnet create` comando.

- Il meccanismo per specificare il tipo di traffico gestito da una LIF è stato modificato. Per ONTAP 9.5 e versioni precedenti, i LIF utilizzavano i ruoli per specificare il tipo di traffico che gestirebbe. A partire da ONTAP 9.6, le LIF utilizzano le policy di servizio per specificare il tipo di traffico che gestirebbe.

### A proposito di questa attività

- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster utilizzando `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).
- A partire da ONTAP 9.7, se sono già presenti altre LIF per la SVM nella stessa sottorete, non è necessario specificare la porta home della LIF. ONTAP sceglie automaticamente una porta casuale sul nodo principale specificato nello stesso dominio di trasmissione delle altre LIF già configurate nella stessa sottorete.

### Fasi

#### 1. Creare una LIF:

```
network interface create -vserver vservice_name -lif lif_name -role data -data
-protocol cifs -home-node node_name -home-port port_name {-address IP_address
-netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
-revert {true|false}
```

#### ONTAP 9.5 e versioni precedenti

```
`network interface create -vserver vservice_name -lif lif_name -role data -data-protocol cifs -home-node
node_name -home-port port_name {-address IP_address -netmask IP_address
-subnet-name subnet_name} -firewall-policy data -auto-revert {true
false}`
```

#### ONTAP 9.6 e versioni successive

```
`network interface create -vserver vservice_name -lif lif_name -service-policy service_policy_name -home
-node node_name -home-port port_name {-address IP_address -netmask IP_address
-subnet-name subnet_name} -firewall-policy data -auto-revert {true
false}`
```

- Il `-role` Il parametro non è necessario quando si crea una LIF utilizzando una politica di servizio (a partire da ONTAP 9.6).
- Il `-data-protocol` Il parametro non è necessario quando si crea una LIF utilizzando una politica di servizio (a partire da ONTAP 9.6). Quando si utilizza ONTAP 9,5 e versioni precedenti, il `-data-protocol` Il parametro deve essere specificato al momento della creazione della LIF e non può essere modificato in seguito senza distruggere e ricreare la LIF dei dati.

- `-home-node` È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

È inoltre possibile specificare se il LIF deve ripristinare automaticamente il nodo home e la porta home con `-auto-revert` opzione.

- `-home-port` È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
- È possibile specificare un indirizzo IP con `-address` e. `-netmask` oppure attivare l'allocazione da una subnet con `-subnet_name` opzione.
- Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene automaticamente aggiunto un percorso predefinito a tale gateway.
- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- Per `-firewall-policy` utilizzare lo stesso valore predefinito `data` Come ruolo LIF.

Se lo si desidera, è possibile creare e aggiungere un criterio firewall personalizzato in un secondo momento.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

- `-auto-revert` Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `false` in base alle policy di gestione della rete nel proprio ambiente.

## 2. Verificare che la LIF sia stata creata correttamente:

```
network interface show
```

## 3. Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

## Esempi

Il seguente comando crea una LIF e specifica i valori dell'indirizzo IP e della maschera di rete utilizzando `-address` e. `-netmask` parametri:

```
network interface create -vserver vs1.example.com -lif datalif1 -role data  
-data-protocol cifs -home-node node-4 -home-port elc -address 192.0.2.145  
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

Il seguente comando crea una LIF e assegna i valori dell'indirizzo IP e della maschera di rete dalla subnet specificata (denominata client1\_sub):

```
network interface create -vserver vs3.example.com -lif datalif3 -role data  
-data-protocol cifs -home-node node-3 -home-port elc -subnet-name  
client1_sub -firewall-policy data -auto-revert true
```

Il seguente comando mostra tutti i LIF nel cluster-1. Data LIF datalif1 e datalif3 sono configurati con indirizzi IPv4 e datalif4 è configurato con un indirizzo IPv6:

```
network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
cluster-1					
true	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
node-1					
true	clus1	up/up	192.0.2.12/24	node-1	e0a
true	clus2	up/up	192.0.2.13/24	node-1	e0b
true	mgmt1	up/up	192.0.2.68/24	node-1	e1a
node-2					
true	clus1	up/up	192.0.2.14/24	node-2	e0a
true	clus2	up/up	192.0.2.15/24	node-2	e0b
true	mgmt1	up/up	192.0.2.69/24	node-2	e1a
vs1.example.com					
true	datalif1	up/down	192.0.2.145/30	node-1	e1c
vs3.example.com					
true	datalif3	up/up	192.0.2.146/30	node-2	e0c
true	datalif4	up/up	2001::2/64	node-2	e0c
5 entries were displayed.					

Il comando seguente mostra come creare una LIF dati NAS assegnata a default-data-files politica di servizio:

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport e0d -service-policy default-data-files -subnet-name ipspace1
```

### Abilitare il DNS per la risoluzione del nome host

È possibile utilizzare `vserver services name-service dns` Per abilitare il DNS su una SVM e configurarlo per l'utilizzo del DNS per la risoluzione dei nomi host. I nomi host

vengono risolti utilizzando server DNS esterni.

**Prima di iniziare**

Per la ricerca dei nomi host, è necessario che sia disponibile un server DNS a livello di sito.

È necessario configurare più server DNS per evitare un singolo punto di errore. Il `vserver services name-service dns create` Viene visualizzato un messaggio di avviso se si immette un solo nome server DNS.

**A proposito di questa attività**

La *Guida alla gestione della rete* contiene informazioni sulla configurazione del DNS dinamico sulla SVM.

**Fasi**

- 1. Abilitare il DNS sulla SVM: `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

Il seguente comando abilita i server DNS esterni su SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```



A partire da ONTAP 9.2, la `vserver services name-service dns create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non riesce a contattare il server dei nomi.

- 2. Visualizzare le configurazioni del dominio DNS utilizzando `vserver services name-service dns show` comando. ``

Il seguente comando visualizza le configurazioni DNS per tutte le SVM nel cluster:

```
vserver services name-service dns show
```

Vserver	State	Domains	Name Servers
cluster1	enabled	example.com	192.0.2.201, 192.0.2.202
vs1.example.com	enabled	example.com	192.0.2.201, 192.0.2.202

Il seguente comando visualizza informazioni dettagliate sulla configurazione DNS per SVM vs1:

```
vserver services name-service dns show -vserver vs1.example.com
Vserver: vs1.example.com
Domains: example.com
Name Servers: 192.0.2.201, 192.0.2.202
Enable/Disable DNS: enabled
Timeout (secs): 2
Maximum Attempts: 1
```

3. Convalidare lo stato dei server dei nomi utilizzando `vserver services name-service dns check` comando.

Il `vserver services name-service dns check` Il comando è disponibile a partire da ONTAP 9.2.

```
vserver services name-service dns check -vserver vs1.example.com
```

Vserver	Name Server	Status	Status Details
-----	-----	-----	
vs1.example.com	10.0.0.50	up	Response time (msec): 2
vs1.example.com	10.0.0.51	up	Response time (msec): 2

## Configurare un server SMB in un dominio Active Directory

### Configurare i servizi di gestione dell'orario

Prima di creare un server SMB in un controller di dominio attivo, è necessario assicurarsi che il tempo del cluster e quello dei controller di dominio del dominio a cui il server SMB appartiene corrispondano entro cinque minuti.

#### A proposito di questa attività

È necessario configurare i servizi NTP del cluster in modo che utilizzino gli stessi server NTP per la sincronizzazione dell'ora utilizzati dal dominio Active Directory.

A partire da ONTAP 9.5, è possibile configurare il server NTP con autenticazione simmetrica.

#### Fasi

1. Configurare i servizi di gestione del tempo utilizzando `cluster time-service ntp server create` comando.
  - Per configurare i servizi temporali senza autenticazione simmetrica, immettere il seguente comando:  
`cluster time-service ntp server create -server server_ip_address`
  - Per configurare i servizi temporali con autenticazione simmetrica, immettere il seguente comando:  
`cluster time-service ntp server create -server server_ip_address -key-id key_id`  
`cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`




2. Verificare che i servizi di orario siano impostati correttamente utilizzando `cluster time-service ntp server show` comando.


```
cluster time-service ntp server show
```

Server	Version
-----	-----
10.10.10.1	auto
10.10.10.2	auto

#### Comandi per la gestione dell'autenticazione simmetrica sui server NTP

A partire da ONTAP 9.5, è supportato il protocollo NTP (Network Time Protocol) versione 3. NTPv3 include l'autenticazione simmetrica utilizzando chiavi SHA-1 che aumenta la sicurezza della rete.

A tal fine...	Utilizzare questo comando...
Configurare un server NTP senza autenticazione simmetrica	<code>cluster time-service ntp server create -server server_name</code>
Configurare un server NTP con autenticazione simmetrica	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Abilitare l'autenticazione simmetrica per un server NTP esistente. È possibile modificare il server NTP esistente per abilitare l'autenticazione aggiungendo l'ID chiave richiesto.	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
Configurare una chiave NTP condivisa	<div><code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code></div> <div> Le chiavi condivise sono indicate da un ID. L'ID, il tipo e il valore devono essere identici sia sul nodo che sul server NTP</div>
Configurare un server NTP con un ID chiave sconosciuto	<code>cluster time-service ntp server create -server server_name -key-id key_id</code>

A tal fine...	Utilizzare questo comando...
Configurare un server con un ID chiave non configurato sul server NTP.	<pre>cluster time-service ntp server create -server server_name -key-id key_id</pre> <div>  <p>L'ID, il tipo e il valore della chiave devono essere identici all'ID, al tipo e al valore della chiave configurati sul server NTP.</p> </div>
Disattiva autenticazione simmetrica	<pre>cluster time-service ntp server modify -server server_name -authentication disabled</pre>

### Creare un server SMB in un dominio Active Directory

È possibile utilizzare `vserver cifs create` Per creare un server SMB su SVM e specificare il dominio Active Directory (ad) a cui appartiene.

#### Prima di iniziare

Le SVM e le LIF utilizzate per la distribuzione dei dati devono essere state configurate per consentire il protocollo SMB. Le LIF devono essere in grado di connettersi ai server DNS configurati sulla SVM e a un domain controller ad del dominio a cui si desidera accedere al server SMB.

Qualsiasi utente autorizzato a creare account di computer nel dominio ad a cui si sta entrando nel server SMB può creare il server SMB su SVM. Questo può includere utenti di altri domini.

A partire da ONTAP 9.7, l'amministratore ad può fornire un URI a un file keytab in alternativa a un nome e una password a un account Windows con privilegi. Quando si riceve l'URI, includerlo in `-keytab-uri` con il `vserver cifs` comandi.

#### A proposito di questa attività

Quando si crea un server SMB in un dominio di Activity Directory:

- Quando si specifica il dominio, è necessario utilizzare il nome di dominio completo (FQDN).
- L'impostazione predefinita prevede l'aggiunta dell'account della macchina server SMB all'oggetto CN=computer di Active Directory.
- È possibile scegliere di aggiungere il server SMB a un'unità organizzativa (OU) diversa utilizzando `-ou` opzione.
- È possibile scegliere di aggiungere un elenco delimitato da virgole di uno o più alias NetBIOS (fino a 200) per il server SMB.

La configurazione degli alias NetBIOS per un server SMB può essere utile quando si consolidano i dati da altri file server al server SMB e si desidera che il server SMB risponda ai nomi dei server originali.

Il `vserver cifs` le pagine man contengono ulteriori parametri opzionali e requisiti di denominazione.



A partire da ONTAP 9.1, è possibile abilitare SMB versione 2.0 per la connessione a un controller di dominio (DC). Questa operazione è necessaria se SMB 1.0 è stato disattivato nei controller di dominio. A partire da ONTAP 9.2, SMB 2.0 è attivato per impostazione predefinita.

A partire da ONTAP 9.8, è possibile specificare che le connessioni ai controller di dominio siano crittografate. ONTAP richiede la crittografia per le comunicazioni del controller di dominio quando `-encryption -required-for-dc-connection` l'opzione è impostata su `true`; il valore predefinito è `false`. Quando l'opzione è impostata, per le connessioni ONTAP-DC verrà utilizzato solo il protocollo SMB3, in quanto la crittografia è supportata solo da SMB3. .

**"Gestione delle PMI"** Contiene ulteriori informazioni sulle opzioni di configurazione del server SMB.

## Fasi

1. Verificare che SMB sia concesso in licenza sul cluster: `system license show -package cifs`

La licenza SMB è inclusa con **"ONTAP uno"**. Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.

Non è richiesta una licenza CIFS se il server SMB viene utilizzato solo per l'autenticazione.

2. Creare il server SMB in un dominio ad: `vserver cifs create -vserver vserver_name -cifs -server smb_server_name -domain FQDN [-ou organizational_unit] [-netbios-aliases NetBIOS_name, ...] [-keytab-uri {(ftp|http)://hostname|IP_address}] [-comment text]`

Quando si entra in un dominio, il completamento di questo comando potrebbe richiedere alcuni minuti.

Il seguente comando crea il server SMB "smb\_server01" nel dominio "example.com":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
smb_server01 -domain example.com
```

Il seguente comando crea il server SMB "smb\_server02" nel dominio "mydomain.com" e autentica l'amministratore ONTAP con un file keytab:

```
cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server  
smb_server02 -domain mydomain.com -keytab-uri  
http://admin.mydomain.com/ontap1.keytab
```

3. Verificare la configurazione del server SMB utilizzando `vserver cifs show` comando.

In questo esempio, l'output del comando mostra che un server SMB denominato "SMB\_SERVER01" è stato creato su SVM vs1.example.com ed è stato Unito al dominio "example.com".

```
cluster1::> vserver cifs show -vserver vs1
```

```
Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: -
```

4. Se lo si desidera, attivare la comunicazione crittografata con il controller di dominio (ONTAP 9.8 e versioni successive): `vserver cifs security modify -vserver svm_name -encryption-required -for-dc-connection true`

### Esempi

Il seguente comando crea un server SMB denominato “smb\_server02” su SVM vs2.example.com nel dominio “example.com”. L’account del computer viene creato nel contenitore “OU=eng,OU=corp,DC=example,DC=com”. Al server SMB viene assegnato un alias NetBIOS.

```
cluster1::> vserver cifs create -vserver vs2.example.com -cifs-server
smb_server02 -domain example.com -ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01
```

```
cluster1::> vserver cifs show -vserver vs1

Vserver: vs2.example.com
CIFS Server NetBIOS Name: SMB_SERVER02
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description: -
List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

Il seguente comando consente a un utente di un dominio diverso, in questo caso un amministratore di un dominio attendibile, di creare un server SMB denominato “smb\_server03” su SVM vs3.example.com. Il `-domain` Option specifica il nome del dominio principale (specificato nella configurazione DNS) in cui si desidera creare il server SMB. Il `username` consente di specificare l’amministratore del dominio attendibile.

- Dominio domestico: example.com
- Dominio attendibile: trust.lab.com
- Nome utente del dominio trusted: Administrator1

```
cluster1::> vsyncer cifs create -vsyncer vs3.example.com -cifs-server  
smb_server03 -domain example.com
```

```
Username: Administrator1@trust.lab.com
```

```
Password: . . .
```

### Creare file keytab per l'autenticazione SMB

A partire da ONTAP 9.7, ONTAP supporta l'autenticazione SVM con server Active Directory (ad) utilizzando file keytab. Gli amministratori DEGLI ANNUNCI generano un file keytab e lo rendono disponibile agli amministratori di ONTAP come URI (Uniform Resource Identifier), che viene fornito quando `vsyncer cifs` I comandi richiedono l'autenticazione Kerberos con il dominio ad.

Gli amministratori DEGLI ANNUNCI possono creare i file keytab utilizzando Windows Server standard `ktpass` comando. Il comando deve essere eseguito sul dominio primario in cui è richiesta l'autenticazione. Il `ktpass` il comando può essere utilizzato per generare i file keytab solo per gli utenti del dominio primario; le chiavi generate utilizzando gli utenti del dominio trusted non sono supportate.

I file keytab vengono generati per specifici utenti amministratori di ONTAP. Se la password dell'utente amministratore non viene modificata, le chiavi generate per il tipo di crittografia e il dominio specifico non verranno modificate. Pertanto, è necessario un nuovo file keytab ogni volta che viene modificata la password dell'utente amministratore.

Sono supportati i seguenti tipi di crittografia:

- AES256-SHA1
- DES-CBC-MD5



ONTAP non supporta il tipo di crittografia DES-CBC-CRC.

- RC4-HMAC

AES256 è il tipo di crittografia più elevato e deve essere utilizzato se abilitato sul sistema ONTAP.

I file keytab possono essere generati specificando la password admin o utilizzando una password generata casualmente. Tuttavia, in qualsiasi momento è possibile utilizzare una sola opzione di password, poiché sul server ad è necessaria una chiave privata specifica per l'utente amministratore per decifrare le chiavi all'interno del file keytab. Qualsiasi modifica della chiave privata per un amministratore specifico invaliderà il file keytab.

### Configurare un server SMB in un gruppo di lavoro

#### Configurare un server SMB in una panoramica del gruppo di lavoro

L'impostazione di un server SMB come membro di un gruppo di lavoro consiste nella creazione del server SMB e quindi nella creazione di utenti e gruppi locali.

È possibile configurare un server SMB in un gruppo di lavoro quando l'infrastruttura di dominio Microsoft Active Directory non è disponibile.

Un server SMB in modalità workgroup supporta solo l'autenticazione NTLM e non l'autenticazione Kerberos.

### Creare un server SMB in un gruppo di lavoro

È possibile utilizzare `vserver cifs create` Per creare un server SMB sulla SVM e specificare il gruppo di lavoro a cui appartiene.

#### Prima di iniziare

Le SVM e le LIF utilizzate per la distribuzione dei dati devono essere state configurate per consentire il protocollo SMB. Le LIF devono essere in grado di connettersi ai server DNS configurati sulla SVM.

#### A proposito di questa attività

I server SMB in modalità workgroup non supportano le seguenti funzionalità SMB:

- Protocollo di controllo SMB3
- Condivisioni SMB3 CA
- SQL su SMB
- Reindirizzamento cartelle
- Profili roaming
- Oggetto Criteri di gruppo (GPO)
- Servizio Volume Snapshot (VSS)

Il `vserver cifs` le pagine man contengono ulteriori parametri di configurazione opzionali e requisiti di denominazione.

#### Fasi

1. Verificare che SMB sia concesso in licenza sul cluster: `system license show -package cifs`

La licenza SMB è inclusa con "ONTAP uno". Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.

Non è richiesta una licenza CIFS se il server SMB viene utilizzato solo per l'autenticazione.

2. Creare il server SMB in un gruppo di lavoro: `vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment text]`

Il seguente comando crea il server SMB "smb\_server01" nel gruppo di lavoro "workgroup01":

```
cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server  
SMB_SERVER01 -workgroup workgroup01
```

3. Verificare la configurazione del server SMB utilizzando `vserver cifs show` comando.

Nell'esempio seguente, l'output del comando mostra che un server SMB denominato "smb\_server01" è stato creato su SVM vs1.example.com nel gruppo di lavoro "workgroup01":

```
cluster1::> vserver cifs show -vserver vs0

Vserver: vs1.example.com
CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
Fully Qualified Domain Name: -
Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
Workgroup Name: workgroup01
Authentication Style: workgroup
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: -
```

### Al termine

Per un server CIFS in un gruppo di lavoro, è necessario creare utenti locali e, facoltativamente, gruppi locali su SVM.

### Informazioni correlate

["Gestione delle PMI"](#)

### Creare account utente locali

È possibile creare un account utente locale da utilizzare per autorizzare l'accesso ai dati contenuti nella SVM tramite una connessione SMB. È inoltre possibile utilizzare account utente locali per l'autenticazione quando si crea una sessione SMB.

### A proposito di questa attività

La funzionalità utente locale viene attivata per impostazione predefinita quando viene creata la SVM.

Quando si crea un account utente locale, è necessario specificare un nome utente e la SVM a cui associare l'account.

Il `vserver cifs users-and-groups local-user` le pagine man contengono dettagli sui parametri opzionali e sui requisiti di denominazione.

### Fasi

1. Creare l'utente locale: `vserver cifs users-and-groups local-user create -vserver vserver_name -user-name user_name optional_parameters`

Potrebbero essere utili i seguenti parametri opzionali:

- ° `-full-name`

Il nome completo dell'utente.

- ° `-description`

Una descrizione per l'utente locale.

◦ `-is-account-disabled {true|false}`

Specifica se l'account utente è attivato o disattivato. Se questo parametro non viene specificato, l'impostazione predefinita prevede l'attivazione dell'account utente.

Il comando richiede la password dell'utente locale.

2. Immettere una password per l'utente locale, quindi confermarla.
3. Verificare che l'utente sia stato creato correttamente: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Esempio

Nell'esempio seguente viene creato un utente locale "SMB\_SERVER01 `Ssue", con il nome completo "ue Chang", associato a SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                               Full Name  Description
-----  -
vs1      SMB_SERVER01\Administrator                 Built-in administrator
account
vs1      SMB_SERVER01\sue                           Sue Chang
```

### Creare gruppi locali

È possibile creare gruppi locali che possono essere utilizzati per autorizzare l'accesso ai dati associati alla SVM tramite una connessione SMB. È inoltre possibile assegnare privilegi che definiscono i diritti o le funzionalità di un membro del gruppo.

#### A proposito di questa attività

La funzionalità del gruppo locale viene attivata per impostazione predefinita quando viene creata la SVM.

Quando si crea un gruppo locale, è necessario specificare un nome per il gruppo e la SVM a cui associare il gruppo. È possibile specificare un nome di gruppo con o senza il nome di dominio locale ed è possibile specificare una descrizione per il gruppo locale. Non è possibile aggiungere un gruppo locale a un altro gruppo locale.

Il `vserver cifs users-and-groups local-group` le pagine man contengono dettagli sui parametri opzionali e sui requisiti di denominazione.

### Fasi

1. Creare il gruppo locale: `vserver cifs users-and-groups local-group create -vserver`



```
vserver_name -group-name group_name
```

Potrebbe essere utile il seguente parametro opzionale:

- ° -description

Una descrizione per il gruppo locale.

2. Verificare che il gruppo sia stato creato correttamente: `vserver cifs users-and-groups local-group show -vserver vserver_name`

### Esempio

Nell'esempio seguente viene creato un gruppo locale "SMB\_SERVER01\engineering" associato a SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group create -vserver  
vs1.example.com -group-name SMB_SERVER01\engineering
```

```
cluster1::> vserver cifs users-and-groups local-group show -vserver  
vs1.example.com
```

Vserver	Group Name	Description
-----	-----	-----
vs1.example.com	BUILTIN\Administrators	Built-in Administrators
group		
vs1.example.com	BUILTIN\Backup Operators	Backup Operators group
vs1.example.com	BUILTIN\Power Users	Restricted administrative
		privileges
vs1.example.com	BUILTIN\Users	All users
vs1.example.com	SMB_SERVER01\engineering	
vs1.example.com	SMB_SERVER01\sales	

### Al termine

È necessario aggiungere membri al nuovo gruppo.

### Gestire l'appartenenza al gruppo locale

È possibile gestire l'appartenenza a un gruppo locale aggiungendo e rimuovendo utenti locali o di dominio oppure aggiungendo e rimuovendo gruppi di dominio. Questa funzione è utile se si desidera controllare l'accesso ai dati in base ai controlli di accesso posizionati nel gruppo o se si desidera che gli utenti dispongano di privilegi associati a tale gruppo.

### A proposito di questa attività

Se non si desidera più che un utente locale, un utente di dominio o un gruppo di dominio disponga di diritti di accesso o privilegi in base all'appartenenza a un gruppo, è possibile rimuovere il membro dal gruppo.

Quando si aggiungono membri a un gruppo locale, è necessario tenere presente quanto segue:

- Non è possibile aggiungere utenti al gruppo speciale *Everyone*.

- Non è possibile aggiungere un gruppo locale a un altro gruppo locale.
- Per aggiungere un utente o un gruppo di dominio a un gruppo locale, ONTAP deve essere in grado di risolvere il nome in un SID.

Quando rimuovi membri da un gruppo locale, devi tenere presente quanto segue:

- Non puoi rimuovere membri dal gruppo speciale *Everyone*.
- Per rimuovere un membro da un gruppo locale, ONTAP deve essere in grado di risolvere il proprio nome in un SID.

## Fasi

### 1. Aggiungere o rimuovere un membro da un gruppo.

- Aggiungere un membro: `vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da aggiungere al gruppo locale specificato.

- Rimuovere un membro: `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da rimuovere dal gruppo locale specificato.

## Esempi

Nell'esempio seguente viene aggiunto un utente locale "SMB\_SERVER01\ sue" al gruppo locale "SMB\_SERVER01 engineering" su SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

Nell'esempio seguente vengono rimossi gli utenti locali "SMB\_SERVER01\ sue" e "SMB\_SERVER01 \Sjames" dal gruppo locale "SMB\_SERVER01 Engineering" su SVM vs1.example.com:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

## Verificare le versioni SMB abilitate

La release di ONTAP 9 determina quali versioni SMB sono abilitate per impostazione predefinita per le connessioni con client e controller di dominio. Verificare che il server SMB supporti i client e le funzionalità richieste nell'ambiente.

### A proposito di questa attività

Per le connessioni con client e controller di dominio, è necessario attivare SMB 2.0 e versioni successive, se

possibile. Per motivi di sicurezza, è consigliabile evitare di utilizzare SMB 1.0 e disattivarlo se si è verificato che non è richiesto nell'ambiente in uso.

In ONTAP 9, le versioni SMB 2.0 e successive sono attivate per impostazione predefinita per le connessioni client, ma la versione di SMB 1.0 attivata per impostazione predefinita dipende dalla versione di ONTAP in uso.

- A partire da ONTAP 9.1 P8, SMB 1.0 può essere disattivato sulle SVM.

Il `-smb1-enabled` al `vserver cifs options modify` Il comando attiva o disattiva SMB 1.0.

- A partire da ONTAP 9.3, viene disattivato per impostazione predefinita sui nuovi SVM.

Se il server SMB si trova in un dominio Active Directory (ad), è possibile abilitare SMB 2.0 per la connessione a un controller di dominio (DC) che inizia con ONTAP 9.1. Questa operazione è necessaria se SMB 1.0 è stato disattivato sui controller di dominio. A partire da ONTAP 9.2, SMB 2.0 è attivato per impostazione predefinita per le connessioni DC.



Se `-smb1-enabled-for-dc-connections` è impostato su `false` mentre `-smb1-enabled` è impostato su `true`, ONTAP nega le connessioni SMB 1.0 come client, ma continua ad accettare connessioni SMB 1.0 in entrata come server.

**"Gestione delle PMI"** Contiene dettagli sulle versioni e sulle funzionalità SMB supportate.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Verificare quali versioni SMB sono abilitate:

```
vserver cifs options show
```

È possibile scorrere l'elenco per visualizzare le versioni SMB abilitate per le connessioni client e, se si configura un server SMB in un dominio ad, per le connessioni di dominio ad.

3. Attivare o disattivare il protocollo SMB per le connessioni client secondo necessità:

- Per attivare una versione SMB:

```
vserver cifs options modify -vserver vserver_name smb_version true
```

- Per disattivare una versione SMB:

```
vserver cifs options modify -vserver vserver_name smb_version false
```

Valori possibili per `smb_version`:

- -smb1-enabled
- -smb2-enabled
- -smb3-enabled
- -smb31-enabled

Il seguente comando abilita SMB 3.1 su SVM vs1.example.com:

```
cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31-enabled true
```

1. Se il server SMB si trova in un dominio Active Directory, attivare o disattivare il protocollo SMB per le connessioni DC come richiesto:

- Per attivare una versione SMB:

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true
```

- Per disattivare una versione SMB:

```
vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false
```

2. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Mappare il server SMB sul server DNS

Il server DNS del sito deve avere una voce che punta il nome del server SMB e qualsiasi alias NetBIOS all'indirizzo IP del LIF dei dati, in modo che gli utenti Windows possano mappare un disco al nome del server SMB.

### Prima di iniziare

È necessario disporre dell'accesso amministrativo al server DNS del sito. Se non si dispone dell'accesso amministrativo, è necessario chiedere all'amministratore DNS di eseguire questa attività.

### A proposito di questa attività

Se si utilizzano alias NetBIOS per il nome del server SMB, si consiglia di creare punti di ingresso del server DNS per ciascun alias.

### Fasi

1. Accedere al server DNS.

2. Creare voci di ricerca in avanti (A - record di indirizzo) e indietro (PTR - record puntatore) per mappare il nome del server SMB all'indirizzo IP dei dati LIF.
3. Se si utilizzano alias NetBIOS, creare una voce di ricerca Alias Canonical name (CNAME resource record) per mappare ciascun alias all'indirizzo IP dei dati LIF del server SMB.

## Risultati

Una volta propagata la mappatura in rete, gli utenti di Windows possono mappare un disco al nome del server SMB o ai relativi alias NetBIOS.

## Configurare l'accesso del client SMB allo storage condiviso

### Configurare l'accesso del client SMB allo storage condiviso

Per fornire l'accesso del client SMB allo storage condiviso su una SVM, è necessario creare un volume o un qtree per fornire un container di storage, quindi creare o modificare una condivisione per tale container. È quindi possibile configurare le autorizzazioni di condivisione e file e verificare l'accesso dai sistemi client.

#### Prima di iniziare

- SMB deve essere completamente configurato sulla SVM.
- Tutti gli aggiornamenti della configurazione dei name service devono essere completi.
- Eventuali aggiunte o modifiche a un dominio Active Directory o alla configurazione del gruppo di lavoro devono essere completate.

### Creare un volume o un contenitore di storage qtree

#### Creare un volume

È possibile creare un volume e specificarne il punto di giunzione e altre proprietà utilizzando `volume create` comando.

#### A proposito di questa attività

Un volume deve includere un *percorso di giunzione* per rendere i dati disponibili ai client. È possibile specificare il percorso di giunzione quando si crea un nuovo volume. Se si crea un volume senza specificare un percorso di giunzione, è necessario *montare* il volume nello spazio dei nomi SVM utilizzando `volume mount` comando.

#### Prima di iniziare

- SMB deve essere configurato e funzionante.
- Lo stile di sicurezza SVM deve essere NTFS.
- A partire da ONTAP 9.13.1, puoi creare volumi con l'analisi della capacità e il monitoraggio delle attività abilitati. Per attivare il monitoraggio della capacità o dell'attività, eseguire il `volume create` comando con `-analytics-state` oppure `-activity-tracking-state` impostare su `on`.

Per ulteriori informazioni sull'analisi della capacità e sul monitoraggio delle attività, consulta [Abilita analisi del file system](#).

## Fasi

1. Creare il volume con un punto di giunzione: `volume create -vserver svm_name -volume`

```
volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]}  
-security-style ntfs -junction-path junction_path]
```

Le scelte per `-junction-path` sono i seguenti:

- Direttamente sotto root, ad esempio `/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio direttamente nel volume root SVM.

- In una directory esistente, ad esempio `/existing_dir/new_vol`

È possibile creare un nuovo volume e specificarne il montaggio in un volume esistente (in una gerarchia esistente), espresso come directory.

Se si desidera creare un volume in una nuova directory (in una nuova gerarchia sotto un nuovo volume), ad esempio, `/new_dir/new_vol`, Quindi, è necessario creare prima un nuovo volume padre che sia congiunto al volume root SVM. Creare quindi il nuovo volume figlio nel percorso di giunzione del nuovo volume padre (nuova directory).

2. Verificare che il volume sia stato creato con il punto di giunzione desiderato: `volume show -vserver svm_name -volume volume_name -junction`

## Esempi

Il seguente comando crea un nuovo volume denominato `users1` su SVM `vs1.example.com` e sull'aggregato `aggr1`. Il nuovo volume è disponibile all'indirizzo `/users`. Il volume ha una dimensione di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume users  
-aggregate aggr1 -size 750g -junction-path /users  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume users -junction
```

		Junction		Junction
Vserver	Volume	Active	Junction Path	Path Source
vs1.example.com	users1	true	/users	RW_volume

Il seguente comando crea un nuovo volume denominato "home4" su SVM "vs1.example.com" e l'aggregato "aggr1". La directory `/eng/` Esiste già nello spazio dei nomi per vs1 SVM e il nuovo volume è disponibile all'indirizzo `/eng/home`, che diventa la home directory di `/eng/` namespace. Il volume è di 750 GB e la relativa garanzia è di tipo volume (per impostazione predefinita).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1.example.com	home4	true	/eng/home	RW_volume

### Creare un qtree

È possibile creare un qtree per contenere i dati e specificarne le proprietà utilizzando volume qtree create comando.

### Prima di iniziare

- La SVM e il volume che conterrà il nuovo qtree devono già esistere.
- Lo stile di sicurezza SVM deve essere NTFS e SMB deve essere configurato e in esecuzione.

### Fasi

1. Creare il qtree: volume qtree create -vserver vserver\_name { -volume volume\_name -qtree qtree\_name | -qtree-path qtree path } -security-style ntfs

È possibile specificare il volume e il qtree come argomenti separati o specificare l'argomento del percorso qtree nel formato /vol/volume\_name/\_qtree\_name.

2. Verificare che il qtree sia stato creato con il percorso di giunzione desiderato: volume qtree show -vserver vserver\_name { -volume volume\_name -qtree qtree\_name | -qtree-path qtree path }

### Esempio

Nell'esempio seguente viene creato un qtree chiamato qt01 situato su SVM vs1.example.com che ha un percorso di giunzione /vol/data1:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path  
/vol/data1/qt01 -security-style ntfs  
[Job 1642] Job succeeded: Successful
```

```
cluster1::> volume qtree show -vserver vs1.example.com -qtree-path  
/vol/data1/qt01
```

```
          Vserver Name: vs1.example.com  
          Volume Name: data1  
          Qtree Name: qt01  
Actual (Non-Junction) Qtree Path: /vol/data1/qt01  
          Security Style: ntfs  
          Oplock Mode: enable  
          Unix Permissions: ---rwxr-xr-x  
          Qtree Id: 2  
          Qtree Status: normal  
          Export Policy: default  
Is Export Policy Inherited: true
```

## Requisiti e considerazioni per la creazione di una condivisione SMB

Prima di creare una condivisione SMB, è necessario comprendere i requisiti per i percorsi di condivisione e le proprietà di condivisione, in particolare per le home directory.

La creazione di una condivisione SMB richiede la specifica di una struttura di percorso di directory (utilizzando l' `-path` in `vserver cifs share create` a cui accederanno i client. Il percorso della directory corrisponde al percorso di giunzione di un volume o qtree creato nello spazio dei nomi SVM. Il percorso di directory e il percorso di giunzione corrispondente devono esistere prima di creare la condivisione.

I percorsi di condivisione hanno i seguenti requisiti:

- Il nome di un percorso di directory può contenere fino a 255 caratteri.
- Se nel nome del percorso è presente uno spazio, l'intera stringa deve essere inserita tra virgolette (ad esempio, `"/new volume/mount here"`).
- Se il percorso UNC (`\\servername\sharename\filepath`) Della condivisione contiene più di 256 caratteri (escludendo l'iniziale `""` nel percorso UNC), quindi la scheda **Security** nella casella Proprietà di Windows non è disponibile.

Si tratta di un problema del client Windows piuttosto che di un problema ONTAP. Per evitare questo problema, non creare condivisioni con percorsi UNC con più di 256 caratteri.

È possibile modificare le impostazioni predefinite della proprietà di condivisione:

- Le proprietà iniziali predefinite per tutte le condivisioni sono `oplocks`, `browsable`, `changenotify`, e `show-previous-versions`.
- È facoltativo specificare le proprietà di condivisione quando si crea una condivisione.



Tuttavia, se si specificano le proprietà di condivisione quando si crea la condivisione, le impostazioni predefinite non vengono utilizzate. Se si utilizza `-share-properties` parametro quando si crea una condivisione, è necessario specificare tutte le proprietà della condivisione che si desidera applicare alla condivisione utilizzando un elenco delimitato da virgole.

- Per designare una condivisione della home directory, utilizzare `homedirectory` proprietà.

Questa funzione consente di configurare una condivisione mappata a diverse directory in base all'utente che si connette ad essa e a una serie di variabili. Invece di dover creare condivisioni separate per ciascun utente, è possibile configurare una singola condivisione con alcuni parametri della home directory per definire la relazione di un utente tra un punto di ingresso (la condivisione) e la propria home directory (una directory sulla SVM).



Non è possibile aggiungere o rimuovere questa proprietà dopo aver creato la condivisione.

Le condivisioni home directory hanno i seguenti requisiti:

- Prima di creare le home directory SMB, è necessario aggiungere almeno un percorso di ricerca della home directory utilizzando `vserver cifs home-directory search-path add` comando.
- Condivisioni home directory specificate dal valore di `homedirectory` su `-share-properties` il parametro deve includere `%w` (Nome utente Windows) variabile dinamica nel nome della condivisione.

Il nome della condivisione può contenere anche `%d` (nome di dominio) variabile dinamica (ad esempio, `%d/%w`) o una parte statica nel nome della condivisione (ad esempio, `home1_%w`).

- Se la condivisione viene utilizzata da amministratori o utenti per connettersi alle home directory di altri utenti (utilizzando le opzioni di `vserver cifs home-directory modify` comando), il modello di nome di condivisione dinamica deve essere preceduto da una tilde (`~`).

"Gestione delle PMI" e `vserver cifs share` le pagine man contengono informazioni aggiuntive.

## Creare una condivisione SMB

È necessario creare una condivisione SMB prima di poter condividere i dati da un server SMB con client SMB. Quando si crea una condivisione, è possibile impostare le proprietà della condivisione, ad esempio designarla come home directory. È inoltre possibile personalizzare la condivisione configurando le impostazioni opzionali.

### Prima di iniziare

Il percorso della directory per il volume o `qtree` deve esistere nello spazio dei nomi SVM prima di creare la condivisione.

### A proposito di questa attività

Quando si crea una condivisione, l'ACL di condivisione predefinito (autorizzazioni di condivisione predefinite) è `Everyone / Full Control`. Dopo aver testato l'accesso alla condivisione, rimuovere l'ACL della condivisione predefinita e sostituirlo con un'alternativa più sicura.

### Fasi

1. Se necessario, creare la struttura del percorso di directory per la condivisione.

Il `vserver cifs share create` il comando verifica il percorso specificato in `-path` durante la

creazione della condivisione. Se il percorso specificato non esiste, il comando non riesce.

2. Creare una condivisione SMB associata alla SVM specificata:  
`vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Verificare che la condivisione sia stata creata:  
`vserver cifs share show -share-name share_name`

## Esempi

Il seguente comando crea una condivisione SMB denominata “SHARE1” su SVM `vs1.example.com`. Il percorso della directory è `/users` e viene creato con le proprietà predefinite.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name SHARE1 -path /users
```

```
cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full Control
			browsable		
			changenotify		
			show-previous-versions		

## Verificare l'accesso al client SMB

Verificare di aver configurato SMB correttamente accedendo e scrivendo i dati nella condivisione. Verificare l'accesso utilizzando il nome del server SMB e gli alias NetBIOS.

### Fasi

1. Accedere a un client Windows.
2. Verificare l'accesso utilizzando il nome del server SMB:
  - a. In Esplora risorse, mappare un disco alla condivisione nel seguente formato: `\\SMB_Server_Name\Share_Name`

Se la mappatura non riesce, è possibile che la mappatura DNS non sia ancora propagata in tutta la rete. È necessario verificare l'accesso utilizzando il nome del server SMB in un secondo momento.

Se il server SMB è denominato `vs1.example.com` e la condivisione è denominata `SHARE1`, immettere quanto segue: `\\vs0.example.com\SHARE1`

- b. Sul disco appena creato, creare un file di prova, quindi eliminare il file.

L'accesso in scrittura alla condivisione è stato verificato utilizzando il nome del server SMB.

3. Ripetere il passaggio 2 per tutti gli alias NetBIOS.

Creare elenchi di controllo degli accessi di condivisione SMB

La configurazione delle autorizzazioni di condivisione mediante la creazione di elenchi di controllo degli accessi (ACL) per le condivisioni SMB consente di controllare il livello di accesso a una condivisione per utenti e gruppi.

Prima di iniziare

È necessario decidere quali utenti o gruppi avranno accesso alla condivisione.

A proposito di questa attività

È possibile configurare gli ACL a livello di condivisione utilizzando nomi di utenti o gruppi Windows locali o di dominio.

Prima di creare un nuovo ACL, è necessario eliminare l'ACL di condivisione predefinito Everyone / Full Control, che comporta un rischio per la sicurezza.

In modalità workgroup, il nome di dominio locale è il nome del server SMB.

Fasi

- 1. Eliminare l'ACL di condivisione predefinito:  
`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
- 2. Configurare il nuovo ACL:

Se si desidera configurare gli ACL utilizzando un...	Immettere il comando...
Utente Windows	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</code>
Gruppo di Windows	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</code>

- 3. Verificare che l'ACL applicato alla condivisione sia corretto utilizzando `vserver cifs share access-control show` comando.

Esempio

Il seguente comando fornisce Change Autorizzazioni al gruppo Windows "Sales Team" per la condivisione "sales" su "`vs1.example.com`"SVM:

```
cluster1::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vsserver cifs share access-control show
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\"Sales Team"	windows	Change

I seguenti comandi impartire Change Autorizzazione al gruppo Windows locale denominato "Tiger Team" e Full\_Control Autorizzazione all'utente Windows locale denominato "Sue Chang" per la condivisione "datavol5" su "vs1" SVM:

```
cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsserver cifs share access-control create -vsserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsserver cifs share access-control show -vsserver vs1
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	DOMAIN\"Tiger Team"	windows	Change
vs1	datavol5	DOMAIN\"Sue Chang"	windows	Full_Control

## Configurare le autorizzazioni per i file NTFS in una condivisione

Per consentire l'accesso ai file agli utenti o ai gruppi che hanno accesso a una condivisione, è necessario configurare le autorizzazioni dei file NTFS su file e directory in tale condivisione da un client Windows.

### Prima di iniziare

L'amministratore che esegue questa attività deve disporre di autorizzazioni NTFS sufficienti per modificare le autorizzazioni sugli oggetti selezionati.

### A proposito di questa attività

"[Gestione delle PMI](#)" La documentazione di Windows contiene informazioni su come impostare le autorizzazioni NTFS standard e avanzate.

### Fasi

1. Accedere a un client Windows come amministratore.
2. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
3. Completare la casella **Map Network Drive** (Connetti unità di rete):
  - a. Selezionare una lettera **Drive**.
  - b. Nella casella **Folder** (cartella), digitare il nome del server SMB contenente la condivisione contenente i dati a cui si desidera applicare le autorizzazioni e il nome della condivisione.

Se il nome del server SMB è SMB\_SERVER01 e la condivisione è denominata "SHARE1", immettere \\SMB\_SERVER01\SHARE1.



È possibile specificare l'indirizzo IP dell'interfaccia dati per il server SMB invece del nome del server SMB.

- c. Fare clic su **fine**.

Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

4. Selezionare il file o la directory per cui si desidera impostare le autorizzazioni per il file NTFS.
5. Fare clic con il pulsante destro del mouse sul file o sulla directory, quindi selezionare **Proprietà**.
6. Selezionare la scheda **sicurezza**.

La scheda Security (sicurezza) visualizza l'elenco di utenti e gruppi per i quali è impostata l'autorizzazione NTFS. La casella Permissions for <Object> (autorizzazioni per utenti) visualizza un elenco di permessi e permessi di negazione in vigore per l'utente o il gruppo selezionato.

7. Fare clic su **Edit** (Modifica).

Viene visualizzata la finestra Permissions for <Object> (autorizzazioni per l'accesso)

8. Eseguire le azioni desiderate:

Se si desidera	Effettuare le seguenti operazioni...
Impostare le autorizzazioni NTFS standard per un nuovo utente o gruppo	<p>a. Fare clic su <b>Aggiungi</b>.</p> <p>Viene visualizzata la finestra Seleziona utente, computer, account di servizio o gruppi.</p> <p>b. Nella casella <b>inserire i nomi degli oggetti da selezionare</b>, digitare il nome dell'utente o del gruppo a cui si desidera aggiungere l'autorizzazione NTFS.</p> <p>c. Fare clic su <b>OK</b>.</p>
Modificare o rimuovere le autorizzazioni NTFS standard da un utente o gruppo	Nella casella <b>nomi gruppo o utente</b> , selezionare l'utente o il gruppo che si desidera modificare o rimuovere.

9. Eseguire le azioni desiderate:

Se si desidera...	Effettuare le seguenti operazioni
Impostare le autorizzazioni NTFS standard per un utente o un gruppo nuovo o esistente	Nella casella <b>Permissions for &lt;Object&gt;</b> (autorizzazioni per l'accesso), selezionare le caselle <b>Allow</b> (Consenti) o <b>Nega</b> per il tipo di accesso che si desidera consentire o meno per l'utente o il gruppo selezionato.
Rimuovere un utente o un gruppo	Fare clic su <b>Rimuovi</b> .



Se alcune o tutte le caselle di autorizzazione standard non sono selezionabili, le autorizzazioni vengono ereditate dall'oggetto padre. La casella **permessi speciali** non è selezionabile. Se selezionata, significa che uno o più diritti avanzati granulari sono stati impostati per l'utente o il gruppo selezionato.

10. Una volta aggiunte, rimosse o modificate le autorizzazioni NTFS per l'oggetto, fare clic su **OK**.

### Verificare l'accesso dell'utente

È necessario verificare che gli utenti configurati possano accedere alla condivisione SMB e ai file in essa contenuti.

#### Fasi

1. Su un client Windows, accedere come uno degli utenti che ora ha accesso alla condivisione.
2. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
3. Completare la casella **Map Network Drive** (Connetti unità di rete):
  - a. Selezionare una lettera **Drive**.
  - b. Nella casella **Folder** (cartella), digitare il nome della condivisione che verrà fornito agli utenti.

Se il nome del server SMB è SMB\_SERVER01 e la condivisione è denominata "SHARE1", immettere \\SMB\_SERVER01\share1.

c. Fare clic su **fine**.

Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

4. Creare un file di test, verificare che esista, scriverne del testo e rimuovere il file di test.

## Gestire SMB con la CLI

### Panoramica di riferimento SMB

Le funzioni di accesso ai file ONTAP sono disponibili per il protocollo SMB. È possibile attivare un server CIFS, creare condivisioni e abilitare i servizi Microsoft.



*SMB* (Server message Block) si riferisce ai dialetti moderni del protocollo CIFS (Common Internet file System). L'interfaccia della riga di comando (CLI) di ONTAP e i tool di gestione di OnCommand sono ancora visibili in *CIFS*.

Attenersi alle seguenti procedure nei seguenti casi:

- Vuoi comprendere la gamma di funzionalità del protocollo SMB di ONTAP.
- Si desidera eseguire attività di configurazione e manutenzione meno comuni, non la configurazione SMB di base.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

### Supporto per server SMB

#### Panoramica sul supporto dei server SMB

È possibile abilitare e configurare server SMB su macchine virtuali storage (SVM) per consentire ai client SMB di accedere ai file sul cluster.

- Ogni SVM di dati nel cluster può essere associata esattamente a un dominio Active Directory.
- Non è necessario che le SVM dei dati siano associate allo stesso dominio.
- È possibile associare più SVM allo stesso dominio.

Prima di creare un server SMB, è necessario configurare le SVM e le LIF utilizzate per la distribuzione dei dati. Se la rete dati non è piatta, potrebbe essere necessario configurare anche gli IPspaces, i domini di trasmissione e le subnet. La *Guida alla gestione della rete* contiene dettagli.

#### Informazioni correlate

["Gestione della rete"](#)

[Modificare i server SMB](#)

["Amministrazione del sistema"](#)

## Versioni e funzionalità SMB supportate

SMB (Server message Block) è un protocollo di condivisione file remoto utilizzato dai client e dai server Microsoft Windows. In ONTAP 9, sono supportate tutte le versioni SMB; tuttavia, il supporto predefinito SMB 1.0 dipende dalla versione di ONTAP in uso. Verificare che il server SMB ONTAP supporti i client e le funzionalità richieste nell'ambiente.

Le informazioni più recenti sui client SMB e sui controller di dominio supportati da ONTAP sono disponibili nello strumento *matrice di interoperabilità*.

SMB 2.0 e le versioni successive sono attivate per impostazione predefinita per i server SMB ONTAP 9 e possono essere attivate o disattivate in base alle necessità. La seguente tabella mostra il supporto SMB 1.0 e la configurazione predefinita.

Funzionalità SMB 1.0:	In queste versioni di ONTAP 9:			
	9.0	9.1	9.2	9.3 e versioni successive
È attivato per impostazione predefinita	Sì	Sì	Sì	No
Può essere attivato o disattivato	No	Sì*9.1 P8 o versione successiva richiesta.	Sì	Sì



Le impostazioni predefinite per le connessioni SMB 1.0 e 2.0 ai domain controller dipendono anche dalla versione di ONTAP. Ulteriori informazioni sono disponibili nella `vserver cifs security modify` pagina man. Per gli ambienti con server CIFS esistenti che eseguono SMB 1.0, è necessario eseguire la migrazione a una versione SMB più recente il prima possibile per prepararsi ai miglioramenti di sicurezza e conformità. Per ulteriori informazioni, contatta il tuo rappresentante NetApp.

La seguente tabella mostra le funzionalità SMB supportate in ciascuna versione SMB. Alcune funzionalità SMB sono attivate per impostazione predefinita e alcune richiedono una configurazione aggiuntiva.

Questa funzionalità:	Richiede l'abilitazione:	È supportato in ONTAP 9 per le seguenti versioni SMB:				
		1.0	2.0	2.1	3.0	3.1.1
Funzionalità SMB 1.0 legacy		X	X	X	X	X
Manici d'urevoli			X	X	X	X



<b>Questa funzionalità:</b>	<b>Richiede l'abilitazione:</b>	<b>È supportato in ONTAP 9 per le seguenti versioni SMB:</b>				
Operazioni composte			X	X	X	X
Operazioni asincrone			X	X	X	X
Maggiori dimensioni dei buffer di lettura e scrittura			X	X	X	X
Maggiore scalabilità			X	X	X	X
Firma SMB	X	X	X	X	X	X
Formato di file ADS (alternate Data Stream)	X	X	X	X	X	X
MTU grande (attivata per impostazione predefinita a partire da ONTAP 9.7)	X			X	X	X
Oplock del lease				X	X	X
Condivisioni a disponibilità continua	X				X	X
Handle persistenti					X	X
Testimone					X	X
CRITTOGRA FIA SMB: AES-128-CCM	X				X	X

Questa funzionalità:	Richiede l'abilitazione:	È supportato in ONTAP 9 per le seguenti versioni SMB:				
		4.1	4.2	4.3	4.4	4.5
Scale-out (richiesto dalle condivisioni CA)					X	X
Failover trasparente					X	X
SMB multicanale (a partire da ONTAP 9.4)	X				X	X
Integrità della preautenticazione						X
Failover del client cluster v.2 (CCFv2)						X
Crittografia SMB: AES-128-GCM (a partire da ONTAP 9.1)	X					X

#### Informazioni correlate

[Utilizzo della firma SMB per migliorare la sicurezza della rete](#)

[Impostazione del livello minimo di sicurezza per l'autenticazione del server SMB](#)

[Configurazione della crittografia SMB richiesta sui server SMB per il trasferimento dei dati su SMB](#)

["Report tecnico di NetApp 4543: Best practice per il protocollo SMB"](#)

["Interoperabilità NetApp"](#)

#### Funzionalità di Windows non supportate

Prima di utilizzare CIFS nella rete, è necessario conoscere alcune funzionalità di Windows non supportate da ONTAP.

ONTAP non supporta le seguenti funzionalità di Windows:

- File system crittografato (EFS)

- Registrazione degli eventi NTFS (NT file System) nel diario delle modifiche
- Servizio di replica file Microsoft (FRS)
- Servizio di indicizzazione Microsoft Windows
- Storage remoto tramite HSM (Hierarchical Storage Management)
- Gestione delle quote dai client Windows
- Semantica delle quote di Windows
- Il file LMHOSTS
- Compressione nativa NTFS

## Configurare i servizi NIS o LDAP sulla SVM

Con l'accesso SMB, il mapping degli utenti a un utente UNIX viene sempre eseguito, anche quando si accede ai dati in un volume di sicurezza NTFS. Se si mappano gli utenti Windows agli utenti UNIX corrispondenti le cui informazioni sono memorizzate negli archivi di directory NIS o LDAP o se si utilizza LDAP per la mappatura dei nomi, è necessario configurare questi servizi durante l'installazione di SMB.

### Prima di iniziare

È necessario personalizzare la configurazione del database dei name service in modo che corrisponda all'infrastruttura del name service.

### A proposito di questa attività

Le SVM utilizzano i database dei name service ns-switch per determinare l'ordine in cui cercare le origini di un dato database dei name service. L'origine ns-switch può essere una combinazione qualsiasi di "Files", "nis" o "ldap". Per il database dei gruppi, ONTAP tenta di ottenere le appartenenze ai gruppi da tutte le origini configurate e utilizza le informazioni consolidate sull'appartenenza ai gruppi per i controlli degli accessi. Se una di queste origini non è disponibile al momento dell'ottenimento delle informazioni sul gruppo UNIX, ONTAP non può ottenere le credenziali UNIX complete e i controlli di accesso successivi potrebbero non riuscire. Pertanto, è necessario controllare sempre che tutte le sorgenti ns-switch siano configurate per il database di gruppo nelle impostazioni ns-switch.

L'impostazione predefinita prevede che il server SMB mappi tutti gli utenti Windows all'utente UNIX predefinito memorizzato in locale `passwd` database. Se si desidera utilizzare la configurazione predefinita, la configurazione dei servizi NIS o LDAP UNIX nome utente e gruppo o la mappatura utente LDAP è facoltativa per l'accesso SMB.

### Fasi

1. Se le informazioni relative a utenti, gruppi e netgroup UNIX sono gestite da NIS name service, configurare NIS name service:
  - a. Determinare l'ordine corrente dei servizi di gestione dei nomi utilizzando `vserver services name-service ns-switch show` comando.

In questo esempio, i tre database (`group`, `passwd`, e `netgroup`) che possono utilizzare `nis` come nome, l'origine del servizio utilizza solo `files` come fonte.

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
-----	-----	-----	-----
vs1	hosts	true	dns, files
vs1	group	true	files
vs1	passwd	true	files
vs1	netgroup	true	files
vs1	namemap	true	files

È necessario aggiungere nis origine di group e. passwd e, facoltativamente, in netgroup database.

- b. Regolare l'ordinamento del database dei name service ns-switch come desiderato utilizzando `vserver services name-service ns-switch modify` comando.

Per ottenere prestazioni ottimali, non aggiungere un name service a un database di name service a meno che non si preveda di configurare tale name service su SVM.

Se si modifica la configurazione per più database di name service, è necessario eseguire il comando separatamente per ogni database di name service che si desidera modificare.

In questo esempio, nis e. files sono configurati come origini per group e. passwd database, in questo ordine. Il resto dei database dei servizi di nome non viene modificato.

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

- c. Verificare che l'ordine dei name service sia corretto utilizzando `vserver services name-service ns-switch show` comando.

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
-----	-----	-----	-----
vs1	hosts	true	dns, files
vs1	group	true	nis, files
vs1	passwd	true	nis, files
vs1	netgroup	true	files
vs1	namemap	true	files

- d. Creare la configurazione NIS name service:

```
vserver services name-service nis-domain create -vserver vserver_name
```

```
-domain NIS_domain_name -servers NIS_server_IPaddress,... -active true+

vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```



A partire da ONTAP 9.2, il campo `-nis-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server NIS.

- e. Verificare che il NIS name service sia configurato correttamente e sia attivo: `vserver services name-service nis-domain show vserver vserver_name`

```
vserver services name-service nis-domain show vserver vs1
```

Vserver	Domain	Active	Server
-----	-----	-----	-----
vs1	example.com	true	10.0.0.60

2. Se le informazioni relative a utenti, gruppi e netgroup UNIX o la mappatura dei nomi sono gestite dai servizi dei nomi LDAP, configurare i servizi dei nomi LDAP utilizzando le informazioni disponibili ["Gestione NFS"](#).

## Funzionamento della configurazione dello switch ONTAP name service

ONTAP memorizza le informazioni di configurazione del name service in una tabella equivalente a `/etc/nsswitch.conf` File su sistemi UNIX. È necessario comprendere la funzione della tabella e il modo in cui ONTAP la utilizza in modo da poterla configurare in modo appropriato per l'ambiente in uso.

La tabella ONTAP name service switch determina le origini del servizio di nomi che ONTAP consulta per recuperare le informazioni relative a un determinato tipo di informazioni sul servizio di nomi. ONTAP gestisce una tabella di switch del name service separata per ogni SVM.

### Tipi di database

La tabella memorizza un elenco di name service separato per ciascuno dei seguenti tipi di database:

Tipo di database	Definisce le origini del servizio nome per...	Le origini valide sono...
host	Conversione dei nomi host in indirizzi IP	file, dns
gruppo	Ricerca di informazioni sul gruppo di utenti	file, nis, ldap
password	Ricerca delle informazioni dell'utente	file, nis, ldap

Tipo di database	Definisce le origini del servizio nome per...	Le origini valide sono...
netgroup	Ricerca di informazioni sul netgroup	file, nis, ldap
mappa dei nomi	Mappatura dei nomi utente	file, ldap

### Tipi di origine

Le origini specificano quale nome di origine del servizio utilizzare per recuperare le informazioni appropriate.

Specifica tipo di origine...	Per cercare informazioni in...	Gestito dalle famiglie di comandi...
file	File di origine locali	<pre>vserver services name- service unix-user vserver services name-service unix-group  vserver services name- service netgroup  vserver services name- service dns hosts</pre>
nis	Server NIS esterni come specificato nella configurazione del dominio NIS di SVM	<pre>vserver services name- service nis-domain</pre>
ldap	Server LDAP esterni come specificato nella configurazione del client LDAP di SVM	<pre>vserver services name- service ldap</pre>
dns	Server DNS esterni come specificato nella configurazione DNS di SVM	<pre>vserver services name- service dns</pre>

Anche se si prevede di utilizzare NIS o LDAP per l'accesso ai dati e l'autenticazione dell'amministrazione SVM, è comunque necessario includere `files` E configurare gli utenti locali come fallback nel caso in cui l'autenticazione NIS o LDAP non riesca.

### Protocolli utilizzati per accedere a fonti esterne

Per accedere ai server per le origini esterne, ONTAP utilizza i seguenti protocolli:

Origine esterna del name service	Protocollo utilizzato per l'accesso
NIS	UDP
DNS	UDP

Origine esterna del name service	Protocollo utilizzato per l'accesso
LDAP	TCP

### Esempio

Nell'esempio seguente viene visualizzata la configurazione dello switch name service per SVM `svm_1`:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source	Order
svm_1	hosts	files,	dns
svm_1	group	files	
svm_1	passwd	files	
svm_1	netgroup	nis,	files

Per cercare informazioni su utenti o gruppi, ONTAP consulta solo i file di origine locali. Se la query non restituisce alcun risultato, la ricerca non riesce.

Per cercare informazioni sui netgroup, ONTAP consulta prima i server NIS esterni. Se la query non restituisce alcun risultato, viene selezionato il file netgroup locale.

Non sono presenti voci di name service per la mappatura dei nomi nella tabella per SVM `svm_1`. Pertanto, ONTAP consulta solo i file di origine locali per impostazione predefinita.

## Gestire i server SMB

### Modificare i server SMB

È possibile spostare un server SMB da un gruppo di lavoro a un dominio Active Directory, da un gruppo di lavoro a un altro gruppo di lavoro o da un dominio Active Directory a un gruppo di lavoro utilizzando `vserver cifs modify` comando.

#### A proposito di questa attività

È inoltre possibile modificare altri attributi del server SMB, ad esempio il nome del server SMB e lo stato amministrativo. Per ulteriori informazioni, consulta la pagina [man](#).

#### Scelte

- Spostare il server SMB da un gruppo di lavoro a un dominio Active Directory:
  - a. Impostare lo stato amministrativo del server SMB su down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Spostare il server SMB dal gruppo di lavoro a un dominio Active Directory: `vserver cifs modify -vserver vserver_name -domain domain_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
```

Per creare un account macchina Active Directory per il server SMB, è necessario fornire il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer a `ou=example` ou container all'interno di `example` dominio .com.

A partire da ONTAP 9.7, l'amministratore può fornire un URI a un file keytab in alternativa a un nome e una password a un account Windows con privilegi. Quando si riceve l'URI, includerlo in `-keytab-uri` con il `vserver cifs` comandi.

- Spostare il server SMB da un gruppo di lavoro a un altro gruppo di lavoro:
  - a. Impostare lo stato amministrativo del server SMB su down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Modificare il gruppo di lavoro per il server SMB: `vserver cifs modify -vserver vserver_name -workgroup new_workgroup_name`

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- Spostare il server SMB da un dominio Active Directory a un gruppo di lavoro:
  - a. Impostare lo stato amministrativo del server SMB su down.

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

- b. Spostare il server SMB dal dominio Active Directory a un gruppo di lavoro: `vserver cifs modify -vserver vserver_name -workgroup workgroup_name`

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```



Per accedere alla modalità workgroup, tutte le funzioni basate sul dominio devono essere disattivate e la relativa configurazione rimossa automaticamente dal sistema, incluse le condivisioni a disponibilità continua, le copie shadow e AES. Tuttavia, gli ACL delle condivisioni configurati nel dominio, come "EXAMPLE.COM\userName", non funzionano correttamente, ma non possono essere rimossi da ONTAP. Rimuovere questi ACL di condivisione il prima possibile utilizzando strumenti esterni dopo il completamento del comando. Se AES è attivato, potrebbe essere richiesto di fornire il nome e la password di un account Windows con privilegi sufficienti per disattivarlo nel dominio "example.com".



- Modificare gli altri attributi utilizzando il parametro appropriato di `vserver cifs modify` comando.

## Utilizzare le opzioni per personalizzare i server SMB

### Opzioni server SMB disponibili

È utile sapere quali opzioni sono disponibili quando si considera come personalizzare il server SMB. Anche se alcune opzioni sono per uso generale sul server SMB, molte vengono utilizzate per abilitare e configurare funzionalità SMB specifiche. Le opzioni dei server SMB sono controllate con `vserver cifs options modify` opzione.

L'elenco seguente specifica le opzioni del server SMB disponibili a livello di privilegi di amministratore:

- **Configurazione del valore di timeout della sessione SMB**

La configurazione di questa opzione consente di specificare il numero di secondi di inattività prima della disconnessione di una sessione SMB. Una sessione inattiva è una sessione in cui un utente non ha file o directory aperti sul client. Il valore predefinito è 900 secondi.

- **Configurazione dell'utente UNIX predefinito**

La configurazione di questa opzione consente di specificare l'utente UNIX predefinito utilizzato dal server SMB. ONTAP crea automaticamente un utente predefinito denominato "pcuser" (con un UID di 65534), crea un gruppo denominato "pcuser" (con un GID di 65534) e aggiunge l'utente predefinito al gruppo "pcuser". Quando si crea un server SMB, ONTAP configura automaticamente "pcuser" come utente UNIX predefinito.

- **Configurazione dell'utente UNIX guest**

La configurazione di questa opzione consente di specificare il nome di un utente UNIX a cui vengono mappati gli utenti che accedono da domini non attendibili, consentendo a un utente di un dominio non attendibile di connettersi al server SMB. Per impostazione predefinita, questa opzione non è configurata (non esiste alcun valore predefinito); pertanto, l'impostazione predefinita è di non consentire agli utenti di domini non attendibili di connettersi al server SMB.

- **Abilitazione o disabilitazione dell'esecuzione della concessione in lettura per i bit di modalità**

L'attivazione o la disattivazione di questa opzione consente di specificare se consentire ai client SMB di eseguire file eseguibili con bit in modalità UNIX ai quali hanno accesso in lettura, anche quando il bit eseguibile UNIX non è impostato. Questa opzione è disattivata per impostazione predefinita.

- **Abilitazione o disabilitazione della possibilità di eliminare i file di sola lettura dai client NFS**

L'attivazione o la disattivazione di questa opzione determina se consentire ai client NFS di eliminare file o cartelle con il set di attributi di sola lettura. La semantica di eliminazione NTFS non consente l'eliminazione di un file o di una cartella quando viene impostato l'attributo di sola lettura. La semantica di eliminazione di UNIX ignora il bit di sola lettura, utilizzando invece le autorizzazioni della directory principale per determinare se un file o una cartella può essere eliminata. L'impostazione predefinita è `disabled`, che determina la semantica di eliminazione di NTFS.

- **Configurazione degli indirizzi del server Windows Internet Name Service**

La configurazione di questa opzione consente di specificare un elenco di indirizzi del server WINS

(Windows Internet Name Service) come elenco delimitato da virgole. Specificare gli indirizzi IPv4. Gli indirizzi IPv6 non sono supportati. Non esiste alcun valore predefinito.

L'elenco seguente specifica le opzioni del server SMB disponibili al livello di privilegio avanzato:

- **Concessione delle autorizzazioni di gruppo UNIX agli utenti CIFS**

La configurazione di questa opzione determina se all'utente CIFS in entrata che non è il proprietario del file può essere concessa l'autorizzazione di gruppo. Se l'utente CIFS non è il proprietario del file di sicurezza UNIX e questo parametro è impostato su `true`, quindi viene concessa l'autorizzazione di gruppo per il file. Se l'utente CIFS non è il proprietario del file di sicurezza UNIX e questo parametro è impostato su `false`, Quindi, le normali regole UNIX sono applicabili per concedere l'autorizzazione al file. Questo parametro è applicabile ai file di sicurezza UNIX con autorizzazione impostata su `mode bits` E non è applicabile ai file con la modalità di sicurezza NTFS o NFSv4. L'impostazione predefinita è `false`.

- **Abilitazione o disabilitazione di SMB 1.0**

SMB 1.0 è disattivato per impostazione predefinita su una SVM per la quale viene creato un server SMB in ONTAP 9.3.



A partire da ONTAP 9.3, SMB 1.0 è disattivato per impostazione predefinita per i nuovi server SMB creati in ONTAP 9.3. È necessario migrare a una versione SMB più recente il prima possibile per prepararsi ai miglioramenti di sicurezza e conformità. Per ulteriori informazioni, contatta il tuo rappresentante NetApp.

- **Abilitazione o disabilitazione di SMB 2.x**

SMB 2.0 è la versione SMB minima che supporta il failover LIF. Se si disattiva SMB 2.x, anche ONTAP disattiva automaticamente SMB 3.X.

SMB 2.0 è supportato solo su SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Abilitazione o disabilitazione di SMB 3.0**

SMB 3.0 è la versione SMB minima che supporta le condivisioni a disponibilità continua. Windows Server 2012 e Windows 8 sono le versioni minime di Windows che supportano SMB 3.0.

SMB 3.0 è supportato solo su SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Abilitazione o disabilitazione di SMB 3.1**

Windows 10 è l'unica versione di Windows che supporta SMB 3.1.

SMB 3.1 è supportato solo su SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Abilitazione o disabilitazione dell'offload delle copie ODX**

L'offload delle copie ODX viene utilizzato automaticamente dai client Windows che lo supportano. Questa opzione è attivata per impostazione predefinita.

- **Abilitazione o disabilitazione del meccanismo di copia diretta per l'offload delle copie ODX**

Il meccanismo di copia diretta aumenta le prestazioni dell'operazione di offload delle copie quando i client Windows tentano di aprire il file di origine di una copia in una modalità che impedisce la modifica del file mentre la copia è in corso. Per impostazione predefinita, il meccanismo di copia diretta è attivato.

- **Abilitazione o disabilitazione dei riferimenti automatici ai nodi**

Con i riferimenti automatici ai nodi, il server SMB fa automaticamente riferimento ai client a una LIF di dati locale al nodo che ospita i dati a cui si accede attraverso la condivisione richiesta.

- **Attivazione o disattivazione delle policy di esportazione per SMB**

Questa opzione è disattivata per impostazione predefinita.

- **Abilitazione o disabilitazione dell'utilizzo dei punti di giunzione come punti di analisi**

Se questa opzione è attivata, il server SMB espone i punti di giunzione ai client SMB come punti di analisi. Questa opzione è valida solo per connessioni SMB 2.x o SMB 3.0. Questa opzione è attivata per impostazione predefinita.

Questa opzione è supportata solo sulle SVM. L'opzione è attivata per impostazione predefinita sulle SVM

- **Configurazione del numero massimo di operazioni simultanee per connessione TCP**

Il valore predefinito è 255.

- **Abilitazione o disabilitazione della funzionalità locale di utenti e gruppi Windows**

Questa opzione è attivata per impostazione predefinita.

- **Attivazione o disattivazione dell'autenticazione degli utenti Windows locali**

Questa opzione è attivata per impostazione predefinita.

- **Attivazione o disattivazione della funzionalità di copia shadow VSS**

ONTAP utilizza la funzionalità di copia shadow per eseguire backup remoti dei dati memorizzati utilizzando la soluzione Hyper-V su SMB.

Questa opzione è supportata solo sulle SVM e solo per le configurazioni Hyper-V su SMB. L'opzione è attivata per impostazione predefinita sulle SVM

- **Configurazione della profondità della directory della copia shadow**

La configurazione di questa opzione consente di definire la profondità massima delle directory in cui creare copie shadow quando si utilizza la funzionalità di copia shadow.

Questa opzione è supportata solo sulle SVM e solo per le configurazioni Hyper-V su SMB. L'opzione è attivata per impostazione predefinita sulle SVM

- **Attivazione o disattivazione delle funzionalità di ricerca multidominio per la mappatura dei nomi**

Se questa opzione è attivata, quando un utente UNIX viene mappato a un utente di dominio Windows utilizzando un carattere jolly (\*) nella parte di dominio del nome utente Windows (ad esempio, \* joe), ONTAP ricerca l'utente specificato in tutti i domini con trust bidirezionali nel dominio principale. Il dominio principale è il dominio che contiene l'account del computer del server SMB.

In alternativa alla ricerca di tutti i domini trusted bidirezionalmente, è possibile configurare un elenco di domini trusted preferiti. Se questa opzione è attivata e viene configurato un elenco preferito, l'elenco preferito viene utilizzato per eseguire ricerche di mappatura dei nomi di più domini.

L'impostazione predefinita prevede l'attivazione delle ricerche di associazione dei nomi a più domini.

- **Configurazione della dimensione del settore del file system**

La configurazione di questa opzione consente di configurare la dimensione del settore del file system in byte che ONTAP invia ai client SMB. Sono disponibili due valori validi per questa opzione: 4096 e 512. Il valore predefinito è 4096. Potrebbe essere necessario impostare questo valore su 512 se l'applicazione Windows supporta solo una dimensione di settore di 512 byte.

- **Attivazione o disattivazione del controllo dinamico degli accessi**

L'attivazione di questa opzione consente di proteggere gli oggetti sul server SMB utilizzando il controllo dinamico dell'accesso (DAC), incluso l'utilizzo del controllo per organizzare i criteri di accesso centrali e l'utilizzo degli oggetti Criteri di gruppo per implementare i criteri di accesso centrali. L'opzione è disattivata per impostazione predefinita.

Questa opzione è supportata solo sulle SVM.

- **Impostazione delle restrizioni di accesso per le sessioni non autenticate (limitazione anonima)**

L'impostazione di questa opzione determina le restrizioni di accesso per le sessioni non autenticate. Le restrizioni vengono applicate agli utenti anonimi. Per impostazione predefinita, non esistono restrizioni di accesso per gli utenti anonimi.

- **Abilitazione o disabilitazione della presentazione di ACL NTFS su volumi con sicurezza efficace UNIX (volumi di sicurezza UNIX o volumi di sicurezza misti con sicurezza effettiva UNIX)**

L'attivazione o la disattivazione di questa opzione determina il modo in cui la sicurezza dei file su file e cartelle con protezione UNIX viene presentata ai client SMB. Se abilitato, ONTAP presenta file e cartelle in volumi con protezione UNIX ai client SMB come dotati di protezione dei file NTFS con ACL NTFS. Se disattivato, ONTAP presenta i volumi con sicurezza UNIX come volumi FAT, senza alcuna protezione dei file. Per impostazione predefinita, i volumi presentano la protezione dei file NTFS con ACL NTFS.

- **Abilitazione o disabilitazione della funzionalità SMB finta aperta**

L'abilitazione di questa funzionalità migliora le performance di SMB 2.x e SMB 3.0 ottimizzando il modo in cui ONTAP effettua richieste aperte e ravvicinate quando si esegue una query per ottenere informazioni sugli attributi su file e directory. Per impostazione predefinita, la funzionalità SMB fake open è attivata. Questa opzione è utile solo per le connessioni effettuate con SMB 2.x o versioni successive.

- **Abilitazione o disabilitazione delle estensioni UNIX**

L'attivazione di questa opzione attiva le estensioni UNIX su un server SMB. Le estensioni UNIX consentono di visualizzare la sicurezza in stile POSIX/UNIX tramite il protocollo SMB. Per impostazione predefinita, questa opzione è disattivata.

Se si dispone di client SMB basati su UNIX, come i client Mac OSX, è necessario attivare le estensioni UNIX. L'abilitazione delle estensioni UNIX consente al server SMB di trasmettere le informazioni di sicurezza POSIX/UNIX tramite SMB al client basato su UNIX, che quindi traduce le informazioni di sicurezza in sicurezza POSIX/UNIX.

- **Abilitazione o disabilitazione del supporto per le ricerche di nomi brevi**

L'attivazione di questa opzione consente al server SMB di eseguire ricerche sui nomi brevi. Una query di ricerca con questa opzione attivata tenta di associare 8.3 nomi di file con nomi di file lunghi. Il valore

predefinito per questo parametro è `false`.

- **Abilitazione o disabilitazione del supporto per la pubblicità automatica delle funzionalità DFS**

L'attivazione o la disattivazione di questa opzione determina se i server SMB pubblicizzano automaticamente le funzionalità DFS ai client SMB 2.x e SMB 3.0 che si connettono alle condivisioni. ONTAP utilizza i riferimenti DFS nell'implementazione di collegamenti simbolici per l'accesso SMB. Se attivato, il server SMB comunica sempre le funzionalità DFS indipendentemente dall'attivazione dell'accesso tramite collegamento simbolico. Se disattivato, il server SMB comunica le funzionalità DFS solo quando i client si connettono alle condivisioni in cui è attivato l'accesso al collegamento simbolico.

- **Configurazione del numero massimo di crediti SMB**

A partire da ONTAP 9.4, configurazione di `-max-credits` L'opzione consente di limitare il numero di crediti da concedere su una connessione SMB quando client e server eseguono SMB versione 2 o successiva. Il valore predefinito è 128.

- **Abilitazione o disabilitazione del supporto per SMB multicanale**

Attivazione di `-is-multichannel-enabled` L'opzione di ONTAP 9.4 e versioni successive consente al server SMB di stabilire più connessioni per una singola sessione SMB quando vengono implementate le NIC appropriate sul cluster e sui relativi client. In questo modo si migliora il throughput e la tolleranza agli errori. Il valore predefinito per questo parametro è `false`.

Quando SMB Multichannel è attivato, è anche possibile specificare i seguenti parametri:

- Numero massimo di connessioni consentite per sessione multicanale. Il valore predefinito per questo parametro è 32.
- Il numero massimo di interfacce di rete pubblicizzate per ogni sessione multicanale. Il valore predefinito per questo parametro è 256.

## Configurazione delle opzioni del server SMB

È possibile configurare le opzioni del server SMB in qualsiasi momento dopo aver creato un server SMB su una macchina virtuale di storage (SVM).

### Fase

1. Eseguire l'azione desiderata:

Se si desidera configurare le opzioni del server SMB...	Immettere il comando...
A livello di privilegi di amministratore	<pre>vserver cifs options modify -vserver vserver_name options</pre>
A livello di privilegi avanzati	<pre>a. set -privilege advanced b. vserver cifs options modify    -vserver vserver_name options c. set -privilege admin</pre>

Per ulteriori informazioni sulla configurazione delle opzioni del server SMB, consultare la pagina man del

`vserver cifs options modify` comando.

### Configurare l'autorizzazione Grant UNIX group per gli utenti SMB

È possibile configurare questa opzione in modo da concedere ai gruppi le autorizzazioni di accesso ai file o alle directory anche se l'utente SMB in entrata non è il proprietario del file.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Configurare l'autorizzazione Grant UNIX group come appropriato:

Se lo si desidera	Immettere il comando
Abilitare l'accesso ai file o alle directory per ottenere le autorizzazioni di gruppo anche se l'utente non è il proprietario del file	<code>vserver cifs options modify -grant-unix-group-perms-to-others true</code>
Disattivare l'accesso ai file o alle directory per ottenere le autorizzazioni di gruppo anche se l'utente non è il proprietario del file	<code>vserver cifs options modify -grant-unix-group-perms-to-others false</code>

3. Verificare che l'opzione sia impostata sul valore desiderato: `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. Tornare al livello di privilegio admin: `set -privilege admin`

### Configurare le restrizioni di accesso per gli utenti anonimi

Per impostazione predefinita, un utente anonimo e non autenticato (noto anche come *null user*) può accedere a determinate informazioni sulla rete. È possibile utilizzare un'opzione del server SMB per configurare le restrizioni di accesso per l'utente anonimo.

#### A proposito di questa attività

Il `-restrict-anonymous` L'opzione del server SMB corrisponde a `RestrictAnonymous` Voce di registro in Windows.

Gli utenti anonimi possono elencare o enumerare determinati tipi di informazioni di sistema dagli host Windows sulla rete, inclusi i nomi e i dettagli degli utenti, i criteri degli account e i nomi di condivisione. È possibile controllare l'accesso per l'utente anonimo specificando una delle tre impostazioni di restrizione dell'accesso:

Valore	Descrizione
<code>no-restriction</code> (impostazione predefinita)	Non specifica restrizioni di accesso per utenti anonimi.
<code>no-enumeration</code>	Specifica che solo l'enumerazione è limitata per gli utenti anonimi.

Valore	Descrizione
no-access	Specifica che l'accesso è limitato agli utenti anonimi.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Configurare l'impostazione limita anonimo: `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`
3. Verificare che l'opzione sia impostata sul valore desiderato: `vserver cifs options show -vserver vserver_name`
4. Tornare al livello di privilegio admin: `set -privilege admin`

## Informazioni correlate

[Opzioni server SMB disponibili](#)

**Gestire il modo in cui la sicurezza dei file viene presentata ai client SMB per i dati di sicurezza UNIX**

**Gestire il modo in cui la sicurezza dei file viene presentata ai client SMB per una panoramica dei dati in stile di sicurezza UNIX**

Puoi scegliere come presentare la sicurezza dei file ai client SMB per i dati di sicurezza UNIX attivando o disattivando la presentazione degli ACL NTFS ai client SMB. Ogni impostazione offre vantaggi che è necessario comprendere per scegliere l'impostazione più adatta alle proprie esigenze di business.

Per impostazione predefinita, ONTAP presenta le autorizzazioni UNIX sui volumi UNIX di tipo Security ai client SMB come ACL NTFS. Esistono scenari in cui ciò è auspicabile, tra cui:

- Per visualizzare e modificare le autorizzazioni UNIX, utilizzare la scheda **Security** nella casella Proprietà di Windows.

Non è possibile modificare le autorizzazioni da un client Windows se l'operazione non è consentita dal sistema UNIX. Ad esempio, non è possibile modificare la proprietà di un file non proprietario, perché il sistema UNIX non consente questa operazione. Questa restrizione impedisce ai client SMB di ignorare le autorizzazioni UNIX impostate sui file e sulle cartelle.

- Gli utenti stanno modificando e salvando i file sul volume UNIX di sicurezza utilizzando alcune applicazioni Windows, ad esempio Microsoft Office, in cui ONTAP deve conservare le autorizzazioni UNIX durante le operazioni di salvataggio.
- Nell'ambiente sono presenti alcune applicazioni Windows che prevedono di leggere gli ACL NTFS sui file utilizzati.

In alcuni casi, è possibile disattivare la presentazione delle autorizzazioni UNIX come ACL NTFS. Se questa funzionalità è disattivata, ONTAP presenta i volumi UNIX di sicurezza come volumi FAT ai client SMB. Esistono motivi specifici per cui potresti voler presentare i volumi UNIX di sicurezza come volumi FAT ai client SMB:

- È possibile modificare le autorizzazioni UNIX solo utilizzando i mount sui client UNIX.

La scheda Security (sicurezza) non è disponibile quando un volume UNIX di tipo Security viene mappato su un client SMB. L'unità mappata sembra essere formattata con il file system FAT, che non dispone di

permessi per i file.

- Si stanno utilizzando applicazioni su SMB che impostano ACL NTFS su file e cartelle a cui si accede, il che può verificarsi se i dati risiedono su volumi UNIX di sicurezza.

Se ONTAP riporta il volume come FAT, l'applicazione non tenta di modificare un ACL.

## Informazioni correlate

[Configurazione degli stili di sicurezza sui volumi FlexVol](#)

[Configurazione degli stili di sicurezza sui qtrees](#)

## Abilitare o disabilitare la presentazione degli ACL NTFS per i dati di sicurezza UNIX

È possibile attivare o disattivare la presentazione degli ACL NTFS ai client SMB per i dati di sicurezza UNIX (volumi di sicurezza UNIX e volumi di sicurezza misti con protezione efficace UNIX).

### A proposito di questa attività

Se si attiva questa opzione, ONTAP presenta file e cartelle su volumi con uno stile di sicurezza UNIX efficace ai client SMB come dotati di ACL NTFS. Se si disattiva questa opzione, i volumi vengono presentati come volumi FAT ai client SMB. L'impostazione predefinita prevede la presentazione degli ACL NTFS ai client SMB.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Configurare l'impostazione dell'opzione UNIX NTFS ACL: `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. Verificare che l'opzione sia impostata sul valore desiderato: `vserver cifs options show -vserver vserver_name`
4. Tornare al livello di privilegio admin: `set -privilege admin`

## In che modo ONTAP conserva le autorizzazioni UNIX

Quando i file in un volume FlexVol che dispongono attualmente di autorizzazioni UNIX vengono modificati e salvati dalle applicazioni Windows, ONTAP può conservare le autorizzazioni UNIX.

Quando le applicazioni sui client Windows modificano e salvano i file, leggono le proprietà di protezione del file, creano un nuovo file temporaneo, applicano tali proprietà al file temporaneo e assegnano al file temporaneo il nome del file originale.

Quando i client Windows eseguono una query per le proprietà di protezione, ricevono un ACL costruito che rappresenta esattamente le autorizzazioni UNIX. L'unico scopo di questo ACL costruito è quello di preservare le autorizzazioni UNIX del file, poiché i file vengono aggiornati dalle applicazioni Windows per garantire che i file risultanti abbiano le stesse autorizzazioni UNIX. ONTAP non imposta alcun ACL NTFS utilizzando l'ACL costruito.

## Gestire le autorizzazioni UNIX utilizzando la scheda protezione di Windows

Se si desidera modificare le autorizzazioni UNIX di file o cartelle in volumi misti di



sicurezza o qtree su SVM, è possibile utilizzare la scheda Security (protezione) sui client Windows. In alternativa, è possibile utilizzare applicazioni in grado di eseguire query e impostare gli ACL di Windows.

- **Modifica delle autorizzazioni UNIX**

È possibile utilizzare la scheda protezione di Windows per visualizzare e modificare le autorizzazioni UNIX per un volume misto di sicurezza o qtree. Se si utilizza la scheda principale di Windows Security per modificare le autorizzazioni UNIX, è necessario rimuovere prima l'ACE esistente che si desidera modificare (in questo modo i bit di modalità vengono impostati su 0) prima di apportare le modifiche. In alternativa, è possibile utilizzare l'editor avanzato per modificare le autorizzazioni.

Se vengono utilizzate le autorizzazioni di modalità, è possibile modificare direttamente le autorizzazioni di modalità per UID, GID e altri (tutti gli altri utenti con un account sul computer). Ad esempio, se l'UID visualizzato dispone delle autorizzazioni r-x, è possibile modificare le autorizzazioni UID in rwx.

- **Modifica delle autorizzazioni UNIX in autorizzazioni NTFS**

È possibile utilizzare la scheda protezione di Windows per sostituire gli oggetti di protezione UNIX con oggetti di protezione di Windows su un volume misto di tipo sicurezza o qtree in cui i file e le cartelle hanno uno stile di protezione efficace UNIX.

Prima di poter sostituire le voci di autorizzazione UNIX con gli oggetti utente e gruppo di Windows desiderati, è necessario rimuovere tutte le voci di autorizzazione UNIX elencate. È quindi possibile configurare gli ACL basati su NTFS sugli oggetti utente e Gruppo di Windows. Rimuovendo tutti gli oggetti di protezione UNIX e aggiungendo solo utenti e gruppi Windows a un file o a una cartella in un volume o qtree misto di sicurezza, è possibile modificare lo stile di protezione effettivo del file o della cartella da UNIX a NTFS.

Quando si modificano le autorizzazioni di una cartella, il comportamento predefinito di Windows consiste nel propagare queste modifiche a tutte le sottocartelle e a tutti i file. Pertanto, se non si desidera propagare una modifica dello stile di protezione a tutte le cartelle figlio, le sottocartelle e i file, è necessario modificare l'impostazione di propagazione desiderata.

## **Gestire le impostazioni di sicurezza del server SMB**

### **In che modo ONTAP gestisce l'autenticazione dei client SMB**

Prima che gli utenti possano creare connessioni SMB per accedere ai dati contenuti nella SVM, devono essere autenticati dal dominio a cui appartiene il server SMB. Il server SMB supporta due metodi di autenticazione, Kerberos e NTLM (NTLMv1 o NTLMv2). Kerberos è il metodo predefinito utilizzato per autenticare gli utenti del dominio.

### **Autenticazione Kerberos**

ONTAP supporta l'autenticazione Kerberos durante la creazione di sessioni SMB autenticate.

Kerberos è il servizio di autenticazione principale di Active Directory. Il server Kerberos o il servizio KDC (Kerberos Key Distribution Center) memorizza e recupera informazioni sui principi di sicurezza in Active Directory. A differenza del modello NTLM, i client Active Directory che desiderano stabilire una sessione con un altro computer, ad esempio il server SMB, contattano direttamente un KDC per ottenere le proprie credenziali di sessione.

## Autenticazione NTLM

L'autenticazione del client NTLM viene eseguita utilizzando un protocollo di risposta alle sfide basato sulla conoscenza condivisa di un segreto specifico dell'utente basato su una password.

Se un utente crea una connessione SMB utilizzando un account utente Windows locale, l'autenticazione viene eseguita localmente dal server SMB utilizzando NTLMv2.

### Linee guida per le impostazioni di sicurezza del server SMB in una configurazione di disaster recovery SVM

Prima di creare una SVM configurata come destinazione di disaster recovery in cui l'identità non viene preservata (la `-identity-preserve` l'opzione è impostata su `false` Nella configurazione di SnapMirror), è necessario conoscere il modo in cui le impostazioni di sicurezza del server SMB vengono gestite sulla SVM di destinazione.

- Le impostazioni di sicurezza del server SMB non predefinite non vengono replicate nella destinazione.

Quando si crea un server SMB sulla SVM di destinazione, tutte le impostazioni di sicurezza del server SMB vengono impostate sui valori predefiniti. Quando la destinazione di disaster recovery SVM viene inizializzata, aggiornata o risincronizzata, le impostazioni di sicurezza del server SMB sull'origine non vengono replicate nella destinazione.

- È necessario configurare manualmente le impostazioni di sicurezza del server SMB non predefinite.

Se sono state configurate impostazioni di sicurezza del server SMB non predefinite sulla SVM di origine, è necessario configurare manualmente queste stesse impostazioni sulla SVM di destinazione dopo che la destinazione diventa di lettura/scrittura (dopo che la relazione SnapMirror è stata interrotta).

### Visualizza informazioni sulle impostazioni di sicurezza del server SMB

È possibile visualizzare informazioni sulle impostazioni di sicurezza dei server SMB sulle macchine virtuali dello storage (SVM). È possibile utilizzare queste informazioni per verificare che le impostazioni di protezione siano corrette.

#### A proposito di questa attività

Un'impostazione di protezione visualizzata può essere il valore predefinito per quell'oggetto o un valore non predefinito configurato utilizzando l'interfaccia CLI di ONTAP o gli oggetti Criteri di gruppo di Active Directory.

Non utilizzare `vserver cifs security show` Comando per i server SMB in modalità workgroup, perché alcune opzioni non sono valide.

#### Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su...	Immettere il comando...
Tutte le impostazioni di sicurezza su una SVM specificata	<code>vserver cifs security show -vserver vserver_name</code>

Se si desidera visualizzare informazioni su...	Immettere il comando...
Una o più impostazioni di sicurezza specifiche sulla SVM	<code>vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]</code> È possibile immettere <code>-fields ?</code> per determinare quali campi è possibile utilizzare.

## Esempio

L'esempio seguente mostra tutte le impostazioni di sicurezza per SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

Kerberos Clock Skew:          5 minutes
Kerberos Ticket Age:         10 hours
Kerberos Renewal Age:        7 days
Kerberos KDC Timeout:        3 seconds
Is Signing Required:         false
Is Password Complexity Required: true
Use start_tls For AD LDAP connection: false
Is AES Encryption Enabled:   false
LM Compatibility Level:      lm-ntlm-ntlmv2-krb
Is SMB Encryption Required:  false
Client Session Security:     none
SMB1 Enabled for DC Connections: false
SMB2 Enabled for DC Connections: system-default
LDAP Referral Enabled For AD LDAP connections: false
Use LDAPS for AD LDAP connection: false
Encryption is required for DC Connections: false
AES session key enabled for NetLogon channel: false
Try Channel Binding For AD LDAP Connections: false
```

Le impostazioni visualizzate dipendono dalla versione di ONTAP in esecuzione.

L'esempio seguente mostra l'inclinazione del clock Kerberos per SVM vs1:

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

vserver kerberos-clock-skew
-----
vs1      5
```

## Informazioni correlate

Attiva o disattiva la complessità della password richiesta per gli utenti SMB locali

La complessità richiesta delle password offre una maggiore sicurezza per gli utenti SMB locali sulle vostre macchine virtuali di storage (SVM). La funzione di complessità della password richiesta è attivata per impostazione predefinita. Puoi disattivarlo e riattivarlo in qualsiasi momento.

Prima di iniziare

Gli utenti locali, i gruppi locali e l'autenticazione dell'utente locale devono essere abilitati sul server CIFS.



A proposito di questa attività

Non utilizzare `vserver cifs security modify` Comando per un server CIFS in modalità gruppo di lavoro perché alcune opzioni non sono valide.

Fasi

- 1. Eseguire una delle seguenti operazioni:

Se si desidera che la complessità della password richiesta per gli utenti SMB locali sia...	Immettere il comando...
Attivato	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required true</code>
Disattivato	<code>vserver cifs security modify -vserver vserver_name -is-password-complexity -required false</code>

- 2. Verificare l'impostazione di sicurezza per la complessità della password richiesta: `vserver cifs security show -vserver vserver_name`

Esempio

L'esempio seguente mostra che la complessità della password richiesta è abilitata per gli utenti SMB locali per SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
-----
vs1      true
```

## Informazioni correlate

[Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS](#)

[Utilizzo di utenti e gruppi locali per l'autenticazione e l'autorizzazione](#)

[Requisiti per le password dell'utente locale](#)

[Modifica delle password degli account utente locali](#)

## Modificare le impostazioni di sicurezza Kerberos del server CIFS

È possibile modificare alcune impostazioni di sicurezza Kerberos del server CIFS, tra cui il tempo massimo consentito di disallineamento del clock Kerberos, la durata del ticket Kerberos e il numero massimo di giorni di rinnovo del ticket.

### A proposito di questa attività

Modifica delle impostazioni Kerberos del server CIFS mediante `vserver cifs security modify` Il comando modifica le impostazioni solo sulla singola SVM (Storage Virtual Machine) specificata con `-vserver` parametro. È possibile gestire centralmente le impostazioni di sicurezza Kerberos per tutte le SVM del cluster appartenenti allo stesso dominio Active Directory utilizzando gli oggetti Criteri di gruppo (GPO) di Active Directory.

### Fasi

1. Eseguire una o più delle seguenti operazioni:

Se si desidera...	Inserisci...
Specificare il tempo massimo consentito di inclinazione dell'orologio Kerberos in minuti (9.13.1 e successivi) o secondi (9.12.1 o precedenti).	<pre>vserver cifs security modify -vserver vserver_name -kerberos-clock-skew integer_in_minutes</pre> <p>L'impostazione predefinita è 5 minuti.</p>
Specificare la durata del ticket Kerberos in ore.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-ticket-age integer_in_hours</pre> <p>L'impostazione predefinita è 10 ore.</p>
Specificare il numero massimo di giorni di rinnovo del ticket.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-renew-age integer_in_days</pre> <p>L'impostazione predefinita è 7 giorni.</p>
Specificare il timeout per i socket sui KDC dopo il quale tutti i KDC sono contrassegnati come irraggiungibili.	<pre>vserver cifs security modify -vserver vserver_name -kerberos-kdc-timeout integer_in_seconds</pre> <p>L'impostazione predefinita è 3 secondi.</p>

## 2. Verificare le impostazioni di sicurezza Kerberos:

```
vserver cifs security show -vserver vserver_name
```

### Esempio

Nell'esempio seguente vengono apportate le seguenti modifiche alla sicurezza Kerberos: "Kerberos Clock Skew" (inclinazione clock Kerberos) è impostato su 3 minuti e "Kerberos Ticket Age" (durata ticket Kerberos) è impostato su 8 ore per SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew 3 -kerberos-ticket-age 8
```

```
cluster1::> vserver cifs security show -vserver vs1
```

Vserver: vs1

Kerberos Clock Skew:	3 minutes
Kerberos Ticket Age:	8 hours
Kerberos Renewal Age:	7 days
Kerberos KDC Timeout:	3 seconds
Is Signing Required:	false
Is Password Complexity Required:	true
Use start_tls For AD LDAP connection:	false
Is AES Encryption Enabled:	false
LM Compatibility Level:	lm-ntlm-ntlmv2-krb
Is SMB Encryption Required:	false

### Informazioni correlate

["Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS"](#)

["GPO supportati"](#)

["Applicazione di oggetti Criteri di gruppo ai server CIFS"](#)

### Impostare il livello minimo di sicurezza per l'autenticazione del server SMB

È possibile impostare il livello di sicurezza minimo del server SMB, noto anche come *LMCompatibilityLevel*, sul server SMB per soddisfare i requisiti di sicurezza aziendali per l'accesso al client SMB. Il livello di sicurezza minimo è il livello minimo dei token di sicurezza che il server SMB accetta dai client SMB.



#### A proposito di questa attività

- I server SMB in modalità workgroup supportano solo l'autenticazione NTLM. L'autenticazione Kerberos non è supportata.
- LMCompatibilityLevel si applica solo all'autenticazione del client SMB, non all'autenticazione dell'amministratore.

È possibile impostare il livello di sicurezza minimo per l'autenticazione su uno dei quattro livelli di sicurezza supportati.

Valore	Descrizione
lm-ntlm-ntlmv2-krb (impostazione predefinita)	La macchina virtuale per lo storage (SVM) accetta la protezione con autenticazione LM, NTLM, NTLMv2 e Kerberos.
ntlm-ntlmv2-krb	SVM accetta la sicurezza di autenticazione NTLM, NTLMv2 e Kerberos. SVM nega l'autenticazione LM.
ntlmv2-krb	SVM accetta la sicurezza di autenticazione NTLMv2 e Kerberos. SVM nega l'autenticazione LM e NTLM.
krb	SVM accetta solo la sicurezza con autenticazione Kerberos. SVM nega l'autenticazione LM, NTLM e NTLMv2.

## Fasi

1. Impostare il livello minimo di protezione per l'autenticazione: `vserver cifs security modify -vserver vserver_name -lm-compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. Verificare che il livello di protezione per l'autenticazione sia impostato sul livello desiderato: `vserver cifs security show -vserver vserver_name`

## Informazioni correlate

[Attivazione o disattivazione della crittografia AES per le comunicazioni basate su Kerberos](#)

### Configurare una protezione avanzata per le comunicazioni basate su Kerberos utilizzando la crittografia AES

Per una maggiore sicurezza con la comunicazione basata su Kerberos, è possibile attivare la crittografia AES-256 e AES-128 sul server SMB. Per impostazione predefinita, quando si crea un server SMB su SVM, la crittografia AES (Advanced Encryption Standard) viene disattivata. È necessario abilitarlo per sfruttare la protezione avanzata fornita dalla crittografia AES.

La comunicazione relativa a Kerberos per SMB viene utilizzata durante la creazione del server SMB sulla SVM e durante la fase di configurazione della sessione SMB. Il server SMB supporta i seguenti tipi di crittografia per le comunicazioni Kerberos:

- AES 256
- AES 128
- DES
- RC4-HMAC

Se si desidera utilizzare il tipo di crittografia con la massima protezione per le comunicazioni Kerberos, è necessario attivare la crittografia AES per le comunicazioni Kerberos su SVM.

Quando viene creato il server SMB, il controller di dominio crea un account computer in Active Directory. A questo punto, il KDC viene a conoscenza delle funzionalità di crittografia di un determinato account di computer. Successivamente, viene selezionato un particolare tipo di crittografia per crittografare il ticket di servizio che il client presenta al server durante l'autenticazione.

A partire da ONTAP 9.12.1, è possibile specificare i tipi di crittografia da segnalare al KDC di Active Directory (ad). È possibile utilizzare `-advertised-enc-types` opzione per attivare i tipi di crittografia consigliati ed è possibile utilizzarla per disattivare i tipi di crittografia più deboli. Scopri come ["Attiva e disattiva i tipi di crittografia per le comunicazioni basate su Kerberos"](#).



Intel AES New Instructions (Intel AES NI) è disponibile in SMB 3.0, migliorando l'algoritmo AES e accelerando la crittografia dei dati con le famiglie di processori supportate. A partire da SMB 3.1.1, AES-128-GCM sostituisce AES-128-CCM come algoritmo hash utilizzato dalla crittografia SMB.

## Informazioni correlate

[Modifica delle impostazioni di sicurezza Kerberos del server CIFS](#)

### Attiva o disattiva la crittografia AES per le comunicazioni basate su Kerberos

Per sfruttare al massimo la protezione della comunicazione basata su Kerberos, è necessario utilizzare la crittografia AES-256 e AES-128 sul server SMB. A partire da ONTAP 9.13.1, la crittografia AES è attivata per impostazione predefinita. Se non si desidera che il server SMB selezioni i tipi di crittografia AES per la comunicazione basata su Kerberos con Active Directory (ad) KDC, è possibile disattivare la crittografia AES.

Se la crittografia AES è attivata per impostazione predefinita e se si dispone dell'opzione per specificare i tipi di crittografia, dipende dalla versione di ONTAP in uso.

Versione di ONTAP	La crittografia AES è abilitata ...	È possibile specificare i tipi di crittografia?
9.13.1 e versioni successive	Per impostazione predefinita	Sì
9.12.1	Manualmente	Sì
9.11.1 e precedenti	Manualmente	No

A partire da ONTAP 9.12.1, la crittografia AES viene attivata e disattivata tramite `-advertised-enc-types`. Che consente di specificare i tipi di crittografia annunciati a ad KDC. L'impostazione predefinita è `rc4` e `des`. Ma quando viene specificato un tipo AES, viene attivata la crittografia AES. È inoltre possibile utilizzare l'opzione per disattivare esplicitamente i tipi di crittografia RC4 e DES più deboli. In ONTAP 9.11.1 e versioni precedenti, è necessario utilizzare `-is-aes-encryption-enabled` Opzione per attivare e disattivare la crittografia AES e i tipi di crittografia non possono essere specificati.

Per migliorare la sicurezza, la macchina virtuale di storage (SVM) modifica la password dell'account della macchina in ad ogni volta che viene modificata l'opzione di sicurezza AES. La modifica della password potrebbe richiedere credenziali amministrative ad per l'unità organizzativa (OU) che contiene l'account del computer.

Se una SVM è configurata come destinazione di disaster recovery in cui l'identità non viene preservata (la `-identity-preserve` l'opzione è impostata su `false` Nella configurazione di SnapMirror), le impostazioni di sicurezza del server SMB non predefinite non vengono replicate nella destinazione. Se è stata attivata la crittografia AES sulla SVM di origine, è necessario abilitarla manualmente.



## Esempio 5. Fasi

### ONTAP 9.12.1 e versioni successive

1. Eseguire una delle seguenti operazioni:

Se si desidera che i tipi di crittografia AES per la comunicazione Kerberos siano...	Immettere il comando...
Attivato	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256</pre>
Disattivato	<pre>vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4</pre>

**Nota:** la `-is-aes-encryption-enabled` L'opzione è obsoleta in ONTAP 9.12.1 e potrebbe essere rimossa in una release successiva.

2. Verificare che la crittografia AES sia attivata o disattivata come desiderato: `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

### Esempi

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc  
-types aes-128,aes-256  
  
cluster1::> vserver cifs security show -vserver vs1 -fields advertised-  
enc-types  
  
vserver  advertised-enc-types  
-----  
vs1      aes-128,aes-256
```

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs2. All'amministratore viene richiesto di inserire le credenziali amministrative ad per l'unità organizzativa contenente il server SMB.

```
cluster1::> vsriver cifs security modify -vsriver vs2 -advertised-enc
-types aes-128,aes-256
```

Info: In order to enable SMB AES encryption, the password for the SMB server machine account must be reset. Enter the username and password for the SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

```
cluster1::> vsriver cifs security show -vsriver vs2 -fields advertised-
enc-types
```

```
vsriver  advertised-enc-types
-----  -----
vs2      aes-128,aes-256
```

## ONTAP 9.11.1 e versioni precedenti

1. Eseguire una delle seguenti operazioni:

Se si desidera che i tipi di crittografia AES per la comunicazione Kerberos siano...	Immettere il comando...
Attivato	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled true</pre>
Disattivato	<pre>vsriver cifs security modify -vsriver vsriver_name -is-aes -encryption-enabled false</pre>

2. Verificare che la crittografia AES sia attivata o disattivata come desiderato: 

```
vsriver cifs security show -vsriver vsriver_name -fields is-aes-encryption-enabled
```

Il `is-aes-encryption-enabled` viene visualizzato il campo `true` Se la crittografia AES è attivata e. `false` se è disattivato.

## Esempi

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs1      true
```

Nell'esempio seguente vengono utilizzati i tipi di crittografia AES per il server SMB su SVM vs2. All'amministratore viene richiesto di inserire le credenziali amministrative ad per l'unità organizzativa contenente il server SMB.

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-----
vs2      true
```

**Utilizza la firma SMB per migliorare la sicurezza di rete**

**Utilizza la firma SMB per migliorare la panoramica sulla sicurezza di rete**

La firma SMB aiuta a garantire che il traffico di rete tra il server SMB e il client non venga compromesso, evitando attacchi di replay. Per impostazione predefinita, ONTAP supporta la firma SMB quando richiesto dal client. Facoltativamente, l'amministratore dello storage può configurare il server SMB in modo che richieda la firma SMB.

## In che modo i criteri di firma SMB influiscono sulla comunicazione con un server CIFS

Oltre alle impostazioni di sicurezza della firma SMB del server CIFS, due criteri di firma SMB sui client Windows controllano la firma digitale delle comunicazioni tra i client e il server CIFS. È possibile configurare l'impostazione che soddisfa i requisiti di business.

I criteri SMB dei client sono controllati tramite le impostazioni dei criteri di protezione locali di Windows, che vengono configurate utilizzando Microsoft Management Console (MMC) o gli oggetti Criteri di gruppo di Active Directory. Per ulteriori informazioni sulla firma SMB del client e sui problemi di sicurezza, consultare la documentazione di Microsoft Windows.

Di seguito sono riportate le descrizioni dei due criteri di firma SMB sui client Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

Questa impostazione controlla se la funzionalità di firma SMB del client è attivata. È attivato per impostazione predefinita. Quando questa impostazione è disattivata sul client, le comunicazioni del client con il server CIFS dipendono dall'impostazione della firma SMB sul server CIFS.

- `Microsoft network client: Digitally sign communications (always)`

Questa impostazione specifica se il client richiede la firma SMB per comunicare con un server. È disattivato per impostazione predefinita. Quando questa impostazione è disattivata sul client, il comportamento della firma SMB si basa sull'impostazione del criterio per `Microsoft network client: Digitally sign communications (if server agrees)` E l'impostazione sul server CIFS.



Se l'ambiente include client Windows configurati per richiedere la firma SMB, è necessario attivare la firma SMB sul server CIFS. In caso contrario, il server CIFS non può fornire dati a questi sistemi.

I risultati effettivi delle impostazioni di firma SMB del client e del server CIFS dipendono dal fatto che le sessioni SMB utilizzino SMB 1.0 o SMB 2.x e versioni successive.

La seguente tabella riassume il comportamento effettivo della firma SMB se la sessione utilizza SMB 1.0:

Client	ONTAP - Firma non richiesta	ONTAP—Firma obbligatoria
Firma disattivata e non richiesta	Non firmato	Firmato
Firma abilitata e non richiesta	Non firmato	Firmato
Firma disattivata e obbligatoria	Firmato	Firmato
Firma abilitata e obbligatoria	Firmato	Firmato



I client SMB 1 di Windows meno recenti e alcuni client SMB 1 non Windows potrebbero non riuscire a connettersi se la firma è disattivata sul client ma richiesta sul server CIFS.

La seguente tabella riassume il comportamento effettivo della firma SMB se la sessione utilizza SMB 2.x o SMB 3.0:



Per i client SMB 2.x e SMB 3.0, la firma SMB è sempre abilitata. Non può essere disattivato.

Client	ONTAP - Firma non richiesta	ONTAP—Firma obbligatoria
Firma non richiesta	Non firmato	Firmato
Firma obbligatoria	Firmato	Firmato

La seguente tabella riassume il comportamento predefinito della firma SMB del client e del server Microsoft:

Protocollo	Algoritmo hash	Può attivare/disattivare	Può richiedere/non richiedere	Impostazione predefinita del client	Server predefinito	DC predefinito
SMB 1.0	MD5	Sì	Sì	Abilitato (non richiesto)	Disattivato (non richiesto)	Obbligatorio
SMB 2.x	HMAC SHA-256	No	Sì	Non richiesto	Non richiesto	Obbligatorio
SMB 3.0	AES-CMAC.	No	Sì	Non richiesto	Non richiesto	Obbligatorio



Microsoft sconsiglia di utilizzare `Digitally sign communications (if client agrees)` oppure `Digitally sign communications (if server agrees)` Impostazioni di Criteri di gruppo. Microsoft non consiglia più di utilizzare `EnableSecuritySignature` impostazioni del registro di sistema. Queste opzioni influiscono solo sul comportamento di SMB 1 e possono essere sostituite da `Digitally sign communications (always)` Impostazione di Criteri di gruppo o l'`RequireSecuritySignature` impostazione del registro di sistema. È inoltre possibile ottenere ulteriori informazioni dal Microsoft Blog.<http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx>[The Basics of SMB Signing (informazioni di base sulla firma SMB) (che riguardano sia SMB1 che SMB2)]

## Impatto delle performance della firma SMB

Quando le sessioni SMB utilizzano la firma SMB, tutte le comunicazioni SMB da e verso i client Windows hanno un impatto sulle performance, che influisce sia sui client che sul server (ovvero sui nodi del cluster che eseguono la SVM contenente il server SMB).

L'impatto delle performance si presenta come un aumento dell'utilizzo della CPU sia sui client che sul server, anche se la quantità di traffico di rete non cambia.

L'entità dell'impatto delle performance dipende dalla versione di ONTAP 9 in esecuzione. A partire da ONTAP 9.7, un nuovo algoritmo di crittografia off-load può consentire migliori performance nel traffico SMB firmato. L'offload della firma SMB è attivato per impostazione predefinita quando è attivata la firma SMB.

Le migliori performance di firma SMB richiedono la funzionalità di offload AES-NI. Consultare Hardware Universe (HWU) per verificare che l'offload AES-NI sia supportato per la piattaforma.

Ulteriori miglioramenti delle prestazioni sono possibili anche se si è in grado di utilizzare SMB versione 3,11

che supporta l'algoritmo GCM molto più veloce.

A seconda della rete, della versione di ONTAP 9, della versione SMB e dell'implementazione di SVM, l'impatto delle performance della firma SMB può variare notevolmente; è possibile verificarlo solo tramite test nell'ambiente di rete.

La maggior parte dei client Windows negozia la firma SMB per impostazione predefinita, se attivata sul server. Se si richiede la protezione SMB per alcuni client Windows e se la firma SMB causa problemi di performance, è possibile disattivare la firma SMB su qualsiasi client Windows che non richieda protezione contro gli attacchi di replay. Per informazioni sulla disattivazione della firma SMB sui client Windows, consultare la documentazione di Microsoft Windows.

### Consigli per la configurazione della firma SMB

È possibile configurare il comportamento della firma SMB tra i client SMB e il server CIFS per soddisfare i requisiti di sicurezza. Le impostazioni scelte durante la configurazione della firma SMB sul server CIFS dipendono dai requisiti di sicurezza.

È possibile configurare la firma SMB sul client o sul server CIFS. Durante la configurazione della firma SMB, prendere in considerazione i seguenti consigli:

Se...	Consiglio...
Si desidera aumentare la sicurezza della comunicazione tra il client e il server	Rendere necessaria la firma SMB sul client abilitando il Require Option (Sign always) impostazione di sicurezza sul client.
Si desidera che tutto il traffico SMB verso una determinata macchina virtuale di storage (SVM) sia firmato	Rendere necessaria la firma SMB sul server CIFS configurando le impostazioni di sicurezza in modo che richiedano la firma SMB.

Per ulteriori informazioni sulla configurazione delle impostazioni di sicurezza del client Windows, consultare la documentazione Microsoft.

### Linee guida per la firma SMB quando sono configurati LIFS di dati multipli

Se si attiva o disattiva la firma SMB richiesta sul server SMB, è necessario conoscere le linee guida per le configurazioni LIFS di dati multipli per una SVM.

Quando si configura un server SMB, potrebbero essere configurate più LIF di dati. In tal caso, il server DNS contiene più server A Registrare le voci per il server CIFS, utilizzando tutti lo stesso nome host del server SMB, ma ciascuna con un indirizzo IP univoco. Ad esempio, un server SMB con due LIF dati configurati potrebbe avere il seguente DNS A voci di record:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

Il comportamento normale è che, quando si modifica l'impostazione richiesta per la firma SMB, solo le nuove connessioni dai client vengono influenzate dalla modifica dell'impostazione della firma SMB. Tuttavia, esiste un'eccezione a questo comportamento. Esiste un caso in cui un client dispone di una connessione esistente a

una condivisione e il client crea una nuova connessione alla stessa condivisione dopo la modifica dell'impostazione, mantenendo la connessione originale. In questo caso, sia la connessione SMB nuova che quella esistente adottano i nuovi requisiti per la firma SMB.

Si consideri il seguente esempio:

1. Client1 si connette a una condivisione senza la firma SMB richiesta utilizzando il percorso `o:\`.
2. L'amministratore dello storage modifica la configurazione del server SMB per richiedere la firma SMB.
3. Client1 si connette alla stessa condivisione con la firma SMB richiesta utilizzando il percorso `s:\` (mantenendo la connessione utilizzando il percorso `o:\`).
4. Il risultato è che la firma SMB viene utilizzata quando si accede ai dati su entrambi `o:\` e `s:\` dischi.

### Attiva o disattiva la firma SMB richiesta per il traffico SMB in entrata

È possibile applicare il requisito per i client di firmare i messaggi SMB attivando la firma SMB richiesta. Se attivato, ONTAP accetta i messaggi SMB solo se dispongono di firme valide. Se si desidera consentire la firma SMB, ma non la si desidera, è possibile disattivare la firma SMB richiesta.

#### A proposito di questa attività

Per impostazione predefinita, la firma SMB richiesta è disattivata. È possibile attivare o disattivare la firma SMB richiesta in qualsiasi momento.

La firma SMB non viene disattivata per impostazione predefinita nei seguenti casi:



1. La firma SMB richiesta è attivata e il cluster viene reinstallato su una versione di ONTAP che non supporta la firma SMB.
2. Il cluster viene successivamente aggiornato a una versione di ONTAP che supporta la firma SMB.

In queste circostanze, la configurazione della firma SMB originariamente configurata su una versione supportata di ONTAP viene mantenuta attraverso la reversione e il successivo aggiornamento.

Quando si imposta una relazione di disaster recovery SVM (Storage Virtual Machine), il valore selezionato per `-identity-preserve` opzione di `snapmirror create` Determina i dettagli di configurazione replicati nella SVM di destinazione.

Se si imposta `-identity-preserve` opzione a `true` (ID-Preserve), l'impostazione di protezione della firma SMB viene replicata nella destinazione.

Se si imposta `-identity-preserve` opzione a `false` (Non-ID-Preserve), l'impostazione di protezione della firma SMB non viene replicata nella destinazione. In questo caso, le impostazioni di sicurezza del server CIFS sulla destinazione vengono impostate sui valori predefiniti. Se è stata attivata la firma SMB richiesta sulla SVM di origine, è necessario attivare manualmente la firma SMB richiesta sulla SVM di destinazione.

#### Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera che la firma SMB richiesta sia...	Immettere il comando...
Attivato	<code>vserver cifs security modify -vserver vserver_name -is-signing-required true</code>
Disattivato	<code>vserver cifs security modify -vserver vserver_name -is-signing-required false</code>

- Verificare che la firma SMB richiesta sia attivata o disattivata determinando se il valore in `Is Signing Required` nell'output del seguente comando viene impostato il valore desiderato: `vserver cifs security show -vserver vserver_name -fields is-signing-required`

### Esempio

L'esempio seguente abilita la firma SMB richiesta per SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-required
vserver  is-signing-required
-----  -
vs1      true
```



Le modifiche alle impostazioni di crittografia sono valide per le nuove connessioni. Le connessioni esistenti non sono interessate.

### Determinare se le sessioni SMB sono firmate

È possibile visualizzare le informazioni sulle sessioni SMB connesse sul server CIFS. È possibile utilizzare queste informazioni per determinare se le sessioni SMB sono firmate. Questo può essere utile per determinare se le sessioni del client SMB si connettono con le impostazioni di sicurezza desiderate.

#### Fasi

- Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su...	Immettere il comando...
Tutte le sessioni firmate su una specifica macchina virtuale di storage (SVM)	<code>vserver cifs session show -vserver vserver_name -is-session-signed true</code>
Dettagli di una sessione firmata con un ID di sessione specifico sulla SVM	<code>vserver cifs session show -vserver vserver_name -session-id integer -instance</code>



## Esempi

Il seguente comando visualizza le informazioni sulla sessione relative alle sessioni firmate su SVM vs1. L'output di riepilogo predefinito non visualizza il campo di output "is Session Signed":

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:      node1
Vserver:   vs1
Connection Session
ID          ID      Workstation      Windows User      Open      Idle
-----
3151272279  1      10.1.1.1      DOMAIN\joe      2      23s
```

Il seguente comando visualizza informazioni dettagliate sulla sessione, incluso se la sessione è firmata, in una sessione SMB con un ID sessione 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

## Informazioni correlate

[Monitoraggio delle statistiche delle sessioni firmate SMB](#)

### Monitorare le statistiche delle sessioni firmate SMB

È possibile monitorare le statistiche delle sessioni SMB e determinare quali sessioni stabilite sono firmate e quali no.

**A proposito di questa attività**

Il `statistics` il comando al livello di privilegio avanzato fornisce `signed_sessions` Contatore che è possibile utilizzare per monitorare il numero di sessioni SMB firmate. Il `signed_sessions` il contatore è disponibile con i seguenti oggetti di statistiche:

- `cifs` Consente di monitorare la firma SMB per tutte le sessioni SMB.
- `smb1` Consente di monitorare la firma SMB per le sessioni SMB 1.0.
- `smb2` Consente di monitorare la firma SMB per le sessioni SMB 2.x e SMB 3.0.

Le statistiche SMB 3.0 sono incluse nell'output di `smb2` oggetto.

Se si desidera confrontare il numero di sessioni firmate con il numero totale di sessioni, è possibile confrontare l'output per `signed_sessions` contatore con l'output per `established_sessions` contatore.

È necessario avviare una raccolta di campioni di statistiche prima di poter visualizzare i dati risultanti. Se non si interrompe la raccolta dei dati, è possibile visualizzare i dati del campione. L'interruzione della raccolta dei dati fornisce un campione fisso. La mancata interruzione della raccolta dei dati consente di ottenere dati aggiornati da utilizzare per il confronto con le query precedenti. Il confronto può aiutarti a identificare le tendenze.

**Fasi**

1. Impostare il livello di privilegio su Advanced:  
`set -privilege advanced`
2. Avviare una raccolta di dati:  
`statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]`

Se non si specifica `-sample-id` Il comando genera un identificatore di esempio e definisce questo campione come campione predefinito per la sessione CLI. Il valore per `-sample-id` è una stringa di testo. Se si esegue questo comando durante la stessa sessione CLI e non si specifica `-sample-id` il comando sovrascrive il campione predefinito precedente.

È possibile specificare il nodo su cui si desidera raccogliere le statistiche. Se non si specifica il nodo, l'esempio raccoglie le statistiche per tutti i nodi nel cluster.

3. Utilizzare `statistics stop` comando per interrompere la raccolta dei dati per il campione.
4. Visualizzare le statistiche della firma SMB:

Se si desidera visualizzare informazioni per...	Inserisci...
Sessioni firmate	<code>`show -sample-id sample_ID -counter signed_sessions`</code>
<code>node_name [-node node_name]</code>	Sessioni firmate e sessioni stabilite
<code>`show -sample-id sample_ID -counter signed_sessions`</code>	<code>established_sessions</code>

Se si desidera visualizzare le informazioni solo per un singolo nodo, specificare l'opzione `-node`

parametro.

5. Tornare al livello di privilegio admin:  
set -privilege admin

## Esempi

L'esempio seguente mostra come monitorare le statistiche di firma SMB 2.x e SMB 3.0 su Storage Virtual Machine (SVM) vs1.

Il seguente comando passa al livello di privilegio avanzato:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

Il seguente comando avvia la raccolta dati per un nuovo campione:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample  
-vserver vs1
```

```
Statistics collection is being started for Sample-id: smbsigning_sample
```

Il seguente comando interrompe la raccolta di dati per l'esempio:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
```

```
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

Il seguente comando mostra le sessioni SMB firmate e le sessioni SMB stabilite per nodo dell'esempio:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|established_sessions|node_name
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:03:04

Cluster: cluster1

Counter	Value
-----	-----
established_sessions	0
node_name	node1
signed_sessions	0
established_sessions	1
node_name	node2
signed_sessions	1
established_sessions	0
node_name	node3
signed_sessions	0
established_sessions	0
node_name	node4
signed_sessions	0

Il seguente comando mostra le sessioni SMB firmate per node2 dell'esempio:

```
cluster1::*> statistics show -sample-id smbSigning_sample -counter
signed_sessions|node_name -node node2
```

Object: smb2

Instance: vs1

Start-time: 2/6/2013 01:00:00

End-time: 2/6/2013 01:22:43

Cluster: cluster1

Counter	Value
-----	-----
node_name	node2
signed_sessions	1

Il seguente comando torna al livello di privilegio admin:

```
cluster1::*> set -privilege admin
```

## Informazioni correlate

[Determinare se le sessioni SMB sono firmate](#)

["Panoramica sulla gestione e sul monitoraggio delle performance"](#)

**Configurare la crittografia SMB richiesta sui server SMB per il trasferimento dei dati su SMB**

### Panoramica sulla crittografia SMB

La crittografia SMB per i trasferimenti di dati su SMB è un miglioramento della sicurezza che è possibile attivare o disattivare sui server SMB. È inoltre possibile configurare l'impostazione di crittografia SMB desiderata in base alla condivisione mediante un'impostazione di proprietà di condivisione.

Per impostazione predefinita, quando si crea un server SMB sulla Storage Virtual Machine (SVM), la crittografia SMB viene disattivata. È necessario abilitarlo per sfruttare la sicurezza avanzata fornita dalla crittografia SMB.

Per creare una sessione SMB crittografata, il client SMB deve supportare la crittografia SMB. I client Windows che iniziano con Windows Server 2012 e Windows 8 supportano la crittografia SMB.

La crittografia SMB sulla SVM è controllata da due impostazioni:

- Un'opzione di sicurezza per server SMB che attiva la funzionalità sulla SVM
- Una proprietà di condivisione SMB che configura l'impostazione di crittografia SMB in base alla condivisione

È possibile decidere se richiedere la crittografia per l'accesso a tutti i dati sulla SVM o se richiedere la crittografia SMB per accedere ai dati solo nelle condivisioni selezionate. Le impostazioni a livello di SVM sostituiscono quelle a livello di condivisione.

La configurazione effettiva della crittografia SMB dipende dalla combinazione delle due impostazioni ed è descritta nella tabella seguente:

<b>Crittografia SMB server abilitata</b>	<b>Share encoded data Setting Enabled (Condividi dati crittografati)</b>	<b>Comportamento della crittografia lato server</b>
Vero	Falso	La crittografia a livello di server è attivata per tutte le condivisioni di SVM. Con questa configurazione, la crittografia viene eseguita per l'intera sessione SMB.
Vero	Vero	La crittografia a livello di server è attivata per tutte le condivisioni di SVM, indipendentemente dalla crittografia a livello di condivisione. Con questa configurazione, la crittografia viene eseguita per l'intera sessione SMB.

<b>Crittografia SMB server abilitata</b>	<b>Share encoded data Setting Enabled (Condividi dati crittografati)</b>	<b>Comportamento della crittografia lato server</b>
Falso	Vero	La crittografia a livello di condivisione è attivata per le condivisioni specifiche. Con questa configurazione, la crittografia viene eseguita dalla connessione ad albero.
Falso	Falso	Nessuna crittografia abilitata.

I client SMB che non supportano la crittografia non possono connettersi a un server SMB o a una condivisione che richiede la crittografia.

Le modifiche alle impostazioni di crittografia sono valide per le nuove connessioni. Le connessioni esistenti non sono interessate.

### **Impatto delle performance della crittografia SMB**

Quando le sessioni SMB utilizzano la crittografia SMB, tutte le comunicazioni SMB da e verso i client Windows hanno un impatto sulle performance, che influisce sia sui client che sul server (ovvero sui nodi del cluster che eseguono la SVM che contiene il server SMB).

L'impatto delle performance si presenta come un aumento dell'utilizzo della CPU sia sui client che sul server, anche se la quantità di traffico di rete non cambia.

L'entità dell'impatto delle performance dipende dalla versione di ONTAP 9 in esecuzione. A partire da ONTAP 9.7, un nuovo algoritmo di crittografia off-load può consentire migliori performance nel traffico SMB crittografato. L'offload della crittografia SMB è attivato per impostazione predefinita quando la crittografia SMB è attivata.

Le performance di crittografia SMB avanzate richiedono la funzionalità di offload AES-NI. Consultare Hardware Universe (HWU) per verificare che l'offload AES-NI sia supportato per la piattaforma.

Ulteriori miglioramenti delle prestazioni sono possibili anche se si è in grado di utilizzare SMB versione 3,11 che supporta l'algoritmo GCM molto più veloce.

A seconda della rete, della versione di ONTAP 9, della versione SMB e dell'implementazione di SVM, l'impatto delle performance della crittografia SMB può variare notevolmente; è possibile verificarlo solo tramite test nell'ambiente di rete.

La crittografia SMB è disattivata per impostazione predefinita sul server SMB. È necessario attivare la crittografia SMB solo sulle condivisioni SMB o sui server SMB che richiedono la crittografia. Con la crittografia SMB, ONTAP esegue un'ulteriore elaborazione della decifratura delle richieste e della crittografia delle risposte per ogni richiesta. La crittografia SMB deve quindi essere attivata solo quando necessario.

### **Attiva o disattiva la crittografia SMB richiesta per il traffico SMB in entrata**

Se si desidera richiedere la crittografia SMB per il traffico SMB in entrata, è possibile

attivarla sul server CIFS o a livello di condivisione. Per impostazione predefinita, la crittografia SMB non è richiesta.

**A proposito di questa attività**

È possibile attivare la crittografia SMB sul server CIFS, che si applica a tutte le condivisioni sul server CIFS. Se non si desidera la crittografia SMB richiesta per tutte le condivisioni sul server CIFS o se si desidera attivare la crittografia SMB richiesta per il traffico SMB in entrata su base share-by-share, è possibile disattivare la crittografia SMB richiesta sul server CIFS.

Quando si imposta una relazione di disaster recovery SVM (Storage Virtual Machine), il valore selezionato per `-identity-preserve` opzione di `snapmirror create` Determina i dettagli di configurazione replicati nella SVM di destinazione.

Se si imposta `-identity-preserve` opzione a `true` (ID-Preserve), l'impostazione di sicurezza della crittografia SMB viene replicata nella destinazione.

Se si imposta `-identity-preserve` opzione a `false` (Non-ID-Preserve), l'impostazione di sicurezza della crittografia SMB non viene replicata nella destinazione. In questo caso, le impostazioni di sicurezza del server CIFS sulla destinazione vengono impostate sui valori predefiniti. Se è stata attivata la crittografia SMB sulla SVM di origine, è necessario attivare manualmente la crittografia SMB del server CIFS sulla destinazione.

**Fasi**

- 1. Eseguire una delle seguenti operazioni:

Se si desidera che la crittografia SMB richiesta per il traffico SMB in entrata sul server CIFS sia...	Immettere il comando...
Attivato	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required true</code>
Disattivato	<code>vserver cifs security modify -vserver vserver_name -is-smb-encryption -required false</code>

- 2. Verificare che la crittografia SMB richiesta sul server CIFS sia attivata o disattivata come desiderato:  
`vserver cifs security show -vserver vserver_name -fields is-smb-encryption-required`  
  
Il `is-smb-encryption-required` viene visualizzato il campo `true` Se necessario, la crittografia SMB è attivata sul server CIFS e. `false` se è disattivato.

**Esempio**

Nell'esempio seguente viene attivata la crittografia SMB richiesta per il traffico SMB in entrata per il server CIFS su SVM vs1:



```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----
vs1      true
```

## Determinare se i client sono connessi utilizzando sessioni SMB crittografate

È possibile visualizzare informazioni sulle sessioni SMB connesse per determinare se i client utilizzano connessioni SMB crittografate. Questo può essere utile per determinare se le sessioni del client SMB si connettono con le impostazioni di sicurezza desiderate.

### A proposito di questa attività

Le sessioni dei client SMB possono avere uno dei tre livelli di crittografia seguenti:

- `unencrypted`

La sessione SMB non è crittografata. Non è stata configurata la crittografia a livello di SVM (Storage Virtual Machine) o a livello di condivisione.

- `partially-encrypted`

La crittografia viene avviata quando si verifica la connessione ad albero. La crittografia a livello di condivisione è configurata. La crittografia a livello di SVM non è attivata.

- `encrypted`

La sessione SMB è completamente crittografata. La crittografia a livello di SVM è attivata. La crittografia a livello di condivisione potrebbe non essere attivata. L'impostazione di crittografia a livello di SVM sostituisce l'impostazione di crittografia a livello di condivisione.

### Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su...	Immettere il comando...
Sessioni con un'impostazione di crittografia specificata per le sessioni su una SVM specificata	<code>`vserver cifs session show -vserver <i>vserver_name</i> {unencrypted</code>
<code>partially-encrypted</code>	<code>encrypted} -instance`</code>
L'impostazione di crittografia per un ID sessione specifico su una SVM specificata	<code>vserver cifs session show -vserver <i>vserver_name</i> -session-id <i>integer</i> -instance</code>

Esempi

Il seguente comando visualizza informazioni dettagliate sulla sessione, inclusa l'impostazione di crittografia, in una sessione SMB con ID sessione 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
Node: node1
Vserver: vs1
Session ID: 2
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\joe
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: CIFS_ALIAS1
SMB Encryption Status: Unencrypted
```

Monitorare le statistiche di crittografia SMB

È possibile monitorare le statistiche di crittografia SMB e determinare quali sessioni stabilite e quali connessioni di condivisione sono crittografate e quali no.

A proposito di questa attività

Il `statistics` Command al livello di privilegio avanzato fornisce i seguenti contatori, che è possibile utilizzare per monitorare il numero di sessioni SMB crittografate e condividere le connessioni:

Nome del contatore	Descrizioni
encrypted_sessions	Indica il numero di sessioni SMB 3.0 crittografate
encrypted_share_connections	Indica il numero di condivisioni crittografate su cui è avvenuta una connessione ad albero
rejected_unencrypted_sessions	Indica il numero di configurazioni di sessione rifiutate a causa della mancanza di funzionalità di crittografia del client

Nome del contatore	Descrizioni
<code>rejected_unencrypted_shares</code>	Indica il numero di mappature di condivisione rifiutate a causa della mancanza di funzionalità di crittografia del client

Questi contatori sono disponibili con i seguenti oggetti di statistiche:

- `cifs` Consente di monitorare la crittografia SMB per tutte le sessioni SMB 3.0.

Le statistiche SMB 3.0 sono incluse nell'output di `cifs` oggetto. Se si desidera confrontare il numero di sessioni crittografate con il numero totale di sessioni, è possibile confrontare l'output per `encrypted_sessions` contatore con l'output per `established_sessions` contatore.

Se si desidera confrontare il numero di connessioni di condivisione crittografate con il numero totale di connessioni di condivisione, è possibile confrontare l'output per `encrypted_share_connections` contatore con l'output per `connected_shares` contatore.

- `rejected_unencrypted_sessions` Fornisce il numero di tentativi di stabilire una sessione SMB che richiede la crittografia da parte di un client che non supporta la crittografia SMB.
- `rejected_unencrypted_shares` Fornisce il numero di tentativi di connessione a una condivisione SMB che richiede la crittografia da parte di un client che non supporta la crittografia SMB.

È necessario avviare una raccolta di campioni di statistiche prima di poter visualizzare i dati risultanti. Se non si interrompe la raccolta dati, è possibile visualizzare i dati del campione. L'interruzione della raccolta dei dati fornisce un campione fisso. La mancata interruzione della raccolta dei dati consente di ottenere dati aggiornati da utilizzare per il confronto con le query precedenti. Il confronto può aiutarti a identificare le tendenze.

## Fasi

1. Impostare il livello di privilegio su Advanced:

```
set -privilege advanced
```

2. Avviare una raccolta di dati:

```
statistics start -object {cifs|smb1|smb2} -instance instance -sample-id sample_ID [-node node_name]
```

Se non si specifica `-sample-id` Il comando genera un identificatore di esempio e definisce questo campione come campione predefinito per la sessione CLI. Il valore per `-sample-id` è una stringa di testo. Se si esegue questo comando durante la stessa sessione CLI e non si specifica `-sample-id` il comando sovrascrive il campione predefinito precedente.

È possibile specificare il nodo su cui si desidera raccogliere le statistiche. Se non si specifica il nodo, l'esempio raccoglie le statistiche per tutti i nodi nel cluster.

3. Utilizzare `statistics stop` comando per interrompere la raccolta dei dati per il campione.
4. Visualizza le statistiche di crittografia SMB:

Se si desidera visualizzare informazioni per...	Inserisci...
Sessioni crittografate	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions</code>

Se si desidera visualizzare informazioni per...	Inserisci...
<i>node_name</i> [-node <i>node_name</i> ]	Sessioni crittografate e sessioni stabilite
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_sessions`</code>	<code>established_sessions</code>
<i>node_name</i> [-node <i>node_name</i> ]	Connessioni di condivisione crittografate
<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections`</code>	<i>node_name</i> [-node <i>node_name</i> ]
Connessioni di condivisione crittografate e condivisioni connesse	<code>`show -sample-id <i>sample_ID</i> -counter encrypted_share_connections`</code>
<code>connected_shares</code>	<i>node_name</i> [-node <i>node_name</i> ]
Sessioni non crittografate rifiutate	<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_sessions`</code>
<i>node_name</i> [-node <i>node_name</i> ]	Connessioni di condivisione non crittografate rifiutate
<code>`show -sample-id <i>sample_ID</i> -counter rejected_unencrypted_share`</code>	<i>node_name</i> [-node <i>node_name</i> ]

Se si desidera visualizzare le informazioni solo per un singolo nodo, specificare l'opzione `-node` parametro.

5. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Esempi

L'esempio seguente mostra come monitorare le statistiche di crittografia SMB 3.0 su storage virtual machine (SVM) vs1.

Il seguente comando passa al livello di privilegio avanzato:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

Il seguente comando avvia la raccolta dati per un nuovo campione:

```
cluster1::*> statistics start -object cifs -sample-id  
smbencryption_sample -vserver vs1  
Statistics collection is being started for Sample-id:  
smbencryption_sample
```

Il seguente comando interrompe la raccolta dei dati per quell'esempio:

```
cluster1::*> statistics stop -sample-id smbencryption_sample  
Statistics collection is being stopped for Sample-id:  
smbencryption_sample
```

Il seguente comando mostra le sessioni SMB crittografate e le sessioni SMB stabilite dal nodo dell'esempio:

```
cluster2::*> statistics show -object cifs -counter  
established_sessions|encrypted_sessions|node_name -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:45

Scope: vsim2

Counter	Value
established_sessions	1
encrypted_sessions	1

2 entries were displayed

Il comando seguente mostra il numero di sessioni SMB non crittografate rifiutate dal nodo dell'esempio:

```
clus-2::*> statistics show -object cifs -counter  
rejected_unencrypted_sessions -node node_name
```

Object: cifs

Instance: [proto\_ctx:003]

Start-time: 4/12/2016 11:17:45

End-time: 4/12/2016 11:21:51

Scope: vsim2

Counter	Value
rejected_unencrypted_sessions	1

1 entry was displayed.

Il comando seguente mostra il numero di condivisioni SMB connesse e di condivisioni SMB crittografate dal nodo dell'esempio:

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:41:43  
Scope: vsim2

Counter	Value
connected_shares	2
encrypted_share_connections	1

2 entries were displayed.

Il comando seguente mostra il numero di connessioni di condivisione SMB non crittografate rifiutate dal nodo dell'esempio:

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name
```

Object: cifs  
Instance: [proto\_ctx:003]  
Start-time: 4/12/2016 10:41:38  
End-time: 4/12/2016 10:42:06  
Scope: vsim2

Counter	Value
rejected_unencrypted_shares	1

1 entry was displayed.

## Informazioni correlate

[Determinazione degli oggetti e dei contatori delle statistiche disponibili](#)

["Panoramica sulla gestione e sul monitoraggio delle performance"](#)

## Comunicazione sicura della sessione LDAP

## Concetti relativi alla firma e al sealing LDAP

A partire da ONTAP 9, è possibile configurare la firma e il sealing per abilitare la sicurezza della sessione LDAP sulle query a un server Active Directory (ad). È

necessario configurare le impostazioni di sicurezza del server CIFS sulla macchina virtuale di storage (SVM) in modo che corrispondano a quelle del server LDAP.

La firma conferma l'integrità dei dati del payload LDAP utilizzando la tecnologia a chiave segreta. Il sealing crittografa i dati del payload LDAP per evitare la trasmissione di informazioni sensibili in testo non crittografato. Un'opzione *LDAP Security Level* indica se il traffico LDAP deve essere firmato, firmato e sigillato o no. L'impostazione predefinita è *none*.

La firma e il sealing LDAP sul traffico CIFS sono attivati sulla SVM con `-session-security-for-ad-ldap` al `vserver cifs security modify` comando.

## Abilitare la firma e il sealing LDAP sul server CIFS

Prima che il server CIFS possa utilizzare la firma e il sealing per una comunicazione sicura con un server LDAP di Active Directory, è necessario modificare le impostazioni di sicurezza del server CIFS per abilitare la firma e il sealing LDAP.

### Prima di iniziare

Per determinare i valori di configurazione della protezione appropriati, rivolgersi all'amministratore del server ad.

### Fasi

1. Configurare l'impostazione di sicurezza del server CIFS che abilita il traffico firmato e sigillato con i server LDAP di Active Directory: `vserver cifs security modify -vserver vserver_name -session -security-for-ad-ldap {none|sign|seal}`

È possibile attivare la firma (*sign*, integrità dei dati), firma e sigillatura (*seal*, integrità dei dati e crittografia), o nessuna delle due *none*, nessuna firma o sigillatura). Il valore predefinito è *none*.

2. Verificare che l'impostazione di protezione per la firma e il sealing LDAP sia impostata correttamente:  
`vserver cifs security show -vserver vserver_name`



Se SVM utilizza lo stesso server LDAP per eseguire query di mappatura dei nomi o altre informazioni UNIX, ad esempio utenti, gruppi e netgroup, è necessario attivare l'impostazione corrispondente con `-session-security` opzione di `vserver services name-service ldap client modify` comando.

## Configurare LDAP su TLS

### Esportare una copia del certificato della CA principale autofirmato

Per utilizzare LDAP su SSL/TLS per la protezione delle comunicazioni Active Directory, è necessario prima esportare una copia del certificato CA principale autofirmato di Active Directory Certificate Service in un file di certificato e convertirla in un file di testo ASCII. Questo file di testo viene utilizzato da ONTAP per installare il certificato sulla macchina virtuale di storage (SVM).

### Prima di iniziare

Active Directory Certificate Service deve essere già installato e configurato per il dominio a cui appartiene il server CIFS. Per informazioni sull'installazione e la configurazione di Active Director Certificate Services,



consultare la Microsoft TechNet Library.

["Microsoft TechNet Library: technet.microsoft.com"](https://technet.microsoft.com)

## Fase

1. Ottenere un certificato CA principale del controller di dominio presente in .pem formato del testo.

["Microsoft TechNet Library: technet.microsoft.com"](https://technet.microsoft.com)

## Al termine

Installare il certificato sulla SVM.

## Informazioni correlate

["Microsoft TechNet Library"](https://technet.microsoft.com)

## Installare il certificato della CA principale autofirmato su SVM

Se è richiesta l'autenticazione LDAP con TLS durante l'associazione ai server LDAP, è necessario installare prima il certificato della CA principale autofirmato su SVM.

## A proposito di questa attività

Quando LDAP su TLS è attivato, il client LDAP di ONTAP su SVM non supporta i certificati revocati in ONTAP 9.0 e 9.1.

A partire da ONTAP 9.2, tutte le applicazioni di ONTAP che utilizzano le comunicazioni TLS possono controllare lo stato dei certificati digitali utilizzando il protocollo OCSP (Online Certificate Status Protocol). Se OCSP è abilitato per LDAP su TLS, i certificati revocati vengono rifiutati e la connessione non riesce.

## Fasi

1. Installare il certificato della CA principale autofirmato:

- a. Avviare l'installazione del certificato: `security certificate install -vserver vserver_name -type server-ca`

L'output della console visualizza il seguente messaggio: `Please enter Certificate: Press <Enter> when done`

- b. Aprire il certificato .pem copiare il certificato con un editor di testo, incluse le righe che iniziano con `-----BEGIN CERTIFICATE-----` e terminando con `-----END CERTIFICATE-----`, quindi incollare il certificato dopo il prompt dei comandi.
- c. Verificare che il certificato sia visualizzato correttamente.
- d. Completare l'installazione premendo Invio.

2. Verificare che il certificato sia installato: `security certificate show -vserver vserver_name`

## Attivare LDAP su TLS sul server

Prima che il server SMB possa utilizzare TLS per una comunicazione sicura con un server LDAP Active Directory, è necessario modificare le impostazioni di sicurezza del server SMB per attivare LDAP su TLS.

A partire da ONTAP 9.10.1, il binding del canale LDAP è supportato per impostazione predefinita sia per le

connessioni LDAP Active Directory (ad) che per i servizi di nomi. ONTAP proverà l'associazione del canale con connessioni LDAP solo se Start-TLS o LDAPS è attivato insieme alla sicurezza della sessione impostata su Sign o Seal. Per disattivare o riabilitare l'associazione del canale LDAP con i server ad, utilizzare `-try -channel-binding-for-ad-ldap` con il `vserver cifs security modify` comando.

Per ulteriori informazioni, consulta:

- ["Panoramica LDAP"](#)
- ["2020 requisiti di binding del canale LDAP e firma LDAP per Windows"](#).

## Fasi

1. Configurare l'impostazione di sicurezza del server SMB che consente la comunicazione LDAP sicura con i server LDAP di Active Directory: `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. Verificare che l'impostazione di protezione LDAP su TLS sia impostata su true: `vserver cifs security show -vserver vserver_name`



Se SVM utilizza lo stesso server LDAP per eseguire query di mappatura dei nomi o altre informazioni UNIX (ad esempio utenti, gruppi e netgroup), è necessario modificare anche `-use-start-tls` utilizzando l'opzione `vserver services name-service ldap client modify` comando.

## Configurare SMB multicanale per performance e ridondanza

A partire da ONTAP 9.4, è possibile configurare SMB multicanale in modo da fornire più connessioni tra ONTAP e client in una singola sessione SMB. In questo modo si migliora il throughput e la tolleranza agli errori.

### Prima di iniziare

È possibile utilizzare la funzionalità SMB multicanale solo quando i client negoziano con SMB 3.0 o versioni successive. SMB 3.0 e versioni successive sono attivate sul server SMB ONTAP per impostazione predefinita.

### A proposito di questa attività

I client SMB rilevano e utilizzano automaticamente più connessioni di rete se viene identificata una configurazione corretta nel cluster ONTAP.

Il numero di connessioni simultanee in una sessione SMB dipende dalle schede NIC implementate:

- **NIC 1G su client e cluster ONTAP**

Il client stabilisce una connessione per NIC e associa la sessione a tutte le connessioni.

- **NIC da 10 G e capacità superiore su cluster client e ONTAP**

Il client stabilisce fino a quattro connessioni per NIC e associa la sessione a tutte le connessioni. Il client può stabilire connessioni su più NIC da 10 G e capacità maggiore.

È inoltre possibile modificare i seguenti parametri (privilegio avanzato):

- `-max-connections-per-session`

Numero massimo di connessioni consentite per sessione multicanale. L'impostazione predefinita è 32 connessioni.

Se si desidera attivare più connessioni rispetto a quelle predefinite, è necessario apportare modifiche simili alla configurazione del client, che ha anche un valore predefinito di 32 connessioni.

- **-max-lifs-per-session**

Il numero massimo di interfacce di rete pubblicizzate per ogni sessione multicanale. L'impostazione predefinita è 256 interfacce di rete.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Abilitare SMB Multichannel sul server SMB: `vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true`
3. Verificare che ONTAP stia segnalando sessioni multicanale SMB: `vserver cifs session show options`
4. Tornare al livello di privilegio admin: `set -privilege admin`

## Esempio

Nell'esempio seguente vengono visualizzate informazioni su tutte le sessioni SMB, che mostrano più connessioni per una singola sessione:

```
cluster1::> vserver cifs session show
Node:      node1
Vserver:   vs1
Connection Session                               Open
Idle
IDs        ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685      1      10.1.1.1      DOMAIN\
4s                               Administrator      0
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate su una sessione SMB con id sessione 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance
```

```
Vserver: vs1
```

```
Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

## Configurare le mappature predefinite dell'utente Windows su UNIX sul server SMB

### Configurare l'utente UNIX predefinito

È possibile configurare l'utente UNIX predefinito da utilizzare se tutti gli altri tentativi di mappatura non riescono per un utente o se non si desidera mappare singoli utenti tra UNIX e Windows. In alternativa, se si desidera che l'autenticazione degli utenti non mappati non venga eseguita correttamente, non configurare l'utente UNIX predefinito.

### A proposito di questa attività

Per impostazione predefinita, il nome dell'utente UNIX predefinito è "pcuser", il che significa che, per impostazione predefinita, è attivata la mappatura dell'utente all'utente UNIX predefinito. È possibile specificare un altro nome da utilizzare come utente UNIX predefinito. Il nome specificato deve esistere nei database del servizio di nomi configurati per la macchina virtuale di storage (SVM). Se questa opzione è impostata su una stringa nulla, nessuno può accedere al server CIFS come utente predefinito UNIX. In altri termini, ogni utente deve disporre di un account nel database delle password prima di poter accedere al server CIFS.

Per consentire a un utente di connettersi al server CIFS utilizzando l'account utente UNIX predefinito, l'utente deve soddisfare i seguenti prerequisiti:

- L'utente viene autenticato.
- L'utente si trova nel database utenti Windows locale del server CIFS, nel dominio principale del server CIFS o in un dominio attendibile (se le ricerche di mappatura dei nomi multidominio sono attivate sul server CIFS).

- Il nome utente non è esplicitamente associato a una stringa nulla.

## Fasi

1. Configurare l'utente UNIX predefinito:

Se si desidera ...	Inserire ...
Utilizzare l'utente UNIX predefinito "pcuser"	<code>vserver cifs options modify -default -unix-user pcuser</code>
Utilizzare un altro account utente UNIX come utente predefinito	<code>vserver cifs options modify -default -unix-user <i>user_name</i></code>
Disattiva l'utente UNIX predefinito	<code>vserver cifs options modify -default -unix-user ""</code>

```
vserver cifs options modify -default-unix-user pcuser
```

2. Verificare che l'utente UNIX predefinito sia configurato correttamente: `vserver cifs options show -vserver vserver_name`

Nell'esempio seguente, sia l'utente UNIX predefinito che l'utente UNIX guest su SVM vs1 sono configurati per utilizzare l'utente UNIX "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

## Configurare l'utente UNIX guest

La configurazione dell'opzione utente UNIX guest implica che gli utenti che accedono da domini non attendibili vengono mappati all'utente UNIX guest e possono connettersi al server CIFS. In alternativa, se si desidera che l'autenticazione degli utenti da domini non attendibili non venga eseguita correttamente, non configurare l'utente UNIX guest. L'impostazione predefinita prevede che gli utenti di domini non attendibili non possano connettersi al server CIFS (l'account UNIX guest non è configurato).

## A proposito di questa attività

Durante la configurazione dell'account UNIX guest, tenere presente quanto segue:

- Se il server CIFS non è in grado di autenticare l'utente rispetto a un controller di dominio per il dominio principale, un dominio attendibile o il database locale e questa opzione è attivata, il server CIFS considera l'utente come un utente guest e lo associa all'utente UNIX specificato.
- Se questa opzione è impostata su una stringa nulla, l'utente UNIX guest viene disattivato.
- È necessario creare un utente UNIX da utilizzare come utente UNIX guest in uno dei database del servizio nomi delle macchine virtuali di storage (SVM).
- Un utente che ha effettuato l'accesso come utente guest è automaticamente membro del gruppo BUILTIN/guest sul server CIFS.
- L'opzione 'homedirs-public' si applica solo agli utenti autenticati. Un utente che ha effettuato l'accesso come ospite non dispone di una home directory e non può accedere alle home directory di altri utenti.

## Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Inserisci...
Configurare l'utente UNIX guest	<code>vserver cifs options modify -guest -unix-user <i>unix_name</i></code>
Disattivare l'utente UNIX guest	<code>vserver cifs options modify -guest -unix-user ""</code>

```
vserver cifs options modify -guest-unix-user pcuser
```

2. Verificare che l'utente UNIX guest sia configurato correttamente: `vserver cifs options show -vserver vserver_name`

Nell'esempio seguente, sia l'utente UNIX predefinito che l'utente UNIX guest su SVM vs1 sono configurati per utilizzare l'utente UNIX "pcuser":

```
vserver cifs options show -vserver vs1
```

```
Vserver: vs1

Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : pcuser
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

## Mappare il gruppo di amministratori alla directory principale

Se nell'ambiente sono presenti solo client CIFS e la macchina virtuale di storage (SVM) è

stata impostata come sistema di storage multiprotocollo, è necessario disporre di almeno un account Windows con privilegi root per accedere ai file sulla SVM; In caso contrario, non è possibile gestire SVM perché non si dispone di diritti utente sufficienti.

**A proposito di questa attività**

Tuttavia, se il sistema storage è stato configurato come solo NTFS, il /etc La directory dispone di un ACL a livello di file che consente al gruppo di amministratori di accedere ai file di configurazione di ONTAP.

**Fasi**

- 1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
- 2. Configurare l'opzione del server CIFS che associa il gruppo di amministratori alla directory principale in base alle esigenze:

Se si desidera...	Quindi...
Associare i membri del gruppo di amministratori alla directory principale	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled true</code> Tutti gli account del gruppo di amministratori sono considerati root, anche se non si dispone di un /etc/usermap.cfg voce che esegue il mapping degli account alla directory principale. Se si crea un file utilizzando un account che appartiene al gruppo di amministratori, il file è di proprietà di root quando si visualizza il file da un client UNIX.
Disattiva il mapping dei membri del gruppo di amministratori alla directory principale	<code>vserver cifs options modify -vserver vserver_name -is-admin-users-mapped-to -root-enabled false</code> Gli account nel gruppo di amministratori non vengono più mappati alla directory principale. È possibile mappare esplicitamente solo un singolo utente a root.

- 3. Verificare che l'opzione sia impostata sul valore desiderato: `vserver cifs options show -vserver vserver_name`
- 4. Tornare al livello di privilegio admin: `set -privilege admin`

**Visualizza informazioni sui tipi di utenti connessi nelle sessioni SMB**

È possibile visualizzare informazioni sul tipo di utenti connessi tramite sessioni SMB. In questo modo è possibile garantire che solo il tipo di utente appropriato si connetta tramite sessioni SMB sulla macchina virtuale di storage (SVM).

**A proposito di questa attività**

I seguenti tipi di utenti possono connettersi tramite sessioni SMB:

- local-user  
Autenticato come utente CIFS locale

- domain-user

Autenticato come utente di dominio (dal dominio principale del server CIFS o da un dominio attendibile)

- guest-user

Autenticato come utente ospite

- anonymous-user

Autenticato come utente anonimo o nullo

## Fasi

1. Determinare il tipo di utente connesso in una sessione SMB: `vserver cifs session show -vserver vserver_name -windows-user windows_user_name -fields windows-user,address,lif-address,user-type`

Se si desidera visualizzare le informazioni sul tipo di utente per le sessioni stabilite...	Immettere il seguente comando...
Per tutte le sessioni con un tipo di utente specificato	<code>`vserver cifs session show -vserver vserver_name -user-type {local-user</code>
domain-user	guest-user
anonymous-user}`	Per un utente specifico

## Esempi

Il seguente comando visualizza le informazioni sulla sessione relative al tipo di utente per le sessioni su SVM vs1 stabilite dall'utente "iepubs` user1":

```
cluster1::> vserver cifs session show -vserver publ -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node          vserver session-id connection-id lif-address  address
windows-user          user-type
-----
-----
publnode1 publ      1          3439441860    10.0.0.1    10.1.1.1
IEPUBS\user1          domain-user
```

## Opzioni di comando per limitare il consumo eccessivo di risorse del client Windows

Opzioni di `vserver cifs options modify` Il comando consente di controllare il consumo di risorse per i client Windows. Questo può essere utile se i client non rientrano nei limiti normali di consumo delle risorse, ad esempio se sono presenti un numero insolitamente elevato di file aperti, sessioni aperte o richieste di notifica delle modifiche.

Le seguenti opzioni di `vserver cifs options modify` Sono stati aggiunti comandi per controllare il



consumo di risorse del client Windows. Se si supera il valore massimo di una di queste opzioni, la richiesta viene rifiutata e viene inviato un messaggio EMS. Viene inoltre inviato un messaggio di avviso EMS quando viene raggiunto il 80% del limite configurato per queste opzioni.

- `-max-opens-same-file-per-tree`

Numero massimo di apertura sullo stesso file per albero CIFS

- `-max-same-user-sessions-per-connection`

Numero massimo di sessioni aperte dallo stesso utente per connessione

- `-max-same-tree-connect-per-session`

Numero massimo di connessioni ad albero sulla stessa condivisione per sessione

- `-max-watches-set-per-tree`

Numero massimo di orologi (noto anche come *change notifes*) stabiliti per albero

Vedere le pagine man per i limiti predefiniti e per visualizzare la configurazione corrente.

A partire da ONTAP 9.4, i server SMB versione 2 o successiva possono limitare il numero di richieste in sospeso (*SMB credits*) che il client può inviare al server con una connessione SMB. La gestione dei crediti SMB viene avviata dal client e controllata dal server.

Il numero massimo di richieste in sospeso che possono essere concesse su una connessione SMB è controllato da `-max-credits` opzione. Il valore predefinito per questa opzione è 128.

## **Migliora le performance del client con gli oplock tradizionali e in leasing**

### **Migliora le performance del client con una panoramica degli oplock tradizionali e del lease**

Gli oplock tradizionali (blocchi opportunistici) e gli oplock di lease consentono a un client SMB in alcuni scenari di condivisione file di eseguire il caching lato client delle informazioni di Read-ahead, write-behind e lock. Un client può quindi leggere o scrivere su un file senza ricordare regolarmente al server che ha bisogno di accedere al file in questione. Ciò migliora le performance riducendo il traffico di rete.

Gli oplock di leasing sono una forma avanzata di oplock disponibili con il protocollo SMB 2.1 e versioni successive. Gli oplock del lease consentono a un client di ottenere e preservare lo stato di caching del client in più SMB aperti che hanno origine da sé.

Gli oplock possono essere controllati in due modi:

- Da una proprietà di condivisione, utilizzando `vserver cifs share create` quando viene creata la condivisione, oppure il `vserver share properties` comando dopo la creazione.
- Da una proprietà `qtree`, utilizzando `volume qtree create` quando viene creato il `qtree`, oppure il `volume qtree oplock` comandi dopo la creazione.

## Considerazioni sulla perdita di dati della cache in scrittura quando si utilizzano gli oplock

In alcuni casi, se un processo ha un oplock esclusivo su un file e un secondo processo tenta di aprire il file, il primo processo deve invalidare i dati memorizzati nella cache e svuotare le scritture e i blocchi. Il client deve quindi rinunciare all'oplock e all'accesso al file. Se si verifica un errore di rete durante questo svuotamento, i dati di scrittura memorizzati nella cache potrebbero andare persi.

- Possibilità di perdita di dati

Qualsiasi applicazione che dispone di dati memorizzati nella cache in scrittura può perdere tali dati nei seguenti casi:

- La connessione viene effettuata utilizzando SMB 1.0.
- Ha un oplock esclusivo sul file.
- Viene richiesto di interrompere l'oplock o chiudere il file.
- Durante il processo di cancellazione della cache di scrittura, il sistema di rete o di destinazione genera un errore.

- Gestione degli errori e completamento della scrittura

La cache stessa non ha alcun tipo di gestione degli errori, come fanno le applicazioni. Quando l'applicazione esegue una scrittura nella cache, la scrittura viene sempre completata. Se la cache, a sua volta, esegue una scrittura nel sistema di destinazione su una rete, deve presumere che la scrittura sia completata perché in caso contrario, i dati vengono persi.

## Attiva o disattiva gli oplock durante la creazione di condivisioni SMB

Gli oplock consentono ai client di bloccare i file e memorizzare nella cache i contenuti localmente, aumentando le performance per le operazioni sui file. Gli oplock sono abilitati sulle condivisioni SMB che risiedono su storage virtual machine (SVM). In alcuni casi, è possibile disattivare gli oplock. È possibile attivare o disattivare gli oplock in base alla condivisione.



### A proposito di questa attività

Se gli oplock sono attivati sul volume che contiene una condivisione ma la proprietà di oplock share per tale condivisione è disattivata, gli oplock sono disattivati per quella condivisione. La disattivazione degli oplock in una condivisione ha la precedenza sull'impostazione dell'oplock del volume. La disattivazione degli oplock sulla condivisione disattiva gli oplock opportunistici e lease.

È possibile specificare altre proprietà di condivisione oltre a specificare la proprietà di condivisione oplock utilizzando un elenco delimitato da virgole. È inoltre possibile specificare altri parametri di condivisione.

### Fasi

1. Eseguire l'azione appropriata:

Se si desidera...	Quindi...
<p>Abilitare gli oplock su una condivisione durante la creazione della condivisione</p>	<p>Immettere il seguente comando: <code>vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share-properties [oplocks,...]</code></p> <div data-bbox="873 615 927 667">  </div> <p>Se si desidera che la condivisione abbia solo le proprietà di condivisione predefinite, che sono <code>oplocks</code>, <code>browsable</code>, e. <code>changenotify</code> attivato, non è necessario specificare <code>-share-properties</code> Parametro durante la creazione di una condivisione SMB. Se si desidera una combinazione di proprietà di condivisione diversa da quella predefinita, è necessario specificare <code>-share-properties</code> parametro con l'elenco delle proprietà di condivisione da utilizzare per la condivisione.</p>
<p>Disattiva gli oplock su una condivisione durante la creazione della condivisione</p>	<p>Immettere il seguente comando: <code>vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]</code></p> <div data-bbox="873 1255 927 1308">  </div> <p>Quando si disattivano gli oplock, è necessario specificare un elenco di proprietà di condivisione durante la creazione della condivisione, ma non è necessario specificare <code>oplocks</code> proprietà.</p>

## Informazioni correlate

[Attivazione o disattivazione degli oplock sulle condivisioni SMB esistenti](#)

[Monitoraggio dello stato dell'oplock](#)

## Comandi per attivare o disattivare gli oplock su volumi e qtree

Gli oplock consentono ai client di bloccare i file e memorizzare nella cache i contenuti localmente, aumentando le performance per le operazioni sui file. È necessario conoscere i comandi per attivare o disattivare gli oplock su volumi o qtree. È inoltre necessario sapere quando è possibile attivare o disattivare gli oplock su volumi e qtree.

- Gli oplock sono attivati sui volumi per impostazione predefinita.
- Non è possibile disattivare gli oplock quando si crea un volume.
- È possibile attivare o disattivare gli oplock sui volumi esistenti per le SVM in qualsiasi momento.
- È possibile abilitare gli oplock sui qtree per le SVM.

L'impostazione della modalità oplock è una proprietà di qtree ID 0, il qtree predefinito di tutti i volumi. Se non si specifica un'impostazione di oplock durante la creazione di un qtree, il qtree eredita l'impostazione di oplock del volume padre, che viene attivata per impostazione predefinita. Tuttavia, se si specifica un'impostazione di oplock sul nuovo qtree, questa ha la precedenza sull'impostazione di oplock sul volume.

Se si desidera...	Utilizzare questo comando...
Abilitare gli oplock sui volumi o sui qtree	<code>volume qtree oplocks con -oplock-mode</code> parametro impostato su <code>enable</code>
Disattiva gli oplock sui volumi o sui qtree	<code>volume qtree oplocks con -oplock-mode</code> parametro impostato su <code>disable</code>

## Informazioni correlate

[Monitoraggio dello stato dell'oplock](#)

### Attiva o disattiva gli oplock sulle condivisioni SMB esistenti



Per impostazione predefinita, gli oplock sono attivati sulle condivisioni SMB sulle macchine virtuali di storage (SVM). In alcuni casi, potrebbe essere necessario disattivare gli oplock; in alternativa, se in precedenza sono stati disattivati gli oplock in una condivisione, potrebbe essere necessario riattivarli.

### A proposito di questa attività

Se gli oplock sono attivati sul volume che contiene una condivisione, ma la proprietà di oplock share per tale condivisione è disattivata, gli oplock sono disattivati per quella condivisione. La disattivazione degli oplock su una condivisione ha la precedenza sull'attivazione degli oplock sul volume. Disattivando gli oplock sulla condivisione, vengono disattivati gli oplock opportunistici e lease. È possibile attivare o disattivare gli oplock sulle condivisioni esistenti in qualsiasi momento.

### Fase

1. Eseguire l'azione appropriata:

Se si desidera...	Quindi...
Abilitare gli oplock su una condivisione modificando una condivisione esistente	<p>Immettere il seguente comando: <code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties oplocks</code></p> <div>  <p>È possibile specificare ulteriori proprietà di condivisione da aggiungere utilizzando un elenco delimitato da virgole.</p> </div> <p>Le nuove proprietà aggiunte vengono aggiunte all'elenco esistente di proprietà di condivisione. Tutte le proprietà di condivisione precedentemente specificate rimangono attive.</p>
Disattivare gli oplock su una condivisione modificando una condivisione esistente	<p>Immettere il seguente comando: <code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks</code></p> <div>  <p>È possibile specificare ulteriori proprietà di condivisione da rimuovere utilizzando un elenco delimitato da virgole.</p> </div> <p>Le proprietà di condivisione rimosse vengono eliminate dall'elenco esistente di proprietà di condivisione; tuttavia, le proprietà di condivisione configurate in precedenza e non rimosse rimangono attive.</p>

## Esempi

Il seguente comando abilita gli oplock per la condivisione denominata “Engineering” sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name Engineering -share-properties oplocks
```

```
cluster1::> vserver cifs share properties show
```

Vserver	Share	Properties
vs1	Engineering	oplocks browsable changenotify showsnapshot

Il seguente comando disattiva gli oplock per la condivisione denominata "Engineering" su SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share          Properties
-----
vs1              Engineering    browsable
                  changenotify
                  showsnapshot
```

### Informazioni correlate

[Attivazione o disattivazione degli oplock durante la creazione di condivisioni SMB](#)

[Monitoraggio dello stato dell'oplock](#)

[Aggiunta o rimozione delle proprietà di condivisione su una condivisione SMB esistente](#)

### Monitorare lo stato dell'oplock

È possibile monitorare e visualizzare informazioni sullo stato dell'oplock. È possibile utilizzare queste informazioni per determinare quali file dispongono di oplock, quali sono il livello di oplock e il livello di oplock state e se viene utilizzato il leasing di oplock. È inoltre possibile determinare le informazioni sui blocchi che potrebbero essere necessari per interrompere manualmente.

### A proposito di questa attività

È possibile visualizzare le informazioni relative a tutti gli oplock in forma di riepilogo o in un elenco dettagliato. È inoltre possibile utilizzare parametri opzionali per visualizzare informazioni su un sottoinsieme più piccolo di blocchi esistenti. Ad esempio, è possibile specificare che l'output restituisca blocchi solo con l'indirizzo IP del client specificato o con il percorso specificato.

È possibile visualizzare le seguenti informazioni sugli oplock tradizionali e di lease:

- SVM, nodo, volume e LIF su cui è stabilito l'oplock
- Blocca UUID
- Indirizzo IP del client con l'oplock
- Percorso in cui viene stabilito l'oplock
- Protocollo di blocco (SMB) e tipo (oplock)
- Stato di blocco
- Livello di oplock
- Stato di connessione e tempo di scadenza SMB
- Aprire ID gruppo se viene concesso un oplock di leasing

Vedere `vserver oplocks show` pagina man per una descrizione dettagliata di ciascun parametro.

## Fasi

1. Visualizzare lo stato dell'oplock utilizzando `vserver locks show` comando.

## Esempi

Il seguente comando visualizza le informazioni predefinite relative a tutti i blocchi. L'oplock sul file visualizzato viene concesso con un `read-batch` livello di oplock:

```
cluster1::> vserver locks show
```

```
Vserver: vs0
```

Volume	Object Path	LIF	Protocol	Lock Type	Client
vol1	/vol1/notes.txt	node1_data1			
			cifs	share-level	192.168.1.5
	Sharelock Mode: read_write-deny_delete				
				op-lock	192.168.1.5
	Oplock Level: read-batch				

Nell'esempio seguente vengono visualizzate informazioni più dettagliate sul blocco di un file con il percorso `/data2/data2_2/intro.pptx`. Un oplock del lease viene concesso sul file con un batch Livello di oplock per un client con un indirizzo IP di `10.3.1.3`:



Quando si visualizzano informazioni dettagliate, il comando fornisce un output separato per le informazioni di oplock e sharlock. Questo esempio mostra solo l'output della sezione oplock.

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx
```

```

    Vserver: vs1
    Volume: data2_2
  Logical Interface: lif2
    Object Path: /data2/data2_2/intro.pptx
    Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
    Lock Protocol: cifs
    Lock Type: op-lock
  Node Holding Lock State: node3
    Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
    Bytelock is Mandatory: -
    Bytelock is Exclusive: -
    Bytelock is Superlock: -
    Bytelock is Soft: -
    Oplock Level: batch
  Shared Lock Access Mode: -
    Shared Lock is Soft: -
    Delegation Type: -
    Client Address: 10.3.1.3
    SMB Open Type: -
    SMB Connect State: connected
  SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

## Informazioni correlate

[Attivazione o disattivazione degli oplock durante la creazione di condivisioni SMB](#)

[Attivazione o disattivazione degli oplock sulle condivisioni SMB esistenti](#)

[Comandi per attivare o disattivare gli oplock su volumi e qtree](#)

## Applicare oggetti Criteri di gruppo ai server SMB

### Panoramica sull'applicazione degli oggetti Criteri di gruppo ai server SMB

Il server SMB supporta gli oggetti Criteri di gruppo (GPO), un insieme di regole note come *attributi dei criteri di gruppo* che si applicano ai computer in un ambiente Active Directory. È possibile utilizzare gli oggetti Criteri di gruppo per gestire centralmente le impostazioni di tutte le macchine virtuali di storage (SVM) nel cluster appartenente allo stesso dominio Active Directory.

Quando gli oggetti Criteri di gruppo sono attivati sul server SMB, ONTAP invia query LDAP al server Active Directory per richiedere informazioni sull'oggetto Criteri di gruppo. Se esistono definizioni di GPO applicabili al



server SMB, il server Active Directory restituisce le seguenti informazioni di GPO:

- Nome dell'oggetto Criteri di gruppo
- Versione attuale dell'oggetto Criteri di gruppo
- Posizione della definizione dell'oggetto Criteri di gruppo
- Elenchi di UUID (universally unique identifier) per set di criteri GPO

### Informazioni correlate

[Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso \(DAC\)](#)

["Controllo SMB e NFS e tracciamento della sicurezza"](#)

### GPO supportati

Sebbene non tutti gli oggetti Criteri di gruppo (GPO) siano applicabili alle SVM (Storage Virtual Machine) abilitate per CIFS, le SVM sono in grado di riconoscere ed elaborare il relativo set di GPO.

I seguenti GPO sono attualmente supportati sulle SVM:

- Impostazioni avanzate di configurazione dei criteri di controllo:

Accesso a oggetti: Staging dei criteri di accesso centrale

Specifica il tipo di eventi da sottoporre a verifica per lo staging dei criteri di accesso centrale (CAP), incluse le seguenti impostazioni:

- Non eseguire audit
- Controllare solo gli eventi di successo
- Controllare solo gli eventi di errore
- Controllare gli eventi di successo e di guasto



Se viene impostata una qualsiasi delle tre opzioni di audit (solo eventi di successo, solo eventi di errore di audit, eventi di successo e di fallimento di audit), ONTAP controlla sia gli eventi di successo che quelli di fallimento.

Impostare utilizzando `Audit Central Access Policy Staging in Advanced Audit Policy Configuration/Audit Policies/Object Access GPO`.



Per utilizzare le impostazioni dell'oggetto Criteri di gruppo per la configurazione avanzata dei criteri di controllo, è necessario configurare il controllo sulla SVM CIFS-Enabled a cui si desidera applicare queste impostazioni. Se il controllo non è configurato sulla SVM, le impostazioni dell'oggetto Criteri di gruppo non verranno applicate e verranno ignorate.

- Impostazioni del Registro di sistema:
  - Intervallo di aggiornamento dei criteri di gruppo per SVM abilitato CIFS

Impostare utilizzando `Registry GPO`.

- Offset casuale di refresh dei criteri di gruppo

Impostare utilizzando `Registry GPO`.

- Pubblicazione hash per BranchCache

La pubblicazione Hash per l'oggetto Criteri di gruppo BranchCache corrisponde alla modalità operativa BranchCache. Sono supportate le seguenti tre modalità operative:

- Per-share
- All-share
- Disattivato tramite `Registry GPO`.

- Supporto della versione hash per BranchCache

Sono supportate le seguenti tre impostazioni di versione hash:

- BranchCache versione 1
- BranchCache versione 2
- BranchCache versioni 1 e 2 impostate tramite `Registry GPO`.



Per utilizzare le impostazioni dell'oggetto Criteri di gruppo BranchCache, è necessario configurare BranchCache sulla SVM CIFS-Enabled a cui si desidera applicare queste impostazioni. Se BranchCache non è configurato sulla SVM, le impostazioni dell'oggetto Criteri di gruppo non verranno applicate e verranno ignorate.

- Impostazioni di sicurezza

- Policy di audit e registro eventi

- Controllare gli eventi di accesso

Specifica il tipo di eventi di accesso da sottoporre a verifica, incluse le seguenti impostazioni:

- Non eseguire audit
- Controllare solo gli eventi di successo
- Verifica degli eventi di guasto
- Controllare gli eventi di successo e di guasto impostati utilizzando `Audit logon events in Local Policies/Audit Policy GPO`.



Se viene impostata una qualsiasi delle tre opzioni di audit (solo eventi di successo, solo eventi di errore di audit, eventi di successo e di fallimento di audit), ONTAP controlla sia gli eventi di successo che quelli di fallimento.

- Controllare l'accesso agli oggetti

Specifica il tipo di accesso a oggetti da sottoporre a controllo, incluse le seguenti impostazioni:

- Non eseguire audit
- Controllare solo gli eventi di successo
- Verifica degli eventi di guasto

- Controllare gli eventi di successo e di guasto impostati utilizzando `Audit object access` in `Local Policies/Audit Policy GPO`.



Se viene impostata una qualsiasi delle tre opzioni di audit (solo eventi di successo, solo eventi di errore di audit, eventi di successo e di fallimento di audit), ONTAP controlla sia gli eventi di successo che quelli di fallimento.

- Metodo di conservazione dei log

Specifica il metodo di conservazione del registro di controllo, incluse le seguenti impostazioni:

- Sovrascrivere il registro eventi quando la dimensione del file di registro supera la dimensione massima
- Non sovrascrivere il registro eventi (cancellare manualmente il registro) impostato utilizzando `Retention method for security log` in `Event Log GPO`.

- Dimensione massima del log

Specifica la dimensione massima del registro di controllo.

Impostare utilizzando `Maximum security log size` in `Event Log GPO`.



Per utilizzare le impostazioni dell'oggetto Criteri di gruppo dei criteri di controllo e del registro eventi, è necessario configurare il controllo sulla SVM CIFS-Enabled a cui si desidera applicare queste impostazioni. Se il controllo non è configurato sulla SVM, le impostazioni dell'oggetto Criteri di gruppo non verranno applicate e verranno ignorate.

- Sicurezza del file system

Specifica un elenco di file o directory su cui viene applicata la protezione dei file tramite un GPO.

Impostare utilizzando `File System GPO`.



Il percorso del volume in cui è configurato l'oggetto Criteri di gruppo di protezione del file system deve esistere all'interno della SVM.

- Policy Kerberos

- Massima inclinazione dell'orologio

Specifica la tolleranza massima in minuti per la sincronizzazione dell'orologio del computer.

Impostare utilizzando `Maximum tolerance for computer clock synchronization` in `Account Policies/Kerberos Policy GPO`.

- Età massima del biglietto

Specifica la durata massima in ore per il ticket utente.

Impostare utilizzando `Maximum lifetime for user ticket` in `Account Policies/Kerberos Policy GPO`.

- Età massima per il rinnovo del biglietto

Specifica la durata massima in giorni per il rinnovo del ticket utente.

Impostare utilizzando `Maximum lifetime for user ticket renewal` in `Account Policies/Kerberos Policy` GPO.

◦ Assegnazione dei diritti dell'utente (diritti di privilegio)

▪ Assuma la proprietà

Specifica l'elenco di utenti e gruppi che hanno il diritto di assumere la proprietà di qualsiasi oggetto a protezione diretta.

Impostare utilizzando `Take ownership of files or other objects` in `Local Policies/User Rights Assignment` GPO.

▪ Privilegio di sicurezza

Specifica l'elenco di utenti e gruppi che possono specificare le opzioni di controllo per l'accesso a oggetti di singole risorse, come file, cartelle e oggetti Active Directory.

Impostare utilizzando `Manage auditing and security log` in `Local Policies/User Rights Assignment` GPO.

▪ Modifica del privilegio di notifica (ignora il controllo incrociato)

Specifica l'elenco di utenti e gruppi che possono attraversare gli alberi di directory anche se gli utenti e i gruppi potrebbero non disporre delle autorizzazioni per la directory attraversata.

Lo stesso privilegio è richiesto per gli utenti per ricevere notifiche delle modifiche apportate a file e directory. Impostare utilizzando `Bypass traverse checking` in `Local Policies/User Rights Assignment` GPO.

◦ Valori del Registro di sistema

▪ Firma obbligatoria

Specifica se la firma SMB richiesta è attivata o disattivata.

Impostare utilizzando `Microsoft network server: Digitally sign communications (always)` in `Security Options` GPO.

◦ Limitare l'anonimato

Specifica quali sono le restrizioni per gli utenti anonimi e include le seguenti tre impostazioni dell'oggetto Criteri di gruppo:

▪ Nessuna enumerazione degli account SAM (Security account Manager):

Questa impostazione di protezione determina le autorizzazioni aggiuntive concesse per le connessioni anonime al computer. Questa opzione viene visualizzata come `no-enumeration` in `ONTAP`, se abilitato.

Impostare utilizzando `Network access: Do not allow anonymous enumeration of SAM accounts` in `Local Policies/Security Options` GPO.

- Nessuna enumerazione di account e condivisioni SAM

Questa impostazione di protezione determina se è consentita l'enumerazione anonima di account e condivisioni SAM. Questa opzione viene visualizzata come `no-enumeration` in ONTAP, se abilitato.

Impostare utilizzando `Network access: Do not allow anonymous enumeration of SAM accounts and shares` in Local Policies/Security Options GPO.

- Limitare l'accesso anonimo alle condivisioni e alle named pipe

Questa impostazione di sicurezza limita l'accesso anonimo alle condivisioni e alle pipe. Questa opzione viene visualizzata come `no-access` in ONTAP, se abilitato.

Impostare utilizzando `Network access: Restrict anonymous access to Named Pipes and Shares` in Local Policies/Security Options GPO.

Quando si visualizzano informazioni sui criteri di gruppo definiti e applicati, il `Resultant restriction for anonymous user` Il campo di output fornisce informazioni sulla restrizione risultante delle tre impostazioni di restrizione anonime dell'oggetto Criteri di gruppo. Le possibili restrizioni risultanti sono le seguenti:

- `no-access`

All'utente anonimo viene negato l'accesso alle condivisioni e alle named pipe specificate e non è possibile utilizzare l'enumerazione degli account e delle condivisioni SAM. Questa restrizione risultante si verifica se `Network access: Restrict anonymous access to Named Pipes and Shares` L'oggetto Criteri di gruppo è attivato.

- `no-enumeration`

L'utente anonimo ha accesso alle condivisioni e alle named pipe specificate, ma non può utilizzare l'enumerazione degli account e delle condivisioni SAM. Questa restrizione risultante si verifica se vengono soddisfatte entrambe le seguenti condizioni:

- Il `Network access: Restrict anonymous access to Named Pipes and Shares` L'oggetto Criteri di gruppo è disattivato.
- Sia il `Network access: Do not allow anonymous enumeration of SAM accounts` o il `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Gli oggetti GPO sono abilitati.

- `no-restriction`

L'utente anonimo ha accesso completo e può utilizzare l'enumerazione. Questa restrizione risultante si verifica se vengono soddisfatte entrambe le seguenti condizioni:

- Il `Network access: Restrict anonymous access to Named Pipes and Shares` L'oggetto Criteri di gruppo è disattivato.
- Entrambi i modelli `Network access: Do not allow anonymous enumeration of SAM accounts` e `Network access: Do not allow anonymous enumeration of SAM accounts and shares` Gli oggetti Criteri di gruppo sono disattivati.
  - Gruppi con restrizioni

È possibile configurare gruppi con restrizioni per gestire centralmente l'appartenenza a gruppi integrati o definiti dall'utente. Quando si applica un gruppo con restrizioni tramite un criterio di gruppo, l'appartenenza di un gruppo locale del server CIFS viene impostata automaticamente in modo che corrisponda alle impostazioni dell'elenco di appartenenze definite nel criterio di gruppo applicato.

Impostare utilizzando `Restricted Groups GPO`.

- Impostazioni dei criteri di accesso centrale

Specifica un elenco di criteri di accesso centrale. I criteri di accesso centrale e le relative regole dei criteri di accesso centrale determinano le autorizzazioni di accesso per più file sulla SVM.

## Informazioni correlate

[Attivazione o disattivazione del supporto GPO su un server CIFS](#)

[Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso \(DAC\)](#)

["Controllo SMB e NFS e tracciamento della sicurezza"](#)

[Modifica delle impostazioni di sicurezza Kerberos del server CIFS](#)

[Utilizzo di BranchCache per memorizzare nella cache SMB i contenuti vengono condivisi in una filiale](#)

[Utilizzo della firma SMB per migliorare la sicurezza della rete](#)

[Configurazione del controllo incrociato bypass](#)

[Configurazione delle restrizioni di accesso per utenti anonimi](#)

## Requisiti per l'utilizzo degli oggetti Criteri di gruppo con il server SMB

Per utilizzare gli oggetti Criteri di gruppo (GPO) con il server SMB, il sistema deve soddisfare diversi requisiti.

- SMB deve essere concesso in licenza sul cluster. La licenza SMB è inclusa con ["ONTAP uno"](#). Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.
- Un server SMB deve essere configurato e collegato a un dominio Active Directory di Windows.
- Lo stato dell'amministratore del server SMB deve essere attivo.
- Gli oggetti Criteri di gruppo devono essere configurati e applicati all'unità organizzativa (OU) di Windows Active Directory contenente l'oggetto computer server SMB.
- Il supporto GPO deve essere attivato sul server SMB.

## Attivare o disattivare il supporto GPO su un server CIFS

È possibile attivare o disattivare il supporto degli oggetti Criteri di gruppo (GPO) su un server CIFS. Se si attiva il supporto GPO su un server CIFS, gli oggetti Criteri di gruppo applicabili definiti nel criterio di gruppo, ovvero il criterio applicato all'unità organizzativa (OU) che contiene l'oggetto computer server CIFS, vengono applicati al server CIFS.



### A proposito di questa attività

I GPO non possono essere abilitati sui server CIFS in modalità workgroup.

### Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Abilitare gli oggetti Criteri di gruppo	<code>vserver cifs group-policy modify -vserver vserver_name -status enabled</code>
Disattivare gli oggetti Criteri di gruppo	<code>vserver cifs group-policy modify -vserver vserver_name -status disabled</code>

2. Verificare che il supporto GPO sia nello stato desiderato: `vserver cifs group-policy show -vserver +vserver_name_`

Lo stato dei criteri di gruppo per i server CIFS in modalità gruppo di lavoro viene visualizzato come “disabled”.

### Esempio

L'esempio seguente abilita il supporto GPO su storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

Vserver: vs1
Group Policy Status: enabled
```

### Informazioni correlate

[GPO supportati](#)

[Requisiti per l'utilizzo degli oggetti Criteri di gruppo con il server CIFS](#)

[Come vengono aggiornati gli oggetti Criteri di gruppo sul server CIFS](#)

[Aggiornamento manuale delle impostazioni dell'oggetto Criteri di gruppo sul server CIFS](#)

[Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo](#)

**Modalità di aggiornamento degli oggetti Criteri di gruppo sul server SMB**

**Come vengono aggiornati gli oggetti Criteri di gruppo nella panoramica del server CIFS**

Per impostazione predefinita, ONTAP recupera e applica le modifiche dell'oggetto Criteri di gruppo ogni 90 minuti. Le impostazioni di sicurezza vengono aggiornate ogni 16 ore. Se si desidera aggiornare gli oggetti Criteri di gruppo per applicare le nuove impostazioni

dei criteri dell'oggetto Criteri di gruppo prima che ONTAP li aggiorni automaticamente, è possibile attivare un aggiornamento manuale su un server CIFS con un comando ONTAP.


- Per impostazione predefinita, tutti gli oggetti Criteri di gruppo vengono verificati e aggiornati in base alle necessità ogni 90 minuti.

Questo intervallo è configurabile e può essere impostato utilizzando `Refresh interval` e `Random offset` Impostazioni dell'oggetto Criteri di gruppo.

ONTAP interroga Active Directory per le modifiche apportate agli oggetti Criteri di gruppo. Se i numeri di versione dell'oggetto Criteri di gruppo registrati in Active Directory sono superiori a quelli del server CIFS, ONTAP recupera e applica i nuovi oggetti Criteri di gruppo. Se i numeri di versione sono gli stessi, gli oggetti Criteri di gruppo sul server CIFS non vengono aggiornati.

- Gli oggetti Criteri di gruppo delle impostazioni di sicurezza vengono aggiornati ogni 16 ore.

ONTAP recupera e applica gli oggetti Criteri di gruppo delle impostazioni di protezione ogni 16 ore, indipendentemente dal fatto che questi oggetti Criteri di gruppo siano stati modificati o meno.



Il valore predefinito di 16 ore non può essere modificato nella versione corrente di ONTAP. Si tratta di un'impostazione predefinita del client Windows.

- Tutti gli oggetti Criteri di gruppo possono essere aggiornati manualmente con un comando ONTAP.

Questo comando simula le finestre `gpupdate.exe /force` command.

Informazioni correlate

[Aggiornamento manuale delle impostazioni dell'oggetto Criteri di gruppo sul server CIFS](#)

Aggiornamento manuale delle impostazioni dell'oggetto Criteri di gruppo sul server CIFS

Se si desidera aggiornare immediatamente le impostazioni dell'oggetto Criteri di gruppo (GPO) sul server CIFS, è possibile aggiornare manualmente le impostazioni. È possibile aggiornare solo le impostazioni modificate oppure forzare un aggiornamento per tutte le impostazioni, incluse quelle applicate in precedenza ma non modificate.

Fase

1. Eseguire l'azione appropriata:

Se si desidera eseguire l'aggiornamento...	Immettere il comando...
Impostazioni GPO modificate	<code>vserver cifs group-policy update -vserver vserver_name</code>
Tutte le impostazioni dell'oggetto Criteri di gruppo	<code>vserver cifs group-policy update -vserver vserver_name -force-reapply -all-settings true</code>

Informazioni correlate



### Visualizza informazioni sulle configurazioni dell'oggetto Criteri di gruppo

È possibile visualizzare informazioni sulle configurazioni degli oggetti Criteri di gruppo (GPO) definite in Active Directory e sulle configurazioni degli oggetti Criteri di gruppo applicate al server CIFS.

#### A proposito di questa attività

È possibile visualizzare informazioni su tutte le configurazioni GPO definite in Active Directory del dominio a cui appartiene il server CIFS oppure solo sulle configurazioni GPO applicate a un server CIFS.

#### Fasi

1. Visualizzare le informazioni sulle configurazioni dell'oggetto Criteri di gruppo eseguendo una delle seguenti operazioni:

Se si desidera visualizzare informazioni su tutte le configurazioni di Criteri di gruppo...	Immettere il comando...
Definito in Active Directory	<code>vserver cifs group-policy show-defined -vserver vserver_name</code>
Applicato a una SVM (Storage Virtual Machine) abilitata per CIFS	<code>vserver cifs group-policy show-applied -vserver vserver_name</code>

#### Esempio

Nell'esempio seguente vengono visualizzate le configurazioni GPO definite in Active Directory a cui appartiene la SVM abilitata per CIFS denominata vs1:

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache : version1
```

```
Security Settings:
```

```
    Event Audit and Event Log:
```

```
        Audit Logon Events: none
```

```
Audit Object Access: success
Log Retention Method: overwrite-as-needed
Max Log Size: 16384
File Security:
    /vol1/home
    /vol1/dir1
Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
             cap2

GPO Name: Resultant Set of Policy
Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication for Mode BranchCache: per-share
    Hash Version Support for BranchCache: version1
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
```

```

/voll/dir1
Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
             cap2

```

Nell'esempio seguente vengono visualizzate le configurazioni GPO applicate a SVM vs1 abilitato CIFS:

```

cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
-----
    GPO Name: Default Domain Policy
        Level: Domain
        Status: enabled
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed

```

```
    Max Log Size: 16384
File Security:
    /vol1/home
    /vol1/dir1
Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
        cap2

GPO Name: Resultant Set of Policy
    Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
```

```
Max Clock Skew: 5
Max Ticket Age: 10
Max Renew Age: 7
Privilege Rights:
  Take Ownership: usr1, usr2
  Security Privilege: usr1, usr2
  Change Notify: usr1, usr2
Registry Values:
  Signing Required: false
Restrict Anonymous:
  No enumeration of SAM accounts: true
  No enumeration of SAM accounts and shares: false
  Restrict anonymous access to shares and named pipes: true
  Combined restriction for anonymous user: no-access
Restricted Groups:
  gpr1
  gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2
```

## Informazioni correlate

[Attivazione o disattivazione del supporto GPO su un server CIFS](#)

**Visualizzare informazioni dettagliate sugli oggetti GPO di gruppo con restrizioni**

È possibile visualizzare informazioni dettagliate sui gruppi con restrizioni definiti come oggetti Criteri di gruppo (GPO) in Active Directory e applicati al server CIFS.

### A proposito di questa attività

Per impostazione predefinita, vengono visualizzate le seguenti informazioni:

- Nome del criterio di gruppo
- Versione dei criteri di gruppo
- Collegamento

Specifica il livello di configurazione dei criteri di gruppo. I valori di output possibili includono:

- Local Quando il criterio di gruppo è configurato in ONTAP
  - Site quando il criterio di gruppo è configurato a livello di sito nel controller di dominio
  - Domain quando il criterio di gruppo è configurato a livello di dominio nel controller di dominio
  - OrganizationalUnit Quando il criterio di gruppo è configurato a livello di unità organizzativa (OU) nel controller di dominio
  - RSOP per l'insieme risultante di criteri derivati da tutti i criteri di gruppo definiti a vari livelli
- Nome del gruppo con restrizioni

- Gli utenti e i gruppi che appartengono al gruppo con restrizioni e che non ne fanno parte
- L'elenco dei gruppi a cui viene aggiunto il gruppo con restrizioni

Un gruppo può essere un membro di gruppi diversi dai gruppi elencati qui.

## Fase

1. Visualizzare le informazioni su tutti gli oggetti Criteri di gruppo con restrizioni eseguendo una delle seguenti operazioni:

Se si desidera visualizzare informazioni su tutti gli oggetti Criteri di gruppo con restrizioni...	Immettere il comando...
Definito in Active Directory	<code>vserver cifs group-policy restricted-group show-defined -vserver vserver_name</code>
Applicato a un server CIFS	<code>vserver cifs group-policy restricted-group show-applied -vserver vserver_name</code>

## Esempio

Nell'esempio seguente vengono visualizzate informazioni sugli oggetti Criteri di gruppo con restrizioni definiti nel dominio Active Directory a cui appartiene la SVM abilitata per CIFS denominata vs1:

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1
```

```
Vserver: vs1
-----
```

```
Group Policy Name: gp01
Version: 16
Link: OrganizationalUnit
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy
Version: 0
Link: RSOP
Group Name: group1
Members: user1
MemberOf: EXAMPLE\group9
```

Nell'esempio seguente vengono visualizzate informazioni sui GPO a gruppi limitati applicati a SVM vs1 abilitato a CIFS:

```
cluster1::> vserver cifs group-policy restricted-group show-applied  
-vserver vs1
```

Vserver: vs1

-----

```
Group Policy Name: gp01  
Version: 16  
Link: OrganizationalUnit  
Group Name: group1  
Members: user1  
MemberOf: EXAMPLE\group9
```

```
Group Policy Name: Resultant Set of Policy  
Version: 0  
Link: RSOP  
Group Name: group1  
Members: user1  
MemberOf: EXAMPLE\group9
```

### Informazioni correlate

[Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo](#)

### Visualizza informazioni sui criteri di accesso centrale

È possibile visualizzare informazioni dettagliate sui criteri di accesso centrale definiti in Active Directory. È inoltre possibile visualizzare informazioni sui criteri di accesso centrale applicati al server CIFS tramite oggetti Criteri di gruppo (GPO).

### A proposito di questa attività

Per impostazione predefinita, vengono visualizzate le seguenti informazioni:

- Nome SVM
- Nome della policy di accesso centrale
- SID
- Descrizione
- Tempo di creazione
- Tempo di modifica
- Regole dei membri



I server CIFS in modalità gruppo di lavoro non vengono visualizzati perché non supportano gli oggetti Criteri di gruppo.

### Fase

1. Visualizzare le informazioni sui criteri di accesso centrale eseguendo una delle seguenti operazioni:

Se si desidera visualizzare informazioni su tutti i criteri di accesso centrale...	Immettere il comando...
Definito in Active Directory	<code>vserver cifs group-policy central-access-policy show-defined -vserver vserver_name</code>
Applicato a un server CIFS	<code>vserver cifs group-policy central-access-policy show-applied -vserver vserver_name</code>

## Esempio

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutti i criteri di accesso centrale definiti in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-policy show-defined
```

```
Vserver  Name                      SID
-----  -
-----  -
vs1      p1                          S-1-17-3386172923-1132988875-3044489393-
3993546205
      Description: policy #1
      Creation Time: Tue Oct 22 09:34:13 2013
      Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                          S-1-17-1885229282-1100162114-134354072-
822349040
      Description: policy #2
      Creation Time: Tue Oct 22 10:28:20 2013
      Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                  r2
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutti i criteri di accesso centrale applicati alle macchine virtuali dello storage (SVM) sul cluster:



```
cluster1::> vserver cifs group-policy central-access-policy show-applied
```

Vserver	Name	SID
vs1	p1	S-1-17-3386172923-1132988875-3044489393-3993546205
Description: policy #1		
Creation Time: Tue Oct 22 09:34:13 2013		
Modification Time: Wed Oct 23 08:59:15 2013		
Member Rules: r1		
vs1	p2	S-1-17-1885229282-1100162114-134354072-822349040
Description: policy #2		
Creation Time: Tue Oct 22 10:28:20 2013		
Modification Time: Thu Oct 31 10:25:32 2013		
Member Rules: r1		
r2		

## Informazioni correlate

[Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso \(DAC\)](#)

[Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo](#)

[Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale](#)

## Visualizza informazioni sulle regole dei criteri di accesso centrale

È possibile visualizzare informazioni dettagliate sulle regole dei criteri di accesso centrale associate ai criteri di accesso centrale definiti in Active Directory. È inoltre possibile visualizzare informazioni sulle regole dei criteri di accesso centrale applicate al server CIFS attraverso gli oggetti Criteri di gruppo (GPO) dei criteri di accesso centrale.

## A proposito di questa attività

È possibile visualizzare informazioni dettagliate sulle regole dei criteri di accesso centrale definite e applicate. Per impostazione predefinita, vengono visualizzate le seguenti informazioni:

- Nome del server virtuale
- Nome della regola di accesso centrale
- Descrizione
- Tempo di creazione
- Tempo di modifica
- Permessi correnti
- Permessi proposti

- Risorse di destinazione

<b>Se si desidera visualizzare informazioni su tutte le regole dei criteri di accesso centrale associate ai criteri di accesso centrale...</b>	<b>Immettere il comando...</b>
Definito in Active Directory	<code>vserver cifs group-policy central-access-rule show-defined -vserver vserver_name</code>
Applicato a un server CIFS	<code>vserver cifs group-policy central-access-rule show-applied -vserver vserver_name</code>

### Esempio

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutte le regole dei criteri di accesso centrale associate ai criteri di accesso centrale definiti in Active Directory:

```
cluster1::> vserver cifs group-policy central-access-rule show-defined
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutte le regole dei criteri di accesso centrale associate ai criteri di accesso centrale applicati alle macchine virtuali di storage (SVM) sul cluster:

```
cluster1::> vserver cifs group-policy central-access-rule show-applied
```

```
Vserver      Name
-----
vs1          r1
             Description: rule #1
             Creation Time: Tue Oct 22 09:33:48 2013
             Modification Time: Tue Oct 22 09:33:48 2013
             Current Permissions: O:SYG:SYD:AR(A;;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;;FA;;;OW)(A;;;FA;;;BA)(A;;;FA;;;SY)

vs1          r2
             Description: rule #2
             Creation Time: Tue Oct 22 10:27:57 2013
             Modification Time: Tue Oct 22 10:27:57 2013
             Current Permissions: O:SYG:SYD:AR(A;;;FA;;;WD)
             Proposed Permissions: O:SYG:SYD:(A;;;FA;;;OW)(A;;;FA;;;BA)(A;;;FA;;;SY)
```

#### Informazioni correlate

[Protezione dell'accesso ai file mediante il controllo dinamico dell'accesso \(DAC\)](#)

[Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo](#)

[Visualizzazione di informazioni sui criteri di accesso centrale](#)

#### Comandi per la gestione delle password degli account dei computer dei server SMB

È necessario conoscere i comandi per la modifica, la reimpostazione e la disattivazione delle password e per la configurazione delle pianificazioni degli aggiornamenti automatici. È inoltre possibile configurare una pianificazione sul server SMB per aggiornarla automaticamente.

Se si desidera...	Utilizzare questo comando...
Modificare o reimpostare la password dell'account di dominio e conoscerla	<code>vserver cifs domain password change</code>
Reimpostare la password dell'account di dominio e non si conosce la password	<code>vserver cifs domain password reset</code>
Configurare i server SMB per la modifica automatica della password dell'account del computer	<code>vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true</code>

Se si desidera...	Utilizzare questo comando...
Disattiva le modifiche automatiche della password dell'account del computer sui server SMB	<pre>vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false</pre>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Gestire le connessioni dei controller di dominio

### Visualizza le informazioni sui server rilevati

È possibile visualizzare le informazioni relative ai server LDAP e ai controller di dominio rilevati sul server CIFS.

#### Fase

1. Per visualizzare le informazioni relative ai server rilevati, immettere il seguente comando: `vserver cifs domain discovered-servers show`

#### Esempio

L'esempio seguente mostra i server rilevati per SVM vs1:

```
cluster1::> vserver cifs domain discovered-servers show
```

Node: node1

Vserver: vs1

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

### Informazioni correlate

[Ripristino e riscoperta dei server](#)

[Interruzione o avvio del server CIFS](#)

### Reimpostare e riscoprire i server

La reimpostazione e la riscoperta dei server sul server CIFS consentono al server CIFS di eliminare le informazioni memorizzate sui server LDAP e sui controller di dominio. Dopo aver scartato le informazioni sul server, il server CIFS acquisisce nuovamente le informazioni correnti su questi server esterni. Questa operazione può essere utile quando i server connessi non rispondono in modo appropriato.

#### Fasi

1. Immettere il seguente comando: `vserver cifs domain discovered-servers reset-servers -vserver vserver_name`
2. Visualizzare le informazioni sui server appena rilevati: `vserver cifs domain discovered-servers show -vserver vserver_name`

### Esempio

Nell'esempio riportato di seguito vengono ripristinati e riutilizzati i server per la macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver vs1
```

```
cluster1::> vserver cifs domain discovered-servers show
```

Node: node1

Vserver: vs1

Domain Name	Type	Preference	DC-Name	DC-Address	Status
example.com	MS-LDAP	adequate	DC-1	1.1.3.4	OK
example.com	MS-LDAP	adequate	DC-2	1.1.3.5	OK
example.com	MS-DC	adequate	DC-1	1.1.3.4	OK
example.com	MS-DC	adequate	DC-2	1.1.3.5	OK

### Informazioni correlate

[Visualizzazione delle informazioni sui server rilevati](#)

[Interruzione o avvio del server CIFS](#)

### Gestire il rilevamento dei controller di dominio

A partire da ONTAP 9.3, è possibile modificare il processo predefinito in base al quale vengono rilevati i controller di dominio (DC). In questo modo, è possibile limitare il rilevamento al sito o a un pool di controller di dominio preferiti, con conseguente miglioramento delle performance a seconda dell'ambiente.

#### A proposito di questa attività

Per impostazione predefinita, il processo di rilevamento dinamico rileva tutti i controller di dominio disponibili, inclusi i controller di dominio preferiti, tutti i controller di dominio nel sito locale e tutti i controller di dominio remoti. Questa configurazione può portare a latenza nell'autenticazione e nell'accesso alle condivisioni in alcuni ambienti. Se il pool di controller di dominio che si desidera utilizzare è già stato determinato o se i controller di dominio remoti sono inadeguati o inaccessibili, è possibile modificare il metodo di ricerca.

In ONTAP 9.3 e versioni successive, il `discovery-mode` del parametro `cifs domain discovered-servers` il comando consente di selezionare una delle seguenti opzioni di ricerca:

- Vengono rilevati tutti i controller di dominio del dominio.

- Vengono rilevati solo i controller di dominio nel sito locale.

Il `default-site` È possibile definire un parametro per il server SMB in modo da utilizzare questa modalità con le LIF non assegnate a un sito in siti e servizi.

- Il rilevamento dei server non viene eseguito, la configurazione dei server SMB dipende solo dai controller di dominio preferiti.

Per utilizzare questa modalità, è necessario prima definire i controller di dominio preferiti per il server SMB.

## Fase

1. Specificare l'opzione di ricerca desiderata: `vserver cifs domain discovered-servers discovery-mode modify -vserver vserver_name -mode {all|site|none}`

Opzioni per `mode` parametro:

- `all`

Rilevare tutti i controller di dominio disponibili (impostazione predefinita).

- `site`

Limita il rilevamento DC al tuo sito.

- `none`

Utilizzare solo i controller di dominio preferiti e non eseguire il rilevamento.

## Aggiungere i domain controller preferiti

ONTAP rileva automaticamente i controller di dominio tramite DNS. In alternativa, è possibile aggiungere uno o più domain controller all'elenco dei domain controller preferiti per un dominio specifico.

### A proposito di questa attività

Se esiste già un elenco di controller di dominio preferito per il dominio specificato, il nuovo elenco viene Unito all'elenco esistente.

## Fase

1. Per aggiungere all'elenco dei domain controller preferiti, immettere il seguente comando:  
`vserver cifs domain preferred-dc add -vserver vserver_name -domain domain_name -preferred-dc IP_address, ...+`  
  
`-vserver vserver_name` Specifica il nome della SVM (Storage Virtual Machine).  
  
`-domain domain_name` Specifica il nome Active Directory completo del dominio a cui appartengono i controller di dominio specificati.  
  
`-preferred-dc IP_address,...` Specifica uno o più indirizzi IP dei domain controller preferiti, come elenco delimitato da virgole, in ordine di preferenza.

### Esempio

Il seguente comando aggiunge i domain controller 172.17.102.25 e 172.17.102.24 all'elenco dei domain controller preferiti che il server SMB su SVM vs1 utilizza per gestire l'accesso esterno al dominio cifs.lab.example.com.

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

### Informazioni correlate

[Comandi per la gestione dei domain controller preferiti](#)

#### Comandi per la gestione dei domain controller preferiti

È necessario conoscere i comandi per aggiungere, visualizzare e rimuovere i domain controller preferiti.

Se si desidera...	Utilizzare questo comando...
Aggiungere un domain controller preferito	<code>vserver cifs domain preferred-dc add</code>
Visualizzare i domain controller preferiti	<code>vserver cifs domain preferred-dc show</code>
Rimuovere un domain controller preferito	<code>vserver cifs domain preferred-dc remove</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

### Informazioni correlate

[Aggiunta di domain controller preferiti](#)

#### Abilitare le connessioni SMB2 ai controller di dominio

A partire da ONTAP 9.1, è possibile abilitare SMB versione 2.0 per la connessione a un controller di dominio. Questa operazione è necessaria se SMB 1.0 è stato disattivato nei controller di dominio. A partire da ONTAP 9.2, SMB2 è attivato per impostazione predefinita.

#### A proposito di questa attività

Il `smb2-enabled-for-dc-connections` L'opzione Command (comando) attiva l'impostazione predefinita di sistema per la release di ONTAP in uso. L'impostazione predefinita di sistema per ONTAP 9.1 è attivata per SMB 1.0 e disattivata per SMB 2.0. L'impostazione predefinita di sistema per ONTAP 9.2 è Enabled (attivato) per SMB 1.0 e Enabled (attivato) per SMB 2.0. Se il controller di dominio non riesce a negoziare inizialmente SMB 2.0, utilizza SMB 1.0.

SMB 1.0 può essere disattivato da ONTAP a un controller di dominio. In ONTAP 9.1, se SMB 1.0 è stato disattivato, SMB 2.0 deve essere attivato per comunicare con un controller di dominio.

Scopri di più su:

- "Verifica delle versioni SMB abilitate".
- "Versioni e funzionalità SMB supportate".



Se `-smb1-enabled-for-dc-connections` è impostato su `false` mentre `-smb1-enabled` è impostato su `true`, ONTAP nega le connessioni SMB 1.0 come client, ma continua ad accettare connessioni SMB 1.0 in entrata come server.

## Fasi

1. Prima di modificare le impostazioni di sicurezza SMB, verificare quali versioni SMB sono abilitate:  
`vserver cifs security show`
2. Scorrere l'elenco per visualizzare le versioni SMB.
3. Eseguire il comando appropriato utilizzando `smb2-enabled-for-dc-connections` opzione.

Se vuoi che SMB2 sia...	Immettere il comando...
Attivato	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections true</code>
Disattivato	<code>vserver cifs security modify -vserver vserver_name -smb2-enabled-for-dc-connections false</code>

## Abilitare le connessioni crittografate ai controller di dominio

A partire da ONTAP 9.8, è possibile specificare che le connessioni ai controller di dominio siano crittografate.

### A proposito di questa attività

ONTAP richiede la crittografia per le comunicazioni del controller di dominio (DC) quando `-encryption-required-for-dc-connection` l'opzione è impostata su `true`; il valore predefinito è `false`. Quando l'opzione è impostata, per le connessioni ONTAP-DC verrà utilizzato solo il protocollo SMB3, in quanto la crittografia è supportata solo da SMB3.

Quando sono richieste comunicazioni DC crittografate, il `-smb2-enabled-for-dc-connections` L'opzione viene ignorata, perché ONTAP negozia solo le connessioni SMB3. Se un controller di dominio non supporta SMB3 e la crittografia, ONTAP non si conatterà con esso.

## Fase

1. Abilitare la comunicazione crittografata con il controller di dominio: `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

## Utilizza sessioni null per accedere allo storage in ambienti non Kerberos

### Utilizza sessioni null per accedere alla panoramica dello storage in ambienti non Kerberos

L'accesso a sessione nulla fornisce le autorizzazioni per le risorse di rete, ad esempio i dati del sistema di storage, e per i servizi basati su client eseguiti nel sistema locale. Una



sessione nulla si verifica quando un processo client utilizza l'account "System `s`" per accedere a una risorsa di rete. La configurazione della sessione Null è specifica per l'autenticazione non Kerberos.

#### Modalità con cui il sistema storage fornisce l'accesso alla sessione Null

Poiché le condivisioni di sessione nulla non richiedono l'autenticazione, i client che richiedono l'accesso di sessione nulla devono avere i propri indirizzi IP mappati sul sistema di storage.

Per impostazione predefinita, i client di sessione Null non mappati possono accedere a determinati servizi di sistema ONTAP, ad esempio l'enumerazione delle condivisioni, ma non possono accedere ai dati del sistema di storage.



ONTAP supporta i valori di impostazione anonimi del Registro di sistema con Windows `RestrictAnonymous -restrict-anonymous` opzione. Ciò consente di controllare in che misura gli utenti Null non mappati possono visualizzare o accedere alle risorse di sistema. Ad esempio, è possibile disattivare l'enumerazione delle condivisioni e l'accesso alla condivisione IPC (la condivisione named pipe nascosta). Il `vserver cifs options modify` e `vserver cifs options show` le pagine man forniscono ulteriori informazioni su `-restrict-anonymous` opzione.

Se non diversamente configurato, un client che esegue un processo locale che richiede l'accesso al sistema di storage attraverso una sessione Null è membro solo di gruppi non restrittivi, come "Everyone". Per limitare l'accesso a sessioni Null alle risorse del sistema di storage selezionate, è possibile creare un gruppo a cui appartengono tutti i client di sessione Null; la creazione di questo gruppo consente di limitare l'accesso al sistema di storage e di impostare le autorizzazioni delle risorse del sistema di storage che si applicano specificamente ai client di sessione Null.

ONTAP fornisce una sintassi di mappatura in `vserver name-mapping` Set di comandi per specificare l'indirizzo IP dei client che hanno consentito l'accesso alle risorse del sistema di storage utilizzando una sessione utente nulla. Dopo aver creato un gruppo per utenti Null, è possibile specificare le restrizioni di accesso per le risorse del sistema di storage e le autorizzazioni delle risorse che si applicano solo alle sessioni Null. L'utente nullo viene identificato come accesso anonimo. Gli utenti Null non hanno accesso ad alcuna home directory.

A qualsiasi utente nullo che accede al sistema di storage da un indirizzo IP mappato vengono concesse autorizzazioni utente mappate. Prendere in considerazione le precauzioni appropriate per impedire l'accesso non autorizzato ai sistemi di storage mappati con utenti nulli. Per la massima protezione, posizionare il sistema di storage e tutti i client che richiedono l'accesso al sistema di storage utente nullo su una rete separata, per eliminare la possibilità di indirizzo IP "spoofing".

#### Informazioni correlate

[Configurazione delle restrizioni di accesso per utenti anonimi](#)

#### Concedere agli utenti Null l'accesso alle condivisioni del file system

È possibile consentire l'accesso alle risorse del sistema di storage da parte di client di sessione Null assegnando un gruppo da utilizzare da parte di client di sessione Null e registrando gli indirizzi IP dei client di sessione Null da aggiungere all'elenco dei client del sistema di storage autorizzati ad accedere ai dati utilizzando sessioni Null.

## Fasi

1. Utilizzare `vserver name-mapping create` Comando per mappare l'utente Null a qualsiasi utente Windows valido, con un qualificatore IP.

Il seguente comando associa l'utente null a user1 con un nome host valido google.com:

```
vserver name-mapping create -direction win-unix -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

Il seguente comando associa l'utente null a user1 con un indirizzo IP valido 10.238.2.54/32:

```
vserver name-mapping create -direction win-unix -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. Utilizzare `vserver name-mapping show` per confermare la mappatura dei nomi.

```
vserver name-mapping show

Vserver:    vs1
Direction: win-unix
Position Hostname      IP Address/Mask
-----
1          -           10.72.40.83/32      Pattern: anonymous logon
                                   Replacement: user1
```

3. Utilizzare `vserver cifs options modify -win-name-for-null-user` Comando per assegnare l'appartenenza a Windows all'utente Null.

Questa opzione è applicabile solo quando esiste una mappatura nome valida per l'utente Null.

```
vserver cifs options modify -win-name-for-null-user user1
```

4. Utilizzare `vserver cifs options show` Per confermare la mappatura dell'utente nullo all'utente o al gruppo Windows.

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

## Gestire gli alias NetBIOS per i server SMB

### Panoramica sulla gestione degli alias NetBIOS per i server SMB

Gli alias NetBIOS sono nomi alternativi per il server SMB che i client SMB possono utilizzare quando si connettono al server SMB. La configurazione degli alias NetBIOS per un server SMB può essere utile quando si consolidano i dati da altri file server nel server SMB e si desidera che il server SMB risponda ai nomi dei file server originali.

È possibile specificare un elenco di alias NetBIOS quando si crea il server SMB o in qualsiasi momento dopo la creazione del server SMB. È possibile aggiungere o rimuovere alias NetBIOS dall'elenco in qualsiasi momento. È possibile connettersi al server SMB utilizzando uno dei nomi presenti nell'elenco degli alias NetBIOS.

### Informazioni correlate

[Visualizzazione di informazioni su connessioni NetBIOS su TCP](#)

### Aggiungere un elenco di alias NetBIOS al server SMB

Se si desidera che i client SMB si connettano al server SMB utilizzando un alias, è possibile creare un elenco di alias NetBIOS oppure aggiungere alias NetBIOS a un elenco esistente di alias NetBIOS.

### A proposito di questa attività

- Il nome alias NetBIOS può contenere fino a 15 caratteri.
- È possibile configurare fino a 200 alias NetBIOS sul server SMB.
- I seguenti caratteri non sono consentiti:

@ \* ( ) = + [ ] | ; : " , < > / ?

### Fasi

#### 1. Aggiungere gli alias NetBIOS:

```
vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases  
NetBIOS_alias,...
```

```
vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases  
alias_1,alias_2,alias_3
```

- È possibile specificare uno o più alias NetBIOS utilizzando un elenco delimitato da virgole.
- Gli alias NetBIOS specificati vengono aggiunti all'elenco esistente.
- Se l'elenco è vuoto, viene creato un nuovo elenco di alias NetBIOS.

#### 2. Verificare che gli alias NetBIOS siano stati aggiunti correttamente: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

## Informazioni correlate

[Rimozione degli alias NetBIOS dall'elenco degli alias NetBIOS](#)

[Visualizzazione dell'elenco degli alias NetBIOS sui server CIFS](#)

## Rimuovere gli alias NetBIOS dall'elenco degli alias NetBIOS

Se non sono necessari alias NetBIOS specifici per un server CIFS, è possibile rimuovere tali alias NetBIOS dall'elenco. È inoltre possibile rimuovere tutti gli alias NetBIOS dall'elenco.

## A proposito di questa attività

È possibile rimuovere più alias NetBIOS utilizzando un elenco delimitato da virgole. È possibile rimuovere tutti gli alias NetBIOS su un server CIFS specificando - come valore per `-netbios-aliases` parametro.

## Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera rimuovere...	Inserisci...
Alias NetBIOS specifici dall'elenco	<pre>vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...</pre>
Tutti gli alias NetBIOS dall'elenco	<pre>vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -</pre>

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. Verificare che gli alias NetBIOS specificati siano stati rimossi: `vserver cifs show -vserver vserver_name -display-netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_2, ALIAS_3
```

## Visualizza l'elenco degli alias NetBIOS sui server CIFS

È possibile visualizzare l'elenco degli alias NetBIOS. Ciò può essere utile quando si desidera determinare l'elenco di nomi sui quali i client SMB possono stabilire connessioni al server CIFS.

### Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su...	Inserisci...
Alias NetBIOS di un server CIFS	<code>vserver cifs show -display-netbios -aliases</code>
L'elenco degli alias NetBIOS come parte delle informazioni dettagliate sul server CIFS	<code>vserver cifs show -instance</code>

Nell'esempio seguente vengono visualizzate informazioni sugli alias NetBIOS di un server CIFS:

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1
```

```
Server Name: CIFS_SERVER
```

```
NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

Nell'esempio seguente viene visualizzato l'elenco degli alias NetBIOS come parte delle informazioni dettagliate sul server CIFS:

```
vserver cifs show -instance
```

```
Vserver: vs1
CIFS Server NetBIOS Name: CIFS_SERVER
NetBIOS Domain/Workgroup Name: EXAMPLE
Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
Authentication Style: domain
CIFS Server Administrative Status: up
CIFS Server Description:
List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

Per ulteriori informazioni, consulta la pagina man per i comandi.

### Informazioni correlate

[Aggiunta di un elenco di alias NetBIOS al server CIFS](#)

**Determinare se i client SMB sono connessi utilizzando alias NetBIOS**

È possibile determinare se i client SMB sono connessi utilizzando alias NetBIOS e, in tal caso, quale alias NetBIOS viene utilizzato per stabilire la connessione. Ciò può essere utile per la risoluzione dei problemi di connessione.

**A proposito di questa attività**

È necessario utilizzare `-instance` Parametro per visualizzare l'alias NetBIOS (se presente) associato a una connessione SMB. Se il nome del server CIFS o un indirizzo IP viene utilizzato per effettuare la connessione SMB, l'output di `NetBIOS Name` il campo è `-` (trattino).

**Fase**

- 1. Eseguire l'azione desiderata:

Se si desidera visualizzare le informazioni NetBIOS per...	Inserisci...
Connessioni SMB	<code>vserver cifs session show -instance</code>
Connessioni che utilizzano un alias NetBIOS specificato:	<code>vserver cifs session show -instance -netbios-name <i>netbios_name</i></code>

Nell'esempio seguente vengono visualizzate informazioni sull'alias NetBIOS utilizzato per stabilire la connessione SMB con ID sessione 1:

```
vserver cifs session show -session-id 1 -instance
```

```
Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 127834
Incoming Data LIF IP Address: 10.1.1.25
Workstation: 10.2.2.50
Authentication Mechanism: NTLMv2
Windows User: EXAMPLE\user1
UNIX User: user1
Open Shares: 2
Open Files: 2
Open Other: 0
Connected Time: 1d 1h 10m 5s
Idle Time: 22s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: true
User Authenticated as: domain-user
NetBIOS Name: ALIAS1
SMB Encryption Status: Unencrypted
```

## Gestire varie attività del server SMB

### Arrestare o avviare il server CIFS

È possibile arrestare il server CIFS su una SVM, che può essere utile quando si eseguono attività mentre gli utenti non accedono ai dati tramite le condivisioni SMB. È possibile riavviare l'accesso SMB avviando il server CIFS. Arrestando il server CIFS, è anche possibile modificare i protocolli consentiti sulla macchina virtuale di storage (SVM).

### Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Arrestare il server CIFS	<code>`vserver cifs stop -vserver vserver_name [-foreground {true</code>
<code>false}}`</code>	Avviare il server CIFS
<code>`vserver cifs start -vserver vserver_name [-foreground {true</code>	<code>false}}`</code>

`-foreground` specifica se il comando deve essere eseguito in primo piano o in background. Se non si inserisce questo parametro, viene impostato su `true` e il comando viene eseguito in primo piano.

2. Verificare che lo stato amministrativo del server CIFS sia corretto utilizzando `vserver cifs show` comando.

### Esempio

I seguenti comandi avviano il server CIFS su SVM vs1:

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                Vserver: vs1
                                CIFS Server NetBIOS Name: VS1
                                NetBIOS Domain/Workgroup Name: DOMAIN
                                Fully Qualified Domain Name: DOMAIN.LOCAL
                                Default Site Used by LIFs Without Site Membership:
                                Authentication Style: domain
                                CIFS Server Administrative Status: up
```

### Informazioni correlate

[Visualizzazione delle informazioni sui server rilevati](#)

[Ripristino e riscoperta dei server](#)

### Spostare i server CIFS in diverse unità organizzative

Il processo di creazione del server CIFS utilizza l'unità organizzativa predefinita (OU) CN=computer durante l'installazione, a meno che non si specifichi un'unità organizzativa diversa. Dopo l'installazione, è possibile spostare i server CIFS in diverse unità organizzative.

### Fasi

1. Sul server Windows, aprire la struttura **utenti e computer di Active Directory**.
2. Individuare l'oggetto Active Directory per la macchina virtuale di storage (SVM).
3. Fare clic con il pulsante destro del mouse sull'oggetto e selezionare **Sposta**.
4. Selezionare l'unità organizzativa che si desidera associare alla SVM

### Risultati

L'oggetto SVM viene posizionato nell'unità organizzativa selezionata.

### Modificare il dominio DNS dinamico sulla SVM prima di spostare il server SMB

Se si desidera che il server DNS integrato in Active Directory registri dinamicamente i record DNS del server SMB in DNS quando si sposta il server SMB in un altro dominio, è necessario modificare il DNS dinamico (DDNS) sulla macchina virtuale di storage (SVM) prima di spostare il server SMB.

### Prima di iniziare



I servizi dei nomi DNS devono essere modificati sulla SVM per utilizzare il dominio DNS che contiene i record di posizione del servizio per il nuovo dominio che conterrà l'account del computer del server SMB. Se si utilizza un DDNS sicuro, è necessario utilizzare i server dei nomi DNS integrati in Active Directory.

### A proposito di questa attività

Sebbene DDNS (se configurato su SVM) aggiunga automaticamente i record DNS per i LIF dei dati al nuovo dominio, i record DNS per il dominio originale non vengono cancellati automaticamente dal server DNS originale. È necessario eliminarli manualmente.

Per completare le modifiche DDNS prima di spostare il server SMB, consultare il seguente argomento:

["Configurare i servizi DNS dinamici"](#)

### Aggiungere una SVM a un dominio Active Directory

È possibile unire una macchina virtuale di storage (SVM) a un dominio Active Directory senza eliminare il server SMB esistente modificando il dominio utilizzando `vserver cifs modify` comando. È possibile riconnessione al dominio corrente o aggiungerne uno nuovo.

#### Prima di iniziare

- La SVM deve già disporre di una configurazione DNS.
- La configurazione DNS per la SVM deve essere in grado di servire il dominio di destinazione.

I server DNS devono contenere i record di posizione del servizio (SRV) per i server LDAP e controller di dominio del dominio.

### A proposito di questa attività

- Lo stato amministrativo del server CIFS deve essere impostato su "dOwn" per procedere con la modifica del dominio Active Directory.
- Se il comando viene completato correttamente, lo stato amministrativo viene automaticamente impostato su "up".
- Quando si unisce un dominio, il completamento di questo comando potrebbe richiedere alcuni minuti.

#### Fasi

1. Unire la SVM al dominio del server CIFS: `vserver cifs modify -vserver vserver_name -domain domain_name -status-admin down`

Per ulteriori informazioni, vedere la pagina man di `vserver cifs modify` comando. Per riconfigurare il DNS per il nuovo dominio, consultare la pagina man del `vserver dns modify` comando.

Per creare un account macchina Active Directory per il server SMB, è necessario fornire il nome e la password di un account Windows con privilegi sufficienti per aggiungere computer a `ou= example ou` container all'interno di ``example`` dominio .com.

A partire da ONTAP 9.7, l'amministratore ad può fornire un URI a un file keytab in alternativa a un nome e una password a un account Windows con privilegi. Quando si riceve l'URI, includerlo in `-keytab-uri` con il `vserver cifs` comandi.

2. Verificare che il server CIFS si trovi nel dominio Active Directory desiderato: `vserver cifs show`

Esempio

Nell'esempio seguente, il server SMB "CIFSSERVER1" su SVM vs1 si unisce al dominio example.com utilizzando l'autenticazione keytab:

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show
```


	Server	Status	Domain/Workgroup	Authentication
Vserver	Name	Admin	Name	Style
-----	-----	-----	-----	-----
vs1	CIFSSERVER1	up	EXAMPLE	domain

Visualizza informazioni su connessioni NetBIOS su TCP

È possibile visualizzare informazioni sulle connessioni NetBIOS su TCP (NBT). Ciò può essere utile per la risoluzione dei problemi relativi a NetBIOS.

Fase

- 1. Utilizzare `vserver cifs nbtstat` Comando per visualizzare informazioni su NetBIOS su connessioni TCP.



NBNS (NetBIOS name service) su IPv6 non supportato.

Esempio

L'esempio seguente mostra le informazioni sul servizio nome NetBIOS visualizzate per "cluster1":

```
cluster1::> vserver cifs nbtstat
```

```
Vserver: vs1
Node:    cluster1-01
Interfaces:
          10.10.10.32
          10.10.10.33
Servers:
          17.17.1.2  (active  )
NBT Scope:
          [ ]
NBT Mode:
          [h]
NBT Name      NetBIOS Suffix  State    Time Left  Type
-----
CLUSTER_1     00                wins     57
CLUSTER_1     20                wins     57

Vserver: vs1
Node:    cluster1-02
Interfaces:
          10.10.10.35
Servers:
          17.17.1.2  (active  )
CLUSTER_1     00                wins     58
CLUSTER_1     20                wins     58
4 entries were displayed.
```

#### Comandi per la gestione dei server SMB

È necessario conoscere i comandi per la creazione, la visualizzazione, la modifica, l'arresto, l'avvio, Ed eliminazione dei server SMB. Sono inoltre disponibili comandi per reimpostare e riscoprire i server, modificare o reimpostare le password degli account dei computer, pianificare le modifiche per le password degli account dei computer e aggiungere o rimuovere alias NetBIOS.

Se si desidera...	Utilizzare questo comando...
Creare un server SMB	<code>vserver cifs create</code>
Visualizzare le informazioni su un server SMB	<code>vserver cifs show</code>
Modificare un server SMB	<code>vserver cifs modify</code>

Spostare un server SMB in un altro dominio	<code>vserver cifs modify</code>
Arrestare un server SMB	<code>vserver cifs stop</code>
Avviare un server SMB	<code>vserver cifs start</code>
Eliminare un server SMB	<code>vserver cifs delete</code>
Reimpostare e riscoprire i server per il server SMB	<code>vserver cifs domain discovered-servers reset-servers</code>
Modificare la password dell'account del computer del server SMB	<code>vserver cifs domain password change</code>
Reimpostare la password dell'account del computer del server SMB	<code>vserver cifs domain password change</code>
Pianificare le modifiche automatiche delle password per l'account del computer del server SMB	<code>vserver cifs domain password schedule modify</code>
Aggiungere alias NetBIOS per il server SMB	<code>vserver cifs add-netbios-aliases</code>
Rimuovere gli alias NetBIOS per il server SMB	<code>vserver cifs remove-netbios-aliases</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Informazioni correlate

["Cosa accade agli utenti e ai gruppi locali quando si eliminano i server SMB"](#)

### Attivare il servizio NetBIOS name

A partire da ONTAP 9, il servizio nomi NetBIOS (NBNS, a volte chiamato Windows Internet Name Service o WINS) è disattivato per impostazione predefinita. In precedenza, le SVM (Storage Virtual Machine) abilitate per CIFS inviavano trasmissioni di registrazione dei nomi indipendentemente dal fatto che WINS fosse abilitato o meno in una rete. Per limitare tali trasmissioni alle configurazioni in cui è richiesto NBNS, è necessario abilitare NBNS esplicitamente per i nuovi server CIFS.

### Prima di iniziare

- Se si utilizza già NBNS e si esegue l'aggiornamento a ONTAP 9, non è necessario completare questa attività. NBNS continuerà a funzionare come prima.
- NBNS è abilitato su UDP (porta 137).
- NBNS su IPv6 non supportato.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato).

```
set -privilege advanced
```

2. Abilitare NBNS su un server CIFS.

```
vserver cifs options modify -vserver <vserver name> -is-nbns-enabled  
true
```

3. Tornare al livello di privilegio admin.

```
set -privilege admin
```

## Utilizza IPv6 per l'accesso SMB e i servizi SMB

### Requisiti per l'utilizzo di IPv6

Prima di poter utilizzare IPv6 sul server SMB, è necessario sapere quali versioni di ONTAP e SMB lo supportano e quali sono i requisiti di licenza.

### Requisiti di licenza ONTAP

Non è richiesta alcuna licenza speciale per IPv6 quando SMB è concesso in licenza. La licenza SMB è inclusa con "ONTAP uno". Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.

### Requisiti di versione del protocollo SMB

- Per le SVM, ONTAP supporta IPv6 su tutte le versioni del protocollo SMB.



NBNS (NetBIOS name service) su IPv6 non supportato.

### Supporto per IPv6 con accesso SMB e servizi CIFS

Se si desidera utilizzare IPv6 sul server CIFS, è necessario conoscere il modo in cui ONTAP supporta IPv6 per l'accesso SMB e la comunicazione di rete per i servizi CIFS.

### Supporto di client e server Windows

ONTAP fornisce supporto per server e client Windows che supportano IPv6. Di seguito viene descritto il supporto IPv6 del client e del server Microsoft Windows:

- Windows 7, Windows 8, Windows Server 2008, Windows Server 2012 e versioni successive supportano IPv6 sia per la condivisione di file SMB che per i servizi Active Directory, inclusi i servizi DNS, LDAP, CLDAP e Kerberos.

Se gli indirizzi IPv6 sono configurati, Windows 7 e Windows Server 2008 e versioni successive utilizzano

IPv6 per impostazione predefinita per i servizi Active Directory. Sono supportate sia l'autenticazione NTLM che Kerberos su connessioni IPv6.

Tutti i client Windows supportati da ONTAP possono connettersi alle condivisioni SMB utilizzando gli indirizzi IPv6.

Per informazioni aggiornate sui client Windows supportati da ONTAP, vedere la "[Matrice di interoperabilità](#)".



I domini NT non sono supportati per IPv6.

### Supporto di servizi CIFS aggiuntivi

Oltre al supporto IPv6 per le condivisioni di file SMB e i servizi Active Directory, ONTAP fornisce il supporto IPv6 per:

- Servizi lato client, tra cui cartelle offline, profili di roaming, reindirizzamento cartelle e versioni precedenti
- Servizi lato server, tra cui home directory dinamiche (funzionalità home directory), symlink e Widelink, BranchCache, offload delle copie ODX, riferimenti automatici dei nodi, E versioni precedenti
- Servizi di gestione dell'accesso ai file, tra cui l'utilizzo di utenti e gruppi locali di Windows per il controllo degli accessi e la gestione dei diritti, l'impostazione delle autorizzazioni dei file e dei criteri di controllo mediante la CLI, il tracciamento della sicurezza, la gestione dei blocchi dei file e il monitoraggio dell'attività SMB
- Audit multiprotocollo NAS
- FPolicy
- Condivisioni continuamente disponibili, protocollo Witness e VSS remoto (utilizzato con configurazioni Hyper-V su SMB)

### Supporto del servizio di autenticazione e dei nomi

IPv6 supporta le comunicazioni con i seguenti name service:

- Controller di dominio
- Server DNS
- Server LDAP
- Server KDC
- Server NIS

### Modalità di utilizzo di IPv6 da parte dei server CIFS per la connessione a server esterni

Per creare una configurazione che soddisfi i requisiti, è necessario conoscere il modo in cui i server CIFS utilizzano IPv6 quando si effettua la connessione a server esterni.

- Selezione dell'indirizzo di origine

Se si tenta di connettersi a un server esterno, l'indirizzo di origine selezionato deve essere dello stesso tipo dell'indirizzo di destinazione. Ad esempio, se ci si connette a un indirizzo IPv6, la macchina virtuale di storage (SVM) che ospita il server CIFS deve disporre di una LIF dati o LIF di gestione che abbia un indirizzo IPv6 da utilizzare come indirizzo di origine. Analogamente, se ci si connette a un indirizzo IPv4, la SVM deve disporre di una LIF dati o LIF di gestione che abbia un indirizzo IPv4 da utilizzare come indirizzo

di origine.

- Per i server rilevati dinamicamente utilizzando il DNS, il rilevamento dei server viene eseguito come segue:
  - Se IPv6 è disattivato nel cluster, vengono rilevati solo gli indirizzi dei server IPv4.
  - Se IPv6 è attivato nel cluster, vengono rilevati gli indirizzi dei server IPv4 e IPv6. Entrambi i tipi possono essere utilizzati in base all' idoneità del server a cui appartiene l'indirizzo e alla disponibilità di dati IPv6 o IPv4 o LIF di gestione. Il rilevamento dinamico dei server viene utilizzato per rilevare i controller di dominio e i servizi associati, come LSA, NETLOGON, Kerberos e LDAP.
- Connettività del server DNS

Se SVM utilizza IPv6 durante la connessione a un server DNS, dipende dalla configurazione dei servizi di nomi DNS. Se i servizi DNS sono configurati per l'utilizzo degli indirizzi IPv6, le connessioni vengono effettuate utilizzando IPv6. Se lo si desidera, la configurazione DNS name Services può utilizzare gli indirizzi IPv4 in modo che le connessioni ai server DNS continuino a utilizzare gli indirizzi IPv4. È possibile specificare combinazioni di indirizzi IPv4 e IPv6 durante la configurazione dei servizi dei nomi DNS.

- Connettività al server LDAP

Se SVM utilizza IPv6 durante la connessione a un server LDAP, dipende dalla configurazione del client LDAP. Se il client LDAP è configurato per l'utilizzo degli indirizzi IPv6, le connessioni vengono effettuate utilizzando IPv6. Se lo si desidera, la configurazione del client LDAP può utilizzare gli indirizzi IPv4 in modo che le connessioni ai server LDAP continuino a utilizzare gli indirizzi IPv4. È possibile specificare combinazioni di indirizzi IPv4 e IPv6 durante la configurazione del client LDAP.



La configurazione del client LDAP viene utilizzata per la configurazione di LDAP per i servizi nome utente, gruppo e netgroup UNIX.

- Connettività del server NIS

La possibilità che SVM utilizzi IPv6 durante la connessione a un server NIS dipende dalla configurazione dei servizi dei nomi NIS. Se i servizi NIS sono configurati per l'utilizzo degli indirizzi IPv6, le connessioni vengono effettuate utilizzando IPv6. Se lo si desidera, la configurazione NIS name Services può utilizzare gli indirizzi IPv4 in modo che le connessioni ai server NIS continuino a utilizzare gli indirizzi IPv4. È possibile specificare combinazioni di indirizzi IPv4 e IPv6 durante la configurazione dei servizi NIS.



I NIS name service vengono utilizzati per memorizzare e gestire gli oggetti utente, gruppo, netgroup e nome host UNIX.

## Informazioni correlate

[Abilitazione di IPv6 per SMB \(solo amministratori di cluster\)](#)

[Monitoraggio e visualizzazione delle informazioni sulle sessioni SMB IPv6](#)

### Abilitare IPv6 per SMB (solo amministratori di cluster)

Le reti IPv6 non sono abilitate durante l'installazione del cluster. Per utilizzare IPv6 per SMB, un amministratore del cluster deve abilitare IPv6 al termine della configurazione del cluster. Quando l'amministratore del cluster attiva IPv6, viene attivato per l'intero cluster.

## Fase

1. Attiva IPv6: `network options ipv6 modify -enabled true`

Per ulteriori informazioni sull'attivazione di IPv6 nel cluster e sulla configurazione di LIF IPv6, consultare la *Guida alla gestione di rete*.

IPv6 è attivato. È possibile configurare le LIF dei dati IPv6 per l'accesso SMB.

### Informazioni correlate

[Monitoraggio e visualizzazione delle informazioni sulle sessioni SMB IPv6](#)

["Gestione della rete"](#)

### Disattiva IPv6 per SMB

Anche se IPv6 è attivato sul cluster utilizzando un'opzione di rete, non è possibile disattivare IPv6 per SMB utilizzando lo stesso comando. Al contrario, ONTAP disattiva IPv6 quando l'amministratore del cluster disattiva l'ultima interfaccia abilitata per IPv6 sul cluster. È necessario comunicare con l'amministratore del cluster in merito alla gestione delle interfacce abilitate per IPv6.

Per ulteriori informazioni sulla disattivazione di IPv6 nel cluster, consultare la *Guida alla gestione di rete*.

### Informazioni correlate

["Gestione della rete"](#)

### Monitorare e visualizzare informazioni sulle sessioni SMB IPv6

È possibile monitorare e visualizzare le informazioni sulle sessioni SMB connesse tramite reti IPv6. Queste informazioni sono utili per determinare quali client si connettono utilizzando IPv6 e altre informazioni utili sulle sessioni SMB IPv6.

### Fase

1. Eseguire l'azione desiderata:

Se si desidera determinare se...	Immettere il comando...
Le sessioni SMB a una macchina virtuale di storage (SVM) sono connesse tramite IPv6	<code>vserver cifs session show -vserver <i>vserver_name</i> -instance</code>
IPv6 viene utilizzato per le sessioni SMB attraverso un indirizzo LIF specificato	<code>vserver cifs session show -vserver <i>vserver_name</i> -lif-address <i>LIF_IP_address</i> -instance</code>  <i>LIF_IP_address</i> È l'indirizzo IPv6 del LIF dei dati.

## Impostare l'accesso ai file utilizzando SMB

### Configurare gli stili di sicurezza



## Quali sono gli stili di sicurezza e i loro effetti

Esistono quattro diversi stili di sicurezza: UNIX, NTFS, misto e unificato. Ogni stile di sicurezza ha un effetto diverso sul modo in cui vengono gestite le autorizzazioni per i dati. È necessario comprendere i diversi effetti per assicurarsi di selezionare lo stile di sicurezza appropriato per i propri scopi.

È importante comprendere che gli stili di sicurezza non determinano quali tipi di client possono o non possono accedere ai dati. Gli stili di sicurezza determinano solo il tipo di autorizzazioni utilizzate da ONTAP per controllare l'accesso ai dati e il tipo di client in grado di modificare tali autorizzazioni.

Ad esempio, se un volume utilizza lo stile di sicurezza UNIX, i client SMB possono comunque accedere ai dati (purché autenticino e autorizzino correttamente) a causa della natura multiprotocollo di ONTAP. Tuttavia, ONTAP utilizza autorizzazioni UNIX che solo i client UNIX possono modificare utilizzando strumenti nativi.

Stile di sicurezza	Client in grado di modificare le autorizzazioni	Autorizzazioni che i client possono utilizzare	Risultato di uno stile di sicurezza efficace	Client che possono accedere ai file
UNIX	NFS	Bit di modalità NFSv3	UNIX	NFS e SMB
ACL NFSv4.x	UNIX	NTFS	PMI	ACL NTFS
NTFS	Misto	NFS o SMB	Bit di modalità NFSv3	UNIX
ACL NFSv4.x	UNIX	ACL NTFS	NTFS	Unificato
NFS o SMB	Bit di modalità NFSv3	UNIX	ACL NFSv4.1	UNIX
ACL NTFS	NTFS	Unificato (solo per volumi infiniti, in ONTAP 9.4 e versioni precedenti).	NFS o SMB	Bit di modalità NFSv3
UNIX	ACL NFSv4.1			ACL NTFS

I volumi FlexVol supportano UNIX, NTFS e stili di sicurezza misti. Quando lo stile di sicurezza è misto o unificato, le autorizzazioni effettive dipendono dal tipo di client che ha modificato le autorizzazioni per ultima, perché gli utenti impostano lo stile di sicurezza su base individuale. Se l'ultimo client che ha modificato le autorizzazioni era un client NFSv3, le autorizzazioni sono bit di modalità UNIX NFSv3. Se l'ultimo client era un client NFSv4, le autorizzazioni sono ACL NFSv4. Se l'ultimo client era un client SMB, le autorizzazioni sono ACL NTFS di Windows.

Lo stile di sicurezza unificato è disponibile solo con volumi infiniti, che non sono più supportati in ONTAP 9.5 e versioni successive. Per ulteriori informazioni, vedere ["Panoramica sulla gestione dei volumi FlexGroup"](#).

A partire da ONTAP 9.2, la `show-effective-permissions al vserver security file-directory` II comando consente di visualizzare le autorizzazioni effettive concesse a un utente Windows o UNIX sul percorso di file o cartella specificato. Inoltre, il parametro opzionale `-share-name` consente di visualizzare

l'autorizzazione di condivisione effettiva.



ONTAP imposta inizialmente alcune autorizzazioni predefinite per i file. Per impostazione predefinita, lo stile di sicurezza effettivo su tutti i dati nei volumi UNIX, misti e di sicurezza unificata è UNIX e il tipo di permessi effettivo è UNIX mode bits (0755 se non diversamente specificato) fino a quando non viene configurato da un client come consentito dallo stile di sicurezza predefinito. Per impostazione predefinita, lo stile di sicurezza effettivo su tutti i dati nei volumi di sicurezza NTFS è NTFS e dispone di un ACL che consente il controllo completo di tutti.

## Dove e quando impostare gli stili di sicurezza

Gli stili di sicurezza possono essere impostati su volumi FlexVol (sia root che volumi di dati) e qtree. Gli stili di sicurezza possono essere impostati manualmente al momento della creazione, ereditati automaticamente o modificati in un secondo momento.

## Decidere quale stile di sicurezza utilizzare sulle SVM

Per aiutarti a decidere quale stile di sicurezza utilizzare su un volume, devi considerare due fattori. Il fattore principale è il tipo di amministratore che gestisce il file system. Il fattore secondario è il tipo di utente o servizio che accede ai dati sul volume.

Quando si configura lo stile di protezione su un volume, è necessario considerare le esigenze dell'ambiente per assicurarsi di selezionare lo stile di protezione migliore ed evitare problemi con la gestione delle autorizzazioni. Le seguenti considerazioni possono aiutarti a decidere:

Stile di sicurezza	Scegliere se...
UNIX	<ul style="list-style-type: none"><li>• Il file system è gestito da un amministratore UNIX.</li><li>• La maggior parte degli utenti sono client NFS.</li><li>• Un'applicazione che accede ai dati utilizza un utente UNIX come account del servizio.</li></ul>
NTFS	<ul style="list-style-type: none"><li>• Il file system è gestito da un amministratore di Windows.</li><li>• La maggior parte degli utenti è costituita da client SMB.</li><li>• Un'applicazione che accede ai dati utilizza un utente Windows come account del servizio.</li></ul>
Misto	Il file system è gestito dagli amministratori UNIX e Windows e gli utenti sono costituiti da client NFS e SMB.

## Come funziona l'ereditarietà dello stile di sicurezza

Se non si specifica lo stile di protezione durante la creazione di un nuovo volume FlexVol o di un qtree, questo eredita il proprio stile di protezione in modi diversi.

Gli stili di sicurezza vengono ereditati nel modo seguente:

- Un volume FlexVol eredita lo stile di sicurezza del volume root del volume SVM contenente.
- Un qtree eredita lo stile di protezione del volume FlexVol contenente.
- Un file o una directory eredita lo stile di protezione del volume o qtree FlexVol contenente.

### **In che modo ONTAP conserva le autorizzazioni UNIX**

Quando i file in un volume FlexVol che dispongono attualmente di autorizzazioni UNIX vengono modificati e salvati dalle applicazioni Windows, ONTAP può conservare le autorizzazioni UNIX.

Quando le applicazioni sui client Windows modificano e salvano i file, leggono le proprietà di protezione del file, creano un nuovo file temporaneo, applicano tali proprietà al file temporaneo e assegnano al file temporaneo il nome del file originale.

Quando i client Windows eseguono una query per le proprietà di protezione, ricevono un ACL costruito che rappresenta esattamente le autorizzazioni UNIX. L'unico scopo di questo ACL costruito è quello di preservare le autorizzazioni UNIX del file, poiché i file vengono aggiornati dalle applicazioni Windows per garantire che i file risultanti abbiano le stesse autorizzazioni UNIX. ONTAP non imposta alcun ACL NTFS utilizzando l'ACL costruito.

### **Gestire le autorizzazioni UNIX utilizzando la scheda protezione di Windows**

Se si desidera modificare le autorizzazioni UNIX di file o cartelle in volumi misti di sicurezza o qtree su SVM, è possibile utilizzare la scheda Security (protezione) sui client Windows. In alternativa, è possibile utilizzare applicazioni in grado di eseguire query e impostare gli ACL di Windows.

- Modifica delle autorizzazioni UNIX

È possibile utilizzare la scheda protezione di Windows per visualizzare e modificare le autorizzazioni UNIX per un volume misto di sicurezza o qtree. Se si utilizza la scheda principale di Windows Security per modificare le autorizzazioni UNIX, è necessario rimuovere prima l'ACE esistente che si desidera modificare (in questo modo i bit di modalità vengono impostati su 0) prima di apportare le modifiche. In alternativa, è possibile utilizzare l'editor avanzato per modificare le autorizzazioni.

Se vengono utilizzate le autorizzazioni di modalità, è possibile modificare direttamente le autorizzazioni di modalità per UID, GID e altri (tutti gli altri utenti con un account sul computer). Ad esempio, se l'UID visualizzato dispone delle autorizzazioni r-x, è possibile modificare le autorizzazioni UID in rwx.

- Modifica delle autorizzazioni UNIX in autorizzazioni NTFS

È possibile utilizzare la scheda protezione di Windows per sostituire gli oggetti di protezione UNIX con oggetti di protezione di Windows su un volume misto di tipo sicurezza o qtree in cui i file e le cartelle hanno uno stile di protezione efficace UNIX.

Prima di poter sostituire le voci di autorizzazione UNIX con gli oggetti utente e gruppo di Windows desiderati, è necessario rimuovere tutte le voci di autorizzazione UNIX elencate. È quindi possibile configurare gli ACL basati su NTFS sugli oggetti utente e Gruppo di Windows. Rimuovendo tutti gli oggetti di protezione UNIX e aggiungendo solo utenti e gruppi Windows a un file o a una cartella in un volume o qtree misto di sicurezza, è possibile modificare lo stile di protezione effettivo del file o della cartella da UNIX a NTFS.

Quando si modificano le autorizzazioni di una cartella, il comportamento predefinito di Windows consiste nel propagare queste modifiche a tutte le sottocartelle e a tutti i file. Pertanto, se non si desidera propagare una modifica dello stile di protezione a tutte le cartelle figlio, le sottocartelle e i file, è necessario modificare l'impostazione di propagazione desiderata.

### Configurare gli stili di sicurezza sui volumi root SVM

È possibile configurare lo stile di protezione del volume root SVM (Storage Virtual Machine) per determinare il tipo di autorizzazioni utilizzate per i dati sul volume root di SVM.

#### Fasi

1. Utilizzare `vserver create` con il `-rootvolume-security-style` parametro per definire lo stile di sicurezza.

Le opzioni possibili per lo stile di protezione del volume root sono: `unix`, `ntfs`, o `mixed`.

2. Visualizzare e verificare la configurazione, incluso lo stile di sicurezza del volume root della SVM creata:  
`vserver show -vserver vserver_name`

### Configurare gli stili di sicurezza sui volumi FlexVol

È possibile configurare lo stile di sicurezza del volume FlexVol per determinare il tipo di autorizzazioni utilizzate per i dati sui volumi FlexVol della macchina virtuale di storage (SVM).

#### Fasi

1. Eseguire una delle seguenti operazioni:

Se il volume FlexVol...	Utilizzare il comando...
Non esiste ancora	<code>volume create</code> e includono <code>-security-style</code> parametro per specificare lo stile di sicurezza.
Esiste già	<code>volume modify</code> e includono <code>-security-style</code> parametro per specificare lo stile di sicurezza.

Le opzioni possibili per lo stile di protezione del volume FlexVol sono `unix`, `ntfs`, o `mixed`.

Se non si specifica uno stile di protezione durante la creazione di un volume FlexVol, il volume eredita lo stile di protezione del volume root.

Per ulteriori informazioni su `volume create` oppure `volume modify` comandi, vedere ["Gestione dello storage logico"](#).

2. Per visualizzare la configurazione, incluso lo stile di protezione del volume FlexVol creato, immettere il seguente comando:

```
volume show -volume volume_name -instance
```

## Configurare gli stili di sicurezza sui qtree

Lo stile di protezione del volume qtree viene configurato per determinare il tipo di autorizzazioni utilizzate per i dati su qtree.

### Fasi

1. Eseguire una delle seguenti operazioni:

Se il qtree...	Utilizzare il comando...
Non esiste ancora	<code>volume qtree create</code> e includono <code>-security -style</code> parametro per specificare lo stile di sicurezza.
Esiste già	<code>volume qtree modify</code> e includono <code>-security -style</code> parametro per specificare lo stile di sicurezza.

Le opzioni possibili per lo stile di sicurezza qtree sono: `unix`, `ntfs`, o `mixed`.

Se non si specifica uno stile di protezione durante la creazione di un qtree, lo stile di protezione predefinito è `mixed`.

Per ulteriori informazioni su `volume qtree create` oppure `volume qtree modify` comandi, vedere ["Gestione dello storage logico"](#).

2. Per visualizzare la configurazione, incluso lo stile di sicurezza del qtree creato, immettere il seguente comando: `volume qtree show -qtree qtree_name -instance`

## Creare e gestire volumi di dati in spazi dei nomi NAS

### Panoramica sulla creazione e gestione dei volumi di dati negli spazi dei nomi NAS

Per gestire l'accesso ai file in un ambiente NAS, è necessario gestire i volumi di dati e i punti di giunzione sulla macchina virtuale di storage (SVM). Ciò include la pianificazione dell'architettura dello spazio dei nomi, la creazione di volumi con o senza punti di giunzione, il montaggio o lo smontaggio di volumi e la visualizzazione di informazioni sui volumi di dati e sugli spazi dei nomi dei server NFS o CIFS.

### Creare volumi di dati con punti di giunzione specificati

È possibile specificare il punto di giunzione quando si crea un volume di dati. Il volume risultante viene montato automaticamente nel punto di giunzione ed è immediatamente disponibile per la configurazione dell'accesso NAS.

### Prima di iniziare

L'aggregato in cui si desidera creare il volume deve già esistere.



I seguenti caratteri non possono essere utilizzati nel percorso di giunzione: \* N. " > < | ? .

Inoltre, la lunghezza del percorso di giunzione non può superare i 255 caratteri.

## Fasi

1. Creare il volume con un punto di giunzione: `volume create -vserver vs1 -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

Il percorso di giunzione deve iniziare con root (/) e può contenere sia directory che volumi congiunti. Il percorso di giunzione non deve contenere il nome del volume. I percorsi di giunzione sono indipendenti dal nome del volume.

Specificare uno stile di sicurezza del volume è facoltativo. Se non si specifica uno stile di protezione, ONTAP crea il volume con lo stesso stile di protezione applicato al volume root della macchina virtuale di storage (SVM). Tuttavia, lo stile di sicurezza del volume root potrebbe non corrispondere allo stile di sicurezza che si desidera applicare al volume di dati creato. Si consiglia di specificare lo stile di protezione quando si crea il volume per ridurre al minimo i problemi di accesso ai file difficili da risolvere.

Il percorso di giunzione è privo di maiuscole e minuscole; /ENG è uguale a. /eng. Se si crea una condivisione CIFS, Windows considera il percorso di giunzione come se fosse sensibile alla distinzione tra maiuscole e minuscole. Ad esempio, se la giunzione è /ENG, il percorso di una condivisione CIFS deve iniziare con /ENG, non /eng.

Per personalizzare un volume di dati, è possibile utilizzare molti parametri opzionali. Per ulteriori informazioni, consultare le pagine man del `volume create` comando.

2. Verificare che il volume sia stato creato con il punto di giunzione desiderato: `volume show -vserver vs1 -volume volume_name -junction`

## Esempio

Nell'esempio riportato di seguito viene creato un volume denominato "home4" situato su SVM vs1 con un percorso di giunzione /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	home4	true	/eng/home	RW_volume

## Creare volumi di dati senza specificare punti di giunzione

È possibile creare un volume di dati senza specificare un punto di giunzione. Il volume risultante non viene montato automaticamente e non è disponibile per la configurazione per l'accesso NAS. È necessario montare il volume prima di poter configurare le

condivisioni SMB o le esportazioni NFS per quel volume.

### Prima di iniziare

L'aggregato in cui si desidera creare il volume deve già esistere.

### Fasi

1. Creare il volume senza un punto di giunzione utilizzando il seguente comando: `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

Specificare uno stile di sicurezza del volume è facoltativo. Se non si specifica uno stile di protezione, ONTAP crea il volume con lo stesso stile di protezione applicato al volume root della macchina virtuale di storage (SVM). Tuttavia, lo stile di sicurezza del volume root potrebbe non corrispondere allo stile di sicurezza che si desidera applicare al volume di dati. Si consiglia di specificare lo stile di protezione quando si crea il volume per ridurre al minimo i problemi di accesso ai file difficili da risolvere.

Per personalizzare un volume di dati, è possibile utilizzare molti parametri opzionali. Per ulteriori informazioni, consultare le pagine man del `volume create` comando.

2. Verificare che il volume sia stato creato senza un punto di giunzione: `volume show -vserver vserver_name -volume volume_name -junction`

### Esempio

Nell'esempio seguente viene creato un volume denominato "sales" situato su SVM vs1 che non è montato in un punto di giunzione:

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful
```

```
cluster1::> volume show -vserver vs1 -junction
```

		Junction		Junction
Vserver	Volume	Active	Junction Path	Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	-	-	-

### Montare o smontare i volumi esistenti nello spazio dei nomi NAS

È necessario montare un volume sullo spazio dei nomi NAS prima di poter configurare l'accesso del client NAS ai dati contenuti nei volumi SVM (Storage Virtual Machine). È possibile montare un volume su un punto di giunzione se non è attualmente montato. È anche possibile smontare i volumi.

### A proposito di questa attività

Se si smonta e si porta un volume offline, tutti i dati all'interno del punto di giunzione, inclusi i dati nei volumi con punti di giunzione contenuti nello spazio dei nomi del volume non montato, sono inaccessibili ai client



Per interrompere l'accesso del client NAS a un volume, non è sufficiente smontare semplicemente il volume. È necessario portare il volume offline o eseguire altre operazioni per assicurarsi che le cache degli handle dei file sul lato client siano invalidate. Per ulteriori informazioni, consultare il seguente articolo della Knowledge base: ["I client NFSv3 hanno ancora accesso a un volume dopo essere stati rimossi dallo spazio dei nomi in ONTAP"](#)

Quando si dismonta e si porta un volume offline, i dati all'interno del volume non vengono persi. Inoltre, vengono mantenute le policy di esportazione dei volumi esistenti e le condivisioni SMB create sul volume o su directory e punti di giunzione all'interno del volume non montato. Se si rimonta il volume non montato, i client NAS possono accedere ai dati contenuti nel volume utilizzando le policy di esportazione e le condivisioni SMB esistenti.

Fasi

- 1. Eseguire l'azione desiderata:

Se si desidera...	Immettere i comandi...
Montare un volume	<code>volume mount -vserver svm_name -volume volume_name -junction-path junction_path</code>
Smontare un volume	<code>volume unmount -vserver svm_name -volume volume_name</code>  <code>volume offline -vserver svm_name -volume volume_name</code>

- 2. Verificare che il volume si trovi nello stato di montaggio desiderato:

```
volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active
```

Esempi

Nell'esempio seguente viene montato un volume denominato "sques" situato su SVM "VS1" al punto di giunzione "/sales»":

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver    volume    state    junction-path    junction-active
-----
vs1        data      online   /data            true
vs1        home4     online   /eng/home        true
vs1        sales     online   /sales           true
```



L'esempio seguente smonta e porta offline un volume chiamato "dati" situato su SVM "VS1":

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active
```

vserver	volume	state	junction-path	junction-active
vs1	data	offline	-	-
vs1	home4	online	/eng/home	true
vs1	sales	online	/sales	true

**Visualizzare le informazioni sul punto di giunzione e sul montaggio del volume**

È possibile visualizzare informazioni sui volumi montati per le macchine virtuali di storage (SVM) e sui punti di giunzione in cui vengono montati i volumi. È inoltre possibile determinare quali volumi non sono montati su un punto di giunzione. È possibile utilizzare queste informazioni per comprendere e gestire lo spazio dei nomi SVM.

**Fasi**

- 1. Eseguire l'azione desiderata:

Se si desidera visualizzare...	Immettere il comando...
Informazioni riepilogative sui volumi montati e non montati su SVM	volume show -vserver vserver_name -junction
Informazioni dettagliate sui volumi montati e non montati su SVM	volume show -vserver vserver_name -volume volume_name -instance
Informazioni specifiche sui volumi montati e non montati su SVM	a. Se necessario, è possibile visualizzare campi validi per -fields utilizzando il seguente comando: volume show -fields ?  b. Visualizzare le informazioni desiderate utilizzando -fields parametro: volume show -vserver vserver_name -fieldname,...

**Esempi**

Nell'esempio seguente viene visualizzato un riepilogo dei volumi montati e non montati su SVM vs1:

```
cluster1::> volume show -vserver vs1 -junction
```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	home4	true	/eng/home	RW_volume
vs1	vs1_root	-	/	-
vs1	sales	true	/sales	RW_volume

Nell'esempio seguente vengono visualizzate informazioni sui campi specificati per i volumi che si trovano su SVM vs2:

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
```

vserver	volume	aggregate	size	state	type	security-style	junction-path	junction-parent	node
vs2	data1	aggr3	2GB	online	RW	unix	-	-	node3
vs2	data2	aggr3	1GB	online	RW	ntfs	/data2		
vs2	data2_root	aggr3	8GB	online	RW	ntfs	/data2/d2_1		
vs2	data2_1	aggr3	8GB	online	RW	ntfs	/data2/d2_2		
vs2	data2_2	aggr3	8GB	online	RW	ntfs	/data2/d2_2		
vs2	pubs	aggr1	1GB	online	RW	unix	/publications		
vs2	images	aggr3	2TB	online	RW	ntfs	/images		
vs2	logs	aggr1	1GB	online	RW	unix	/logs		
vs2	vs2_root	aggr3	1GB	online	RW	ntfs	/	-	node3

## Configurare le mappature dei nomi

### Panoramica sulla configurazione delle mappature dei nomi

ONTAP utilizza la mappatura dei nomi per mappare le identità CIFS alle identità UNIX, le identità Kerberos alle identità UNIX e le identità UNIX alle identità CIFS. Queste informazioni sono necessarie per ottenere le credenziali dell'utente e fornire l'accesso corretto ai file, indipendentemente dal fatto che si stia connettendo da un client NFS o

## CIFS.

Esistono due eccezioni per le quali non è necessario utilizzare la mappatura dei nomi:

- Si configura un ambiente UNIX puro e non si prevede di utilizzare l'accesso CIFS o lo stile di sicurezza NTFS sui volumi.
- Viene configurato l'utente predefinito da utilizzare.

In questo scenario, la mappatura dei nomi non è necessaria perché, invece di mappare ogni singola credenziale client, tutte le credenziali client vengono mappate allo stesso utente predefinito.

Si noti che è possibile utilizzare la mappatura dei nomi solo per gli utenti, non per i gruppi.

Tuttavia, è possibile mappare un gruppo di singoli utenti a un utente specifico. Ad esempio, è possibile mappare tutti gli utenti ad che iniziano o terminano con la parola SALES a un utente UNIX specifico e all'UID dell'utente.

### Come funziona la mappatura dei nomi

Quando ONTAP deve mappare le credenziali per un utente, controlla innanzitutto il database di mappatura dei nomi locali e il server LDAP per verificare la presenza di una mappatura esistente. Se controlla uno o entrambi e in quale ordine viene determinato dalla configurazione del servizio di nomi della SVM.

- Per la mappatura da Windows a UNIX

Se non viene trovata alcuna mappatura, ONTAP verifica se il nome utente Windows minuscolo è un nome utente valido nel dominio UNIX. Se non funziona, utilizza l'utente UNIX predefinito, a condizione che sia configurato. Se l'utente UNIX predefinito non è configurato e ONTAP non può ottenere un mapping in questo modo, il mapping non riesce e viene restituito un errore.

- Per la mappatura da UNIX a Windows

Se non viene trovata alcuna mappatura, ONTAP tenta di trovare un account Windows che corrisponda al nome UNIX nel dominio SMB. Se non funziona, utilizza l'utente SMB predefinito, a condizione che sia configurato. Se l'utente CIFS predefinito non è configurato e ONTAP non può ottenere un mapping in questo modo, il mapping non riesce e viene restituito un errore.

Per impostazione predefinita, gli account del computer vengono mappati all'utente UNIX predefinito specificato. Se non viene specificato alcun utente UNIX predefinito, il mapping degli account del computer non riesce.

- A partire da ONTAP 9.5, è possibile mappare gli account dei computer a utenti diversi da quelli predefiniti.
- In ONTAP 9.4 e versioni precedenti, non è possibile mappare gli account dei computer ad altri utenti.

Anche se vengono definite le mappature dei nomi per gli account macchina, le mappature vengono ignorate.

### Multidominio ricerca le mappature dei nomi utente da UNIX a Windows

ONTAP supporta le ricerche su più domini durante la mappatura degli utenti UNIX agli utenti Windows. In tutti i domini attendibili rilevati vengono ricercate le corrispondenze del

modello di sostituzione fino a quando non viene restituito un risultato corrispondente. In alternativa, è possibile configurare un elenco di domini attendibili preferiti, che viene utilizzato al posto dell'elenco di domini attendibili rilevati e che viene ricercato in ordine fino a quando non viene restituito un risultato corrispondente.

### **Il modo in cui i trust di dominio influiscono sulle ricerche di mappatura dei nomi utente da UNIX a Windows**

Per comprendere il funzionamento della mappatura dei nomi utente multidominio, è necessario comprendere il funzionamento dei trust di dominio con ONTAP. Le relazioni di trust di Active Directory con il dominio principale del server CIFS possono essere un trust bidirezionale o possono essere uno dei due tipi di trust unidirezionali, un trust inbound o un trust outbound. Il dominio principale è il dominio a cui appartiene il server CIFS sulla SVM.

- *Fiducia bidirezionale*

Con trust bidirezionali, entrambi i domini si fidano l'uno dell'altro. Se il dominio principale del server CIFS ha un trust bidirezionale con un altro dominio, il dominio principale può autenticare e autorizzare un utente appartenente al dominio attendibile e viceversa.

Le ricerche di associazione dei nomi utente da UNIX a Windows possono essere eseguite solo su domini con trust bidirezionali tra il dominio principale e l'altro dominio.

- *Fiducia in uscita*

Con un trust in uscita, il dominio principale considera attendibile l'altro dominio. In questo caso, il dominio principale può autenticare e autorizzare un utente appartenente al dominio trusted in uscita.

Un dominio con un trust in uscita con il dominio principale viene *not* ricercato quando si eseguono ricerche di mappatura da utente UNIX a nome utente Windows.

- *Fiducia in entrata*

Con un trust inbound, l'altro dominio considera attendibile il dominio principale del server CIFS. In questo caso, il dominio principale non può autenticare o autorizzare un utente appartenente al dominio trusted in entrata.

Un dominio con un trust in entrata con il dominio principale viene *not* ricercato quando si eseguono ricerche di associazione tra utenti UNIX e nomi utente Windows.

### **Modalità di utilizzo dei caratteri jolly (\*) per configurare le ricerche su più domini per la mappatura dei nomi**

Le ricerche di mappatura dei nomi multidominio sono facilitate dall'utilizzo di caratteri jolly nella sezione dominio del nome utente di Windows. Nella tabella seguente viene illustrato come utilizzare i caratteri jolly nella parte di dominio di una voce di mappatura dei nomi per abilitare le ricerche su più domini:

Schema	Sostituzione	Risultato
root	amministratore	L'utente UNIX "root" viene mappato all'utente "Administrator". Tutti i domini attendibili vengono ricercati in ordine fino a quando non viene trovato il primo utente corrispondente "Administrator".
*	*	<p>Gli utenti UNIX validi vengono mappati ai corrispondenti utenti Windows. Tutti i domini attendibili vengono ricercati in ordine fino a quando non viene trovato il primo utente corrispondente a tale nome.</p> <div>  <p>Il modello è valido solo per la mappatura dei nomi da UNIX a Windows, non viceversa.</p> </div>

### Come vengono eseguite le ricerche di nomi multidominio

È possibile scegliere uno dei due metodi per determinare l'elenco di domini attendibili utilizzati per la ricerca di nomi di più domini:

- Utilizzare l'elenco di attendibilità bidirezionale rilevato automaticamente compilato da ONTAP
- Utilizzare l'elenco di domini attendibili preferito compilato

Se un utente UNIX viene mappato a un utente Windows con un carattere jolly utilizzato per la sezione di dominio del nome utente, l'utente Windows viene ricercato in tutti i domini attendibili nel modo seguente:

- Se viene configurato un elenco di domini attendibili preferito, l'utente Windows mappato viene ricercato solo in questo elenco di ricerca, in ordine.
- Se un elenco preferito di domini attendibili non è configurato, l'utente Windows viene ricercato in tutti i domini attendibili bidirezionali del dominio principale.
- Se non esistono domini trusted bidirezionalmente per il dominio principale, l'utente viene ricercato nel dominio principale.

Se un utente UNIX viene mappato a un utente Windows senza una sezione di dominio nel nome utente, l'utente Windows viene ricercato nel dominio principale.

### Regole di conversione del mapping dei nomi

Un sistema ONTAP mantiene una serie di regole di conversione per ogni SVM. Ogni regola è composta da due parti: Un *pattern* e un *replacement*. Le conversioni iniziano all'inizio dell'elenco appropriato ed eseguono una sostituzione in base alla prima regola di corrispondenza. Il modello è un'espressione regolare in stile UNIX. La sostituzione è una stringa contenente sequenze di escape che rappresentano sottoespressioni del modello,

come in UNIX `sed` programma.

### Creare una mappatura dei nomi

È possibile utilizzare `vserver name-mapping create` per creare una mappatura dei nomi. Si utilizzano le mappature dei nomi per consentire agli utenti Windows di accedere ai volumi di sicurezza UNIX e viceversa.

### A proposito di questa attività

Per ogni SVM, ONTAP supporta fino a 12,500 mappature di nomi per ciascuna direzione.

### Fase

1. Creazione di una mappatura dei nomi: `vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-unix|unix-win} -position integer -pattern text -replacement text`



Il `-pattern` e `-replacement` le dichiarazioni possono essere formulate come espressioni regolari. È inoltre possibile utilizzare `-replacement` per negare esplicitamente un mapping all'utente utilizzando la stringa di sostituzione nulla " " (il carattere dello spazio). Vedere `vserver name-mapping create` pagina man per i dettagli.

Quando vengono create mappature da Windows a UNIX, tutti i client SMB che hanno connessioni aperte al sistema ONTAP al momento della creazione delle nuove mappature devono disconnettersi e riconnettersi per visualizzare le nuove mappature.

### Esempi

Il seguente comando crea un mapping dei nomi sulla SVM denominata `vs1`. Il mapping è un mapping da UNIX a Windows nella posizione 1 nell'elenco delle priorità. Il mapping associa l'utente UNIX `Johnd` all'utente Windows `ENG/JohnDoe`.

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

Il seguente comando crea un'altra mappatura dei nomi sulla SVM denominata `vs1`. Il mapping è un mapping da Windows a UNIX nella posizione 1 nell'elenco delle priorità. Qui il modello e la sostituzione includono espressioni regolari. Il mapping associa ogni utente CIFS nel dominio `ENG` agli utenti nel dominio LDAP associato alla SVM.

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\\1"
```

Il seguente comando crea un'altra mappatura dei nomi sulla SVM denominata `vs1`. Qui il modello include `""` come elemento nel nome utente di Windows che deve essere escapato. La mappatura mappa l'utente Windows `ENG` all'utente UNIX `john_Ops`.

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\${ops}
-replacement john_ops
```

### Configurare l'utente predefinito

È possibile configurare un utente predefinito da utilizzare se tutti gli altri tentativi di mappatura non riescono per un utente o se non si desidera mappare singoli utenti tra UNIX e Windows. In alternativa, se si desidera che l'autenticazione degli utenti non mappati non venga eseguita correttamente, non è necessario configurare un utente predefinito.

### A proposito di questa attività

Per l'autenticazione CIFS, se non si desidera associare ciascun utente Windows a un singolo utente UNIX, è possibile specificare un utente UNIX predefinito.

Per l'autenticazione NFS, se non si desidera associare ciascun utente UNIX a un singolo utente Windows, è possibile specificare un utente Windows predefinito.

### Fasi


1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il seguente comando...
Configurare l'utente UNIX predefinito	<code>vserver cifs options modify -default -unix-user <i>user_name</i></code>
Configurare l'utente Windows predefinito	<code>vserver nfs modify -default-win-user <i>user_name</i></code>

### Comandi per la gestione delle mappature dei nomi

Esistono comandi ONTAP specifici per la gestione delle mappature dei nomi.

Se si desidera...	Utilizzare questo comando...
Creare una mappatura dei nomi	<code>vserver name-mapping create</code>
Inserire una mappatura dei nomi in una posizione specifica	<code>vserver name-mapping insert</code>
Visualizza mappature dei nomi	<code>vserver name-mapping show</code>

Se si desidera...	Utilizzare questo comando...
 <p>Lo swap non è consentito quando la mappatura dei nomi è configurata con una voce di qualificatore ip.</p>	<code>vserver name-mapping swap</code>
Modificare una mappatura dei nomi	<code>vserver name-mapping modify</code>
Eliminare una mappatura dei nomi	<code>vserver name-mapping delete</code>
Convalidare la corretta mappatura dei nomi	<code>vserver security file-directory show-effective-permissions -vserver vs1 -win -user-name user1 -path / -share-name sh1</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Configurare le ricerche di mappatura dei nomi di più domini

### Attivare o disattivare le ricerche di mappatura dei nomi multidominio

Con le ricerche di mappatura dei nomi di più domini, è possibile utilizzare un carattere jolly (**) nella parte di dominio di un nome Windows quando si configura l'associazione di utenti UNIX con nomi utente Windows. L'utilizzo di un wild card (**) nella parte di dominio del nome consente a ONTAP di cercare tutti i domini con un trust bidirezionale con il dominio che contiene l'account del computer del server CIFS.

### A proposito di questa attività

In alternativa alla ricerca di tutti i domini con attendenza bidirezionale, è possibile configurare un elenco di domini attendibili preferiti. Quando viene configurato un elenco di domini trusted preferiti, ONTAP utilizza l'elenco di domini trusted preferito invece dei domini trusted bidirezionalmente rilevati per eseguire ricerche di mappatura dei nomi a più domini.

- Per impostazione predefinita, le ricerche di mappatura dei nomi multidominio sono attivate.
- Questa opzione è disponibile al livello di privilegio avanzato.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:



Se si desidera che le ricerche di mappatura dei nomi di più domini siano...	Immettere il comando...
Attivato	<code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false</code>

3. Tornare al livello di privilegio admin: `set -privilege admin`

#### Informazioni correlate

[Opzioni server SMB disponibili](#)

#### Reimpostare e riscoprire i domini attendibili

È possibile forzare la riscoperta di tutti i domini attendibili. Ciò può risultare utile quando i server di dominio attendibili non rispondono in modo appropriato o le relazioni di trust sono cambiate. Vengono rilevati solo i domini con un trust bidirezionale con il dominio principale, ovvero il dominio contenente l'account del computer del server CIFS.

#### Fase

1. Reimpostare e riscoprire i domini attendibili utilizzando `vserver cifs domain trusts rediscover` comando.

```
vserver cifs domain trusts rediscover -vserver vs1
```

#### Informazioni correlate

[Visualizzazione delle informazioni sui domini attendibili rilevati](#)

#### Visualizza informazioni sui domini attendibili rilevati

È possibile visualizzare informazioni sui domini attendibili rilevati per il dominio principale del server CIFS, ovvero il dominio contenente l'account del computer del server CIFS. Ciò può essere utile quando si desidera sapere quali domini attendibili vengono rilevati e come vengono ordinati all'interno dell'elenco di domini attendibili rilevati.

#### A proposito di questa attività

Vengono rilevati solo i domini con trust bidirezionali con il dominio principale. Poiché il domain controller (DC) del dominio principale restituisce l'elenco dei domini attendibili in un ordine determinato dal controller di dominio, non è possibile prevedere l'ordine dei domini all'interno dell'elenco. Visualizzando l'elenco dei domini attendibili, è possibile determinare l'ordine di ricerca per le ricerche di mappatura dei nomi multidominio.

Le informazioni di dominio attendibile visualizzate sono raggruppate per nodo e SVM (Storage Virtual Machine).

#### Fase

1. Visualizzare le informazioni sui domini attendibili rilevati utilizzando `vserver cifs domain trusts show` comando.

```
vserver cifs domain trusts show -vserver vs1
```

```
Node: node1
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM

Node: node2
Vserver: vs1

Home Domain          Trusted Domain
-----
EXAMPLE.COM          CIFS1.EXAMPLE.COM,
                     CIFS2.EXAMPLE.COM
                     EXAMPLE.COM
```

## Informazioni correlate

[Reimpostazione e riscoperta di domini attendibili](#)

**Aggiungere, rimuovere o sostituire i domini attendibili negli elenchi di domini attendibili preferiti**

È possibile aggiungere o rimuovere domini attendibili dall'elenco dei domini attendibili preferiti per il server SMB oppure modificare l'elenco corrente. Se si configura un elenco di domini trusted preferito, questo elenco viene utilizzato al posto dei domini trusted bidirezionali rilevati durante le ricerche di mappatura dei nomi di più domini.

### A proposito di questa attività

- Se si aggiungono domini attendibili a un elenco esistente, il nuovo elenco viene Unitto all'elenco esistente con le nuove voci alla fine I domini attendibili vengono ricercati nell'ordine in cui vengono visualizzati nell'elenco dei domini attendibili.
- Se si rimuovono domini attendibili dall'elenco esistente e non si specifica un elenco, l'intero elenco di domini attendibili per la macchina virtuale di storage (SVM) specificata viene rimosso.
- Se si modifica l'elenco esistente di domini attendibili, il nuovo elenco sovrascrive quello esistente.



Nell'elenco Preferred trusted domain (dominio trusted preferito), inserire solo domini trusted bidirezionalmente attendibili. Anche se è possibile inserire domini trust in uscita o in entrata nell'elenco dei domini preferiti, questi non vengono utilizzati durante le ricerche di mappatura dei nomi di più domini. ONTAP ignora la voce relativa al dominio unidirezionale e passa al successivo dominio attendibile bidirezionale nell'elenco.

## Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera eseguire le seguenti operazioni con l'elenco dei domini attendibili preferiti...	Utilizzare il comando...
Aggiungere domini attendibili all'elenco	<code>vserver cifs domain name-mapping-search add -vserver _vserver_name_-trusted-domains FQDN, ...</code>
Rimuovere i domini attendibili dall'elenco	<code>vserver cifs domain name-mapping-search remove -vserver _vserver_name_-trusted-domains FQDN, ...]</code>
Modificare l'elenco esistente	<code>vserver cifs domain name-mapping-search modify -vserver _vserver_name_-trusted-domains FQDN, ...</code>

## Esempi

Il seguente comando aggiunge due domini attendibili (cifs1.example.com e cifs2.example.com) all'elenco di domini attendibili preferito utilizzato da SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Il seguente comando rimuove due domini attendibili dall'elenco utilizzato da SVM vs1:

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

Il seguente comando modifica l'elenco di domini attendibili utilizzato da SVM vs1. Il nuovo elenco sostituisce quello originale:

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

## Informazioni correlate

[Visualizzazione delle informazioni sull'elenco di domini attendibili preferiti](#)

**Visualizzare le informazioni relative all'elenco di domini attendibili preferiti**

È possibile visualizzare le informazioni sui domini attendibili presenti nell'elenco dei domini attendibili preferiti e l'ordine in cui vengono ricercati se sono attivate le ricerche di mappatura dei nomi multidominio. È possibile configurare un elenco di domini attendibili

preferito in alternativa all'elenco di domini attendibili rilevati automaticamente.

## Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su...	Utilizzare il comando...
Tutti i domini trusted preferiti nel cluster raggruppati per SVM (Storage Virtual Machine)	<code>vserver cifs domain name-mapping-search show</code>
Tutti i domini trusted preferiti per una SVM specificata	<code>vserver cifs domain name-mapping-search show -vserver <i>vserver_name</i></code>

Il seguente comando visualizza informazioni su tutti i domini attendibili preferiti nel cluster:

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
-----
vs1              CIFS1.EXAMPLE.COM
```

## Informazioni correlate

[Aggiunta, rimozione o sostituzione di domini attendibili in elenchi di domini attendibili preferiti](#)

## Creare e configurare le condivisioni SMB

### Panoramica sulla creazione e la configurazione delle condivisioni SMB

Prima che utenti e applicazioni possano accedere ai dati sul server CIFS tramite SMB, è necessario creare e configurare le condivisioni SMB, che è un access point denominato in un volume. È possibile personalizzare le condivisioni specificando i parametri di condivisione e le proprietà di condivisione. È possibile modificare una condivisione esistente in qualsiasi momento.

Quando si crea una condivisione SMB, ONTAP crea un ACL predefinito per la condivisione con autorizzazioni di controllo completo per tutti.

Le condivisioni SMB sono legate al server CIFS sulla macchina virtuale di storage (SVM). Le condivisioni SMB vengono eliminate se la SVM viene eliminata o se il server CIFS a cui è associata viene cancellato dalla SVM. Se si ricrea il server CIFS su SVM, è necessario ricreare le condivisioni SMB.

## Informazioni correlate

[Gestire l'accesso ai file utilizzando SMB](#)

["Configurazione SMB per Microsoft Hyper-V e SQL Server"](#)

[Configurare la mappatura dei caratteri per la conversione dei nomi file SMB sui volumi](#)

## Quali sono le condivisioni amministrative predefinite

Quando si crea un server CIFS sulla macchina virtuale di storage (SVM), vengono create automaticamente le condivisioni amministrative predefinite. È necessario comprendere quali sono le condivisioni predefinite e come vengono utilizzate.

Quando si crea il server CIFS, ONTAP crea le seguenti condivisioni amministrative predefinite:



A partire da ONTAP 9.8, la condivisione in dollari di amministrazione non viene più creata per impostazione predefinita.

- ipc
- admin (solo ONTAP 9.7 e versioni precedenti)
- €

Poiché le condivisioni che terminano con il carattere € sono condivisioni nascoste, le condivisioni amministrative predefinite non sono visibili da risorse del computer, ma è possibile visualizzarle utilizzando le cartelle condivise.

## Come vengono utilizzate le condivisioni predefinite ipc e admin

Le condivisioni ipc e admin vengono utilizzate da ONTAP e non possono essere utilizzate dagli amministratori Windows per accedere ai dati che risiedono sulla SVM.

- condivisione ipc

La condivisione ipc è una risorsa che condivide le named pipe che sono essenziali per la comunicazione tra i programmi. La condivisione ipc viene utilizzata durante l'amministrazione remota di un computer e durante la visualizzazione delle risorse condivise di un computer. Non è possibile modificare le impostazioni di condivisione, le proprietà di condivisione o gli ACL della condivisione ipc. Inoltre, non è possibile rinominare o eliminare la condivisione ipc.

- Quota amministrativa (solo ONTAP 9.7 e versioni precedenti)



A partire da ONTAP 9.8, la condivisione in dollari di amministrazione non viene più creata per impostazione predefinita.

La condivisione admin viene utilizzata durante l'amministrazione remota di SVM. Il percorso di questa risorsa è sempre il percorso verso la radice SVM. Non è possibile modificare le impostazioni di condivisione, le proprietà di condivisione o gli ACL per la condivisione admin. Inoltre, non è possibile rinominare o eliminare la condivisione admin.

## Modalità di utilizzo della condivisione predefinita

La condivisione è una condivisione amministrativa che il cluster o l'amministratore SVM può utilizzare per accedere e gestire il volume root SVM.

Di seguito sono riportate le caratteristiche della quota:

- Il percorso per questa condivisione è sempre il percorso del volume root SVM e non può essere modificato.

- L'ACL predefinito per la condivisione è Amministratore/controllo completo.

Questo utente è il BUILTIN/amministratore. Per impostazione predefinita, il BUILTIN/amministratore può eseguire il mapping alla condivisione e visualizzare, creare, modificare o eliminare file e cartelle nella directory principale mappata. Prestare attenzione durante la gestione di file e cartelle in questa directory.

- È possibile modificare l'ACL della condivisione.
- È possibile modificare le impostazioni di condivisione e le proprietà di condivisione.
- Non è possibile eliminare la condivisione.
- L'amministratore di SVM può accedere al resto dello spazio dei nomi SVM dalla condivisione mappata incrociando le giunzioni dello spazio dei nomi.
- È possibile accedere alla condivisione utilizzando Microsoft Management Console.

## Informazioni correlate

[Configurazione delle autorizzazioni avanzate per i file NTFS mediante la scheda protezione di Windows](#)

## Requisiti di naming delle condivisioni SMB

Quando si creano condivisioni SMB sul server SMB, è necessario tenere presenti i requisiti di denominazione delle condivisioni ONTAP.

Le convenzioni di denominazione delle condivisioni per ONTAP sono le stesse di Windows e includono i seguenti requisiti:

- Il nome di ciascuna condivisione deve essere univoco per il server SMB.
- I nomi delle condivisioni non rilevano la distinzione tra maiuscole e minuscole.
- La lunghezza massima del nome di condivisione è di 80 caratteri.
- I nomi di condivisione Unicode sono supportati.
- I nomi delle condivisioni che terminano con il carattere € sono condivisioni nascoste.
- Per ONTAP 9.7 e versioni precedenti, le condivisioni amministrative admin, ipc e c vengono create automaticamente su ogni server CIFS e sono nomi di condivisione riservati. A partire da ONTAP 9.8, la condivisione admin non viene più creata automaticamente.
- Non è possibile utilizzare il nome di condivisione ONTAP\_ADMIN quando si crea una condivisione.
- Sono supportati i nomi di condivisione contenenti spazi:
  - Non è possibile utilizzare uno spazio come primo carattere o come ultimo carattere di un nome di condivisione.
  - È necessario racchiudere i nomi delle condivisioni contenenti uno spazio tra virgolette.



Le virgolette singole sono considerate parte del nome della condivisione e non possono essere utilizzate al posto delle virgolette.

- I seguenti caratteri speciali sono supportati quando si assegnano le condivisioni SMB:

! @ % E ' \_ - . ~ ( ) { }

- I seguenti caratteri speciali non sono supportati quando si assegnano nomi SMB share:

◦ " / " ; | < > , ? \* =

## Requisiti di distinzione tra maiuscole e minuscole per la creazione di condivisioni in un ambiente multiprotocollo

Se si creano condivisioni in una SVM in cui viene utilizzato lo schema di denominazione 8.3 per distinguere tra nomi di directory in cui esistono solo differenze di maiuscole e minuscole tra i nomi, è necessario utilizzare il nome 8.3 nel percorso di condivisione per garantire che il client si connetta al percorso di directory desiderato.

Nell'esempio seguente, due directory denominate "testdir" e "TESTDIR" sono state create su un client Linux. Il percorso di giunzione del volume contenente le directory è /home. Il primo output proviene da un client Linux e il secondo da un client SMB.

```
ls -l
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1 4096 Apr 17 11:24 TESTDIR
```

```
dir

Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

Quando si crea una condivisione nella seconda directory, è necessario utilizzare il nome 8.3 nel percorso di condivisione. In questo esempio, il percorso di condivisione per la prima directory è /home/testdir il percorso di condivisione per la seconda directory è /home/TESTDI~1.

### Utilizzare le proprietà di condivisione SMB

#### Utilizza la panoramica delle proprietà di condivisione SMB

È possibile personalizzare le proprietà delle condivisioni SMB.

Le proprietà di condivisione disponibili sono le seguenti:

Condividere le proprietà	Descrizione
oplocks	Questa proprietà specifica che la condivisione utilizza blocchi opportunistici, noti anche come caching lato client.
browsable	Questa proprietà consente ai client Windows di esplorare la condivisione.
showsnapshot	Questa proprietà specifica che le copie Snapshot possono essere visualizzate e attraversate dai client.

Condividere le proprietà	Descrizione
changenotify	Questa proprietà specifica che la condivisione supporta le richieste di notifica delle modifiche. Per le condivisioni su una SVM, si tratta di una proprietà iniziale predefinita.
attributecache	Questa proprietà abilita il caching degli attributi del file nella condivisione SMB per fornire un accesso più rapido agli attributi. L'impostazione predefinita prevede la disattivazione del caching degli attributi. Questa proprietà deve essere attivata solo se ci sono client che si connettono alle condivisioni su SMB 1.0. Questa proprietà di condivisione non è applicabile se i client si connettono alle condivisioni tramite SMB 2.x o SMB 3.0.
continuously-available	Questa proprietà consente ai client SMB che lo supportano di aprire i file in modo persistente. I file aperti in questo modo sono protetti da eventi di interruzione, come failover e giveback.
branchcache	Questa proprietà specifica che la condivisione consente ai client di richiedere gli hash BranchCache sui file all'interno di questa condivisione. Questa opzione è utile solo se si specifica "per-share" come modalità operativa nella configurazione CIFS BranchCache.
access-based-enumeration	Questa proprietà specifica che l'opzione <i>Access Based Enumeration</i> (ABE) è attivata per questa condivisione. Le cartelle condivise con filtro ABE sono visibili a un utente in base ai diritti di accesso del singolo utente, impedendo la visualizzazione di cartelle o altre risorse condivise a cui l'utente non dispone dei diritti di accesso.
namespace-caching	Questa proprietà specifica che i client SMB che si connettono a questa condivisione possono memorizzare nella cache i risultati dell'enumerazione delle directory restituiti dai server CIFS, in modo da ottenere performance migliori. Per impostazione predefinita, i client SMB 1 non memorizzano nella cache i risultati dell'enumerazione delle directory. Poiché i client SMB 2 e SMB 3 memorizzano nella cache i risultati dell'enumerazione delle directory per impostazione predefinita, la specifica di questa proprietà di condivisione offre vantaggi in termini di prestazioni solo per le connessioni client SMB 1.



Condividere le proprietà	Descrizione
encrypt-data	Questa proprietà specifica che la crittografia SMB deve essere utilizzata quando si accede a questa condivisione. I client SMB che non supportano la crittografia durante l'accesso ai dati SMB non potranno accedere a questa condivisione.

### Aggiungere o rimuovere le proprietà di condivisione su una condivisione SMB esistente

È possibile personalizzare una condivisione SMB esistente aggiungendo o rimuovendo le proprietà della condivisione. Questo può essere utile se si desidera modificare la configurazione della condivisione per soddisfare i requisiti in continuo cambiamento nell'ambiente.

#### Prima di iniziare

La condivisione di cui si desidera modificare le proprietà deve esistere.

#### A proposito di questa attività

Linee guida per l'aggiunta di proprietà di condivisione:

- È possibile aggiungere una o più proprietà di condivisione utilizzando un elenco delimitato da virgole.
- Tutte le proprietà di condivisione precedentemente specificate rimangono attive.

Le nuove proprietà aggiunte vengono aggiunte all'elenco esistente di proprietà di condivisione.

- Se si specifica un nuovo valore per le proprietà di condivisione già applicate alla condivisione, il nuovo valore specificato sostituisce il valore originale.
- Non è possibile rimuovere le proprietà di condivisione utilizzando `vserver cifs share properties add` comando.

È possibile utilizzare `vserver cifs share properties remove` comando per rimuovere le proprietà di condivisione.

Linee guida per la rimozione delle proprietà di condivisione:

- È possibile rimuovere una o più proprietà di condivisione utilizzando un elenco delimitato da virgole.
- Tutte le proprietà di condivisione precedentemente specificate ma non rimosse rimangono attive.

#### Fasi

1. Immettere il comando appropriato:

Se si desidera...	Immettere il comando...
Aggiungere proprietà di condivisione	<pre>vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</pre>

Se si desidera...	Immettere il comando...
Rimuovere le proprietà di condivisione	<code>vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...</code>

2. Verificare le impostazioni della proprietà di condivisione: `vserver cifs share show -vserver vserver_name -share-name share_name`

## Esempi

Il seguente comando aggiunge `showsnapshot` Condividere la proprietà con una condivisione denominata “share1” su SVM vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver      Share    Path      Properties    Comment    ACL
-----
vs1          share1   /share1   oplocks       -          Everyone / Full
Control
                                browsable
                                changenotify
                                showsnapshot
```

Il seguente comando rimuove `browsable` Condividere la proprietà da una condivisione denominata “share2” su SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver      Share    Path      Properties    Comment    ACL
-----
vs1          share2   /share2   oplocks       -          Everyone / Full
Control
                                changenotify
```

## Informazioni correlate

[Comandi per la gestione delle condivisioni SMB](#)

**Ottimizza l'accesso degli utenti SMB con l'impostazione di `force-group share`**

Quando si crea una condivisione dalla riga di comando di ONTAP ai dati con protezione

effettiva UNIX, è possibile specificare che tutti i file creati dagli utenti SMB in tale condivisione appartengano allo stesso gruppo, noto come *force-group*, che deve essere un gruppo predefinito nel database dei gruppi UNIX. L'utilizzo di un gruppo di forze semplifica l'accesso ai file da parte degli utenti SMB appartenenti a diversi gruppi.

Specificare un gruppo di forze è significativo solo se la condivisione si trova in un qtree UNIX o misto. Non è necessario impostare un gruppo di forza per le condivisioni in un volume o qtree NTFS, in quanto l'accesso ai file in queste condivisioni è determinato dalle autorizzazioni di Windows, non dai GID UNIX.

Se è stato specificato un gruppo di forze per una condivisione, si verifica quanto segue:

- Gli utenti SMB nel gruppo di forza che accedono a questa condivisione vengono temporaneamente modificati in GID del gruppo di forze.

Questo GID consente loro di accedere ai file in questa condivisione che non sono normalmente accessibili con il GID o UID primario.

- Tutti i file in questa condivisione creati dagli utenti SMB appartengono allo stesso gruppo di forze, indipendentemente dal GID primario del proprietario del file.

Quando gli utenti SMB tentano di accedere a un file creato da NFS, i GID primari degli utenti SMB determinano i diritti di accesso.

Il *force-group* non influisce sul modo in cui gli utenti NFS accedono ai file in questa condivisione. Un file creato da NFS acquisisce il GID dal proprietario del file. La determinazione delle autorizzazioni di accesso si basa sull'UID e sul GID primario dell'utente NFS che sta tentando di accedere al file.

L'utilizzo di un gruppo di forze semplifica l'accesso ai file da parte degli utenti SMB appartenenti a diversi gruppi. Ad esempio, se si desidera creare una condivisione per memorizzare le pagine Web dell'azienda e concedere l'accesso in scrittura agli utenti dei reparti Engineering e Marketing, è possibile creare una condivisione e assegnare l'accesso in scrittura a un gruppo di forze denominato "webgroup1". A causa del gruppo di forza, tutti i file creati dagli utenti SMB in questa condivisione sono di proprietà del gruppo "webgroup1". Inoltre, agli utenti viene assegnato automaticamente il GID del gruppo "webgroup1" quando accedono alla condivisione. Di conseguenza, tutti gli utenti possono scrivere su questa condivisione senza dover gestire i diritti di accesso degli utenti nei reparti Engineering e Marketing.

## Informazioni correlate

[Creazione di una condivisione SMB con l'impostazione \*force-group share\*](#)

### Creare una condivisione SMB con l'impostazione di *force-group share*

È possibile creare una condivisione SMB con l'impostazione *force-group share* se si desidera che gli utenti SMB che accedono ai dati su volumi o qtree con sicurezza dei file UNIX siano considerati da ONTAP come appartenenti allo stesso gruppo UNIX.

## Fase

1. Creare la condivisione SMB: `vserver cifs share create -vserver vserver_name -share -name share_name -path path -force-group-for-create UNIX_group_name`

Se il percorso UNC (\\servername\sharename\filepath) della condivisione contiene più di 256 caratteri (escluso il " iniziale\\ " Nel percorso UNC), la scheda **Security** nella casella Proprietà di Windows non è disponibile. Si tratta di un problema del client Windows piuttosto che di un problema ONTAP. Per evitare questo problema, non creare condivisioni con percorsi UNC con più di 256 caratteri.

Se si desidera rimuovere il gruppo di forza dopo la creazione della condivisione, è possibile modificare la condivisione in qualsiasi momento e specificare una stringa vuota ("") come valore per `-force-group` `-for-create` parametro. Se si rimuove il gruppo di forza modificando la condivisione, tutte le connessioni esistenti a questa condivisione continueranno a avere il gruppo di forza precedentemente impostato come GID primario.

## Esempio

Il seguente comando crea una condivisione “webpages” accessibile sul Web in `/corp/companyinfo` Directory in cui tutti i file creati dagli utenti SMB sono assegnati al gruppo `webgroup1`:

```
vserver cifs share create -vserver vs1 -share-name webpages -path  
/corp/companyinfo -force-group-for-create webgroup1
```

## Informazioni correlate

[Ottimizza l'accesso degli utenti SMB con l'impostazione di `force-group share`](#)

### Visualizzare le informazioni sulle condivisioni SMB utilizzando MMC

È possibile visualizzare informazioni sulle condivisioni SMB sulla SVM ed eseguire alcune attività di gestione utilizzando Microsoft Management Console (MMC). Prima di poter visualizzare le condivisioni, è necessario collegare MMC a SVM.

#### A proposito di questa attività

È possibile eseguire le seguenti attività sulle condivisioni contenute in SVM utilizzando MMC:

- Visualizza condivisioni
- Visualizzare le sessioni attive
- Visualizzare i file aperti
- Enumerare l'elenco di sessioni, file e connessioni ad albero nel sistema
- Chiudere i file aperti nel sistema
- Chiudere le sessioni aperte
- Creare/gestire le condivisioni



Le viste visualizzate dalle funzionalità precedenti sono specifiche del nodo e non del cluster. Pertanto, quando si utilizza MMC per connettersi al nome host del server SMB (cioè, `cifs01.domain.local`), si viene indirizzati, in base alla configurazione del DNS, a una singola LIF all'interno del cluster.

Le seguenti funzioni non sono supportate in MMC per ONTAP:

- Creazione di nuovi utenti/gruppi locali
- Gestione/visualizzazione di utenti/gruppi locali esistenti
- Visualizzazione di eventi o log delle performance
- Storage
- Servizi e applicazioni

Nei casi in cui l'operazione non è supportata, potrebbe verificarsi un'operazione `remote procedure call`

failed errori.

## "Domande frequenti: Utilizzo di Windows MMC con ONTAP"

### Fasi

1. Per aprire la MMC Gestione computer su qualsiasi server Windows, nel pannello di controllo, selezionare **Strumenti di amministrazione > Gestione computer**.
2. Selezionare **azione > connessione a un altro computer**.

Viene visualizzata la finestra di dialogo Select computer (Seleziona computer).

3. Digitare il nome del sistema di storage o fare clic su **Browse** (Sfoglia) per individuare il sistema di storage.
4. Fare clic su **OK**.

MMC si connette a SVM.

5. Nel riquadro di navigazione, fare clic su **Shared Folders > Shares**.

Nel riquadro di visualizzazione di destra viene visualizzato un elenco di condivisioni su SVM.

6. Per visualizzare le proprietà di una condivisione, fare doppio clic sulla condivisione per aprire la finestra di dialogo **Proprietà**.
7. Se non è possibile connettersi al sistema di storage utilizzando MMC, è possibile aggiungere l'utente al gruppo BUILTIN/Administrators o al gruppo BUILTIN/Power Users utilizzando uno dei seguenti comandi sul sistema di storage:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>  
-group-name BUILTIN\Administrators -member-names <domainuser>
```

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>  
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

### Comandi per la gestione delle condivisioni SMB

Si utilizza `vserver cifs share` e `vserver cifs share properties` Comandi per gestire le condivisioni SMB.

Se si desidera...	Utilizzare questo comando...
Creare una condivisione SMB	<code>vserver cifs share create</code>
Visualizzare le condivisioni SMB	<code>vserver cifs share show</code>
Modificare una condivisione SMB	<code>vserver cifs share modify</code>
Eliminare una condivisione SMB	<code>vserver cifs share delete</code>

Se si desidera...	Utilizzare questo comando...
Aggiungere le proprietà di condivisione a una condivisione esistente	<code>vserver cifs share properties add</code>
Rimuovere le proprietà di condivisione da una condivisione esistente	<code>vserver cifs share properties remove</code>
Visualizza le informazioni sulle proprietà di condivisione	<code>vserver cifs share properties show</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Accesso sicuro ai file utilizzando gli ACL di condivisione SMB

### Linee guida per la gestione degli ACL a livello di condivisione SMB

È possibile modificare gli ACL a livello di condivisione per offrire agli utenti più o meno diritti di accesso alla condivisione. È possibile configurare ACL a livello di condivisione utilizzando utenti e gruppi Windows o utenti e gruppi UNIX.

Dopo aver creato una condivisione, per impostazione predefinita, l'ACL a livello di condivisione fornisce l'accesso in lettura al gruppo standard denominato Everyone. L'accesso in lettura nell'ACL significa che tutti gli utenti del dominio e tutti i domini attendibili hanno accesso in sola lettura alla condivisione.

È possibile modificare un ACL a livello di condivisione utilizzando la console di gestione Microsoft su un client Windows o la riga di comando di ONTAP.

Quando si utilizza MMC, si applicano le seguenti linee guida:

- I nomi utente e gruppo specificati devono essere nomi Windows.
- È possibile specificare solo le autorizzazioni di Windows.

Quando si utilizza la riga di comando ONTAP, si applicano le seguenti linee guida:

- I nomi utente e gruppo specificati possono essere nomi Windows o UNIX.

Se durante la creazione o la modifica degli ACL non viene specificato un tipo di utente e gruppo, il tipo predefinito è utenti e gruppi Windows.

- È possibile specificare solo le autorizzazioni di Windows.

### Creare elenchi di controllo degli accessi di condivisione SMB

La configurazione delle autorizzazioni di condivisione mediante la creazione di elenchi di controllo degli accessi (ACL) per le condivisioni SMB consente di controllare il livello di accesso a una condivisione per utenti e gruppi.

#### A proposito di questa attività

È possibile configurare gli ACL a livello di condivisione utilizzando nomi di utenti o gruppi Windows locali o di dominio o nomi di utenti o gruppi UNIX.

Prima di creare un nuovo ACL, è necessario eliminare l'ACL di condivisione predefinito `Everyone / Full Control`, che comporta un rischio per la sicurezza.

In modalità workgroup, il nome di dominio locale è il nome del server SMB.

**Fasi**

- 1. Eliminare l'ACL della condivisione predefinita: ``vserver cifs share access control delete -vserver vserver_name -share share_name -user-or-group everyone``
- 2. Configurare il nuovo ACL:

Se si desidera configurare gli ACL utilizzando un...	Immettere il comando...
Utente Windows	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\user_name -permission access_right</code>
Gruppo di Windows	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\group_name -permission access_right</code>
Utente UNIX	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-user -user-or-group UNIX_user_name -permission access_right</code>
Gruppo UNIX	<code>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type unix-group -user-or-group UNIX_group_name -permission access_right</code>

- 3. Verificare che l'ACL applicato alla condivisione sia corretto utilizzando `vserver cifs share access-control show` comando.

**Esempio**

Il seguente comando fornisce `Change Permessi` al gruppo Windows "Sales Team" per la condivisione "sales" su `"vs1.example.com`"SVM:`

```
cluster1::> vsserver cifs share access-control create -vsserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vsserver cifs share access-control show -vsserver
vs1.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs1.example.com	sales	DOMAIN\Sales Team	windows	Change

Il seguente comando fornisce Read Autorizzazione al gruppo UNIX “engineering” per la condivisione “eng” su “vs2.example.com” SVM:

```
cluster1::> vsserver cifs share access-control create -vsserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vsserver cifs share access-control show -vsserver
vs2.example.com
```

Vserver	Share Name	User/Group Name	User/Group Type	Access Permission
vs2.example.com	c\$	BUILTIN\Administrators	windows	Full_Control
vs2.example.com	eng	engineering	unix-group	Read

I seguenti comandi impartire Change Autorizzazione al gruppo Windows locale denominato “Tiger Team” e. Full\_Control Autorizzazione all’utente Windows locale “Sue Chang” per la condivisione “datavol5” su “vs1” SVM:



```

cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vsriver cifs share access-control create -vsriver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vsriver cifs share access-control show -vsriver vs1

```

Vsriver	Share Name	User/Group Name	User/Group Type	Access Permission
vs1	c\$	BUILTIN\Administrators	windows	Full_Control
vs1	datavol5	Tiger Team	windows	Change
vs1	datavol5	Sue Chang	windows	Full_Control

#### Comandi per la gestione degli elenchi di controllo degli accessi di condivisione SMB

È necessario conoscere i comandi per la gestione degli ACL (Access Control List) SMB, che includono la creazione, la visualizzazione, la modifica e l'eliminazione di tali elenchi.

Se si desidera...	Utilizzare questo comando...
Creare un nuovo ACL	<code>vsriver cifs share access-control create</code>
Visualizza ACL	<code>vsriver cifs share access-control show</code>
Modificare un ACL	<code>vsriver cifs share access-control modify</code>
Eliminare un ACL	<code>vsriver cifs share access-control delete</code>

#### Proteggere l'accesso ai file utilizzando i permessi

Configurare le autorizzazioni avanzate per i file NTFS utilizzando la scheda protezione di Windows

È possibile configurare le autorizzazioni standard per i file NTFS su file e cartelle utilizzando la scheda **Windows Security** nella finestra Proprietà di Windows.

#### Prima di iniziare

L'amministratore che esegue questa attività deve disporre di autorizzazioni NTFS sufficienti per modificare le

autorizzazioni sugli oggetti selezionati.

### A proposito di questa attività

La configurazione delle autorizzazioni dei file NTFS viene eseguita su un host Windows aggiungendo voci agli elenchi di controllo degli accessi discrezionali (DACL) NTFS associati a un descrittore di protezione NTFS. Il descrittore di protezione viene quindi applicato ai file e alle directory NTFS. Queste attività vengono gestite automaticamente dalla GUI di Windows.

### Fasi

1. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
2. Completare la finestra di dialogo **Map Network Drive** (Connetti unità di rete):
  - a. Selezionare una lettera **Drive**.
  - b. Nella casella **Folder**, digitare il nome del server CIFS contenente la condivisione contenente i dati a cui si desidera applicare le autorizzazioni e il nome della condivisione.

Se il nome del server CIFS è "CIFS\_SERVER" e la condivisione è denominata "share1", digitare \\CIFS\_SERVER\share1.



È possibile specificare l'indirizzo IP dell'interfaccia dati per il server CIFS invece del nome del server CIFS.

- c. Fare clic su **fine**.

Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

3. Selezionare il file o la directory per cui si desidera impostare le autorizzazioni per il file NTFS.
4. Fare clic con il pulsante destro del mouse sul file o sulla directory, quindi selezionare **Proprietà**.
5. Selezionare la scheda **sicurezza**.

La scheda **Security** visualizza l'elenco di utenti e gruppi per i quali è impostata l'autorizzazione NTFS. La casella **Permissions for** (autorizzazioni per) visualizza un elenco delle autorizzazioni Allow e Nega in vigore per ogni utente o gruppo selezionato.

6. Fare clic su **Avanzate**.

La finestra Proprietà di Windows visualizza informazioni sulle autorizzazioni file esistenti assegnate a utenti e gruppi.

7. Fare clic su **Modifica permessi**.

Viene visualizzata la finestra Permissions (autorizzazioni).

8. Eseguire le azioni desiderate:

Se si desidera...	Effettuare le seguenti operazioni...
Impostare autorizzazioni NTFS avanzate per un nuovo utente o gruppo	a. Fare clic su <b>Aggiungi</b> . b. Nella casella <b>inserire il nome dell'oggetto da selezionare</b> , digitare il nome dell'utente o del gruppo che si desidera aggiungere. c. Fare clic su <b>OK</b> .
Modificare le autorizzazioni NTFS avanzate da un utente o da un gruppo	a. Nella casella <b>Permissions entries:</b> , selezionare l'utente o il gruppo di cui si desidera modificare le autorizzazioni avanzate. b. Fare clic su <b>Edit</b> (Modifica).
Rimuovere le autorizzazioni NTFS avanzate per un utente o un gruppo	a. Nella casella <b>Permissions entries:</b> , selezionare l'utente o il gruppo che si desidera rimuovere. b. Fare clic su <b>Rimuovi</b> . c. Passare alla fase 13.

Se si aggiungono autorizzazioni NTFS avanzate a un nuovo utente o gruppo o si modificano le autorizzazioni avanzate NTFS per un utente o un gruppo esistente, viene visualizzata la finestra immissione autorizzazioni per <Object>.

9. Nella casella **Apply to** (Applica a), selezionare la modalità di applicazione della voce di autorizzazione del file NTFS.

Se si impostano le autorizzazioni per un file NTFS su un singolo file, la casella **Apply to** (Applica a) non è attiva. L'impostazione predefinita di **Apply to** (Applica a) è **solo questo oggetto**.

10. Nella casella **Permissions** (autorizzazioni), selezionare le caselle **Allow** (Consenti) o **Nega** per le autorizzazioni avanzate che si desidera impostare su questo oggetto.

- Per consentire l'accesso specificato, selezionare la casella **allow**.
- Per non consentire l'accesso specificato, selezionare la casella **Nega**. È possibile impostare le autorizzazioni per i seguenti diritti avanzati:

- **Controllo completo**

Se si sceglie questo diritto avanzato, tutti gli altri diritti avanzati vengono scelti automaticamente (diritti Allow o Nega).

- **Cartella Traverse / file di esecuzione**
- **Elenca cartella / leggi dati**
- **Attributi di lettura**
- **Leggi attributi estesi**
- **Creare file / scrivere dati**
- **Crea cartelle/Aggiungi dati**
- **Attributi di scrittura**

- **Scrivi attributi estesi**
- **Elimina sottocartelle e file**
- **Elimina**
- **Permessi di lettura**
- **Modifica delle autorizzazioni**
- **Assumere la proprietà**



Se una delle caselle di autorizzazione avanzate non è selezionabile, le autorizzazioni vengono ereditate dall'oggetto padre.

- Se si desidera che le sottocartelle e i file di questo oggetto ereditino queste autorizzazioni, selezionare la casella **Applica queste autorizzazioni solo agli oggetti e/o ai contenitori all'interno di questo contenitore**.
- Fare clic su **OK**.
- Dopo aver aggiunto, rimosso o modificato le autorizzazioni NTFS, specificare l'impostazione di ereditarietà per questo oggetto:

- Selezionare la casella **include inheritable permissions from this object's parent**.

Questa è l'impostazione predefinita.

- Selezionare la casella **Sostituisci tutte le autorizzazioni dell'oggetto figlio con le autorizzazioni ereditabili da questo oggetto**.

Questa impostazione non è presente nella casella permessi se si impostano i permessi del file NTFS su un singolo file.



Fare attenzione quando si seleziona questa impostazione. Questa impostazione rimuove tutte le autorizzazioni esistenti su tutti gli oggetti figlio e le sostituisce con le impostazioni di autorizzazione dell'oggetto. È possibile rimuovere inavvertitamente le autorizzazioni che non si desidera rimuovere. È particolarmente importante quando si impostano le autorizzazioni in un volume misto di sicurezza o in un qtree. Se gli oggetti figlio dispongono di uno stile di protezione UNIX effettivo, la propagazione delle autorizzazioni NTFS a tali oggetti figlio comporta la modifica di tali oggetti da stile di protezione UNIX a stile di protezione NTFS da parte di ONTAP e la sostituzione di tutte le autorizzazioni UNIX per tali oggetti figlio con autorizzazioni NTFS.

- Selezionare entrambe le caselle.
- Selezionare nessuna delle due caselle.

- Fare clic su **OK** per chiudere la casella **Permissions**.
- Fare clic su **OK** per chiudere la casella **Impostazioni di protezione avanzate per <Object>**.

Per ulteriori informazioni su come impostare le autorizzazioni NTFS avanzate, consultare la documentazione di Windows.

## Informazioni correlate

[Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI](#)

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security](#)

### Configurare le autorizzazioni per i file NTFS utilizzando l'interfaccia utente di ONTAP

È possibile configurare le autorizzazioni dei file NTFS su file e directory utilizzando l'interfaccia utente di ONTAP. Ciò consente di configurare le autorizzazioni per i file NTFS senza la necessità di connettersi ai dati utilizzando una condivisione SMB su un client Windows.

È possibile configurare le autorizzazioni dei file NTFS aggiungendo voci agli elenchi di controllo degli accessi discrezionali (DACL) NTFS associati a un descrittore di protezione NTFS. Il descrittore di protezione viene quindi applicato ai file e alle directory NTFS.

È possibile configurare le autorizzazioni dei file NTFS solo dalla riga di comando. Non è possibile configurare gli ACL NFSv4 utilizzando l'interfaccia CLI.

#### Fasi

1. Creare un descrittore di protezione NTFS.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -owner owner_name -group primary_group_name  
-control-flags-raw raw_control_flags
```

2. Aggiungere DACL al descrittore di protezione NTFS.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name  
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to  
{this-folder|sub-folders|files}
```

3. Creare una policy di sicurezza per file/directory.

```
vserver security file-directory policy create -vserver svm_name -policy-name  
policy_name
```

### In che modo le autorizzazioni dei file UNIX forniscono il controllo degli accessi quando si accede ai file tramite SMB

Un volume FlexVol può avere uno dei tre tipi di protezione: NTFS, UNIX o misto. È possibile accedere ai dati tramite SMB indipendentemente dallo stile di sicurezza; tuttavia, sono necessarie autorizzazioni appropriate per i file UNIX per accedere ai dati con una protezione efficace UNIX.

Quando si accede ai dati tramite SMB, vengono utilizzati diversi controlli di accesso per determinare se un utente è autorizzato a eseguire un'azione richiesta:

- Permessi di esportazione

La configurazione delle autorizzazioni di esportazione per l'accesso SMB è facoltativa.

- Autorizzazioni di condivisione

- Permessi del file

I seguenti tipi di permessi di file potrebbero essere applicati ai dati sui quali l'utente desidera eseguire un'azione:

- NTFS
- ACL NFSv4 UNIX
- Bit di modalità UNIX

Per i dati con ACL NFSv4 o bit di modalità UNIX impostati, vengono utilizzate autorizzazioni di stile UNIX per determinare i diritti di accesso ai dati. L'amministratore di SVM deve impostare l'autorizzazione file appropriata per garantire che gli utenti dispongano dei diritti per eseguire l'azione desiderata.



I dati in un volume misto di sicurezza potrebbero avere uno stile di sicurezza efficace NTFS o UNIX. Se i dati hanno uno stile di sicurezza UNIX effettivo, le autorizzazioni NFSv4 o i bit di modalità UNIX vengono utilizzati per determinare i diritti di accesso ai dati.

## **Accesso sicuro ai file utilizzando il controllo dinamico degli accessi (DAC)**

### **Proteggere l'accesso ai file utilizzando la panoramica del controllo dinamico dell'accesso (DAC)**

È possibile proteggere l'accesso utilizzando il controllo dinamico degli accessi e creando policy di accesso centrali in Active Directory e applicandole a file e cartelle su SVM tramite oggetti Criteri di gruppo applicati (GPO). È possibile configurare il controllo in modo che utilizzi gli eventi di staging dei criteri di accesso centrale per visualizzare gli effetti delle modifiche ai criteri di accesso centrale prima di applicarli.

### **Aggiunte alle credenziali CIFS**

Prima di Dynamic Access Control, una credenziale CIFS includeva l'identità di un'entità di protezione (l'utente) e l'appartenenza al gruppo Windows. Con Dynamic Access Control, alla credenziale vengono aggiunti altri tre tipi di informazioni: Identità del dispositivo, attestazioni del dispositivo e attestazioni dell'utente:

- Identità del dispositivo

L'analogo delle informazioni di identità dell'utente, ad eccezione dell'identità e dell'appartenenza al gruppo del dispositivo da cui l'utente effettua l'accesso.

- Dichiarazioni dei dispositivi

Asserzioni su un'entità di sicurezza del dispositivo. Ad esempio, un'attestazione del dispositivo potrebbe essere che è un membro di una specifica unità organizzativa.

- Richieste dell'utente

Asserzioni su un'identità di sicurezza dell'utente. Ad esempio, un utente può affermare che il proprio account ad è membro di una specifica unità organizzativa.

## **Policy di accesso centrale**

I criteri di accesso centrale per i file consentono alle organizzazioni di implementare e gestire centralmente policy di autorizzazione che includono espressioni condizionali utilizzando gruppi di utenti, attestazioni utente,

attestazioni dispositivo e proprietà delle risorse.

Ad esempio, per accedere ai dati ad alto impatto sul business, un utente deve essere un dipendente a tempo pieno e avere accesso ai dati solo da un dispositivo gestito. I criteri di accesso centrale sono definiti in Active Directory e distribuiti ai file server tramite il meccanismo GPO.

### **Staging dei criteri di accesso centralizzato con auditing avanzato**

Le policy di accesso centrale possono essere “staged”, nel qual caso vengono valutate in modo “what-if” durante i controlli di accesso ai file. I risultati di ciò che sarebbe accaduto se la policy fosse stata applicata e in che modo differisce da ciò che è attualmente configurato vengono registrati come evento di audit. In questo modo, gli amministratori possono utilizzare i registri degli eventi di audit per studiare l'impatto di una modifica dei criteri di accesso prima di mettere effettivamente in pratica i criteri. Dopo aver valutato l'impatto di una modifica della policy di accesso, la policy può essere implementata tramite GPO nelle SVM desiderate.

#### **Informazioni correlate**

[GPO supportati](#)

[Applicazione di oggetti Criteri di gruppo ai server CIFS](#)

[Attivazione o disattivazione del supporto GPO su un server CIFS](#)

[Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo](#)

[Visualizzazione di informazioni sui criteri di accesso centrale](#)

[Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale](#)

[Configurazione delle policy di accesso centrale per proteggere i dati sui server CIFS](#)

[Visualizzazione di informazioni sulla sicurezza del controllo dinamico degli accessi](#)

["Controllo SMB e NFS e tracciamento della sicurezza"](#)

#### **Funzionalità Dynamic Access Control supportata**

Se si desidera utilizzare il controllo dinamico degli accessi (DAC) sul server CIFS, è necessario comprendere in che modo ONTAP supporta la funzionalità di controllo dinamico degli accessi negli ambienti Active Directory.

#### **Supportato per Dynamic Access Control**

ONTAP supporta le seguenti funzionalità quando il controllo dinamico degli accessi è attivato sul server CIFS:

Funzionalità	Commenti
Attestazioni nel file system	Le affermazioni sono semplici coppie di nomi e valori che indicano una certa verità su un utente. Le credenziali utente contengono informazioni sulle attestazioni e i descrittori di protezione sui file possono eseguire controlli di accesso che includono controlli delle attestazioni. In questo modo, gli amministratori possono avere un maggiore controllo sugli utenti che possono accedere ai file.
Espressioni condizionali per i controlli di accesso al file	Quando si modificano i parametri di protezione di un file, gli utenti possono aggiungere espressioni condizionali arbitrariamente complesse al descrittore di protezione del file. L'espressione condizionale può includere controlli per le attestazioni.
Controllo centralizzato dell'accesso ai file tramite policy di accesso centrali	I criteri di accesso centrale sono un tipo di ACL memorizzato in Active Directory che può essere contrassegnato in un file. L'accesso al file viene concesso solo se i controlli di accesso del descrittore di protezione su disco e del criterio di accesso centrale con tag consentono l'accesso. In questo modo, gli amministratori possono controllare l'accesso ai file da una posizione centrale (ad) senza dover modificare il descrittore di protezione su disco.
Staging dei criteri di accesso centrale	Aggiunge la possibilità di provare le modifiche di sicurezza senza influire sull'accesso effettivo ai file, "eseguendo `staging`" una modifica alle policy di accesso centrale e osservando l'effetto della modifica in un report di audit.
Supporto per la visualizzazione di informazioni sulla sicurezza dei criteri di accesso centrale mediante l'interfaccia utente di ONTAP	Estende <code>vserver security file-directory show</code> per visualizzare le informazioni sui criteri di accesso centrale applicati.
Analisi della sicurezza che include policy di accesso centralizzate	Estende <code>vserver security trace</code> famiglia di comandi per visualizzare i risultati che includono informazioni sui criteri di accesso centrale applicati.

### Non supportato per Dynamic Access Control

ONTAP non supporta le seguenti funzionalità quando il controllo dinamico degli accessi è attivato sul server CIFS:



Funzionalità	Commenti
Classificazione automatica degli oggetti del file system NTFS	Si tratta di un'estensione dell'infrastruttura di classificazione dei file di Windows non supportata in ONTAP.
Auditing avanzato diverso dalla gestione temporanea dei criteri di accesso centrale	Solo lo staging dei criteri di accesso centrale è supportato per il controllo avanzato.

#### **Considerazioni sull'utilizzo del controllo dinamico degli accessi e delle policy di accesso centrale con i server CIFS**

È necessario tenere presente alcune considerazioni quando si utilizza il controllo dinamico dell'accesso (DAC) e i criteri di accesso centrale per proteggere file e cartelle sui server CIFS.

#### **L'accesso NFS può essere negato all'utente root se la regola dei criteri si applica all'utente di dominio/amministratore**

In alcuni casi, l'accesso NFS a root potrebbe essere negato quando la sicurezza del criterio di accesso centrale viene applicata ai dati a cui l'utente root sta tentando di accedere. Il problema si verifica quando il criterio di accesso centrale contiene una regola che viene applicata al dominio/amministratore e l'account root viene mappato all'account di dominio/amministratore.

Invece di applicare una regola all'utente di dominio/amministratore, è necessario applicarla a un gruppo con privilegi amministrativi, ad esempio il gruppo dominio/amministratori. In questo modo, è possibile mappare root all'account di dominio/amministratore senza che root sia interessato da questo problema.

#### **Il gruppo BUILTIN/Administrators del server CIFS ha accesso alle risorse quando il criterio di accesso centrale applicato non viene trovato in Active Directory**

È possibile che alle risorse contenute nel server CIFS siano applicati criteri di accesso centrale, ma quando il server CIFS utilizza il SID del criterio di accesso centrale per tentare di recuperare informazioni da Active Directory, il SID non corrisponde ai SID dei criteri di accesso centrale esistenti in Active Directory. In questi casi, il server CIFS applica il criterio di ripristino locale predefinito per tale risorsa.

Il criterio di ripristino locale predefinito consente al gruppo BUILTIN/Administrators del server CIFS di accedere a tale risorsa.

#### **Attiva o disattiva la panoramica del controllo dinamico degli accessi**

L'opzione che consente di utilizzare il controllo dinamico dell'accesso (DAC) per proteggere gli oggetti sul server CIFS è disattivata per impostazione predefinita. Attivare l'opzione se si desidera utilizzare Dynamic Access Control sul server CIFS. Se in seguito si decide di non utilizzare il controllo dinamico degli accessi per proteggere gli oggetti memorizzati nel server CIFS, è possibile disattivare l'opzione.

#### **A proposito di questa attività**

Una volta attivato il controllo dinamico degli accessi, il file system può contenere ACL con voci correlate al controllo dinamico degli accessi. Se Dynamic Access Control è disattivato, le voci correnti di Dynamic Access Control verranno ignorate e non saranno consentite le nuove.

Questa opzione è disponibile solo al livello di privilegio avanzato.

## Fase

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera che Dynamic Access Control sia...	Immettere il comando...
Attivato	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -is-dac-enabled false</code>

3. Tornare al livello di privilegi di amministratore: `set -privilege admin`

## Informazioni correlate

[Configurazione delle policy di accesso centrale per proteggere i dati sui server CIFS](#)

**Gestire gli ACL che contengono le ACE di controllo dinamico degli accessi quando il controllo dinamico degli accessi è disattivato**

Se si dispone di risorse con ACL applicati con ACE di controllo dinamico degli accessi e si disattiva il controllo dinamico degli accessi sulla macchina virtuale di storage (SVM), è necessario rimuovere le ACE di controllo dinamico degli accessi prima di poter gestire le ACE di controllo degli accessi non dinamico su tale risorsa.

### A proposito di questa attività

Una volta disattivato il controllo dinamico degli accessi, non è possibile rimuovere le ACE di controllo degli accessi non dinamiche esistenti o aggiungere nuove ACE di controllo degli accessi non dinamiche fino a quando non sono state rimosse le ACE di controllo degli accessi dinamici esistenti.

È possibile utilizzare lo strumento utilizzato normalmente per gestire gli ACL per eseguire questi passaggi.

## Fasi

1. Determinare quali ACE di controllo dinamico degli accessi vengono applicati alla risorsa.
2. Rimuovere le ACE di controllo dinamico degli accessi dalla risorsa.
3. Aggiungere o rimuovere ACE di controllo degli accessi non dinamici come desiderato dalla risorsa.

## Configurare le policy di accesso centrale per proteggere i dati sui server CIFS

Per proteggere l'accesso ai dati sul server CIFS mediante criteri di accesso centrali, è necessario eseguire diversi passaggi, tra cui l'attivazione del controllo dinamico dell'accesso (DAC) sul server CIFS, la configurazione dei criteri di accesso centrale in Active Directory, l'applicazione dei criteri di accesso centrale ai container Active Directory con GPO, E abilitazione degli oggetti Criteri di gruppo sul server CIFS.

## Prima di iniziare

- Active Directory deve essere configurato per utilizzare criteri di accesso centrali.
- È necessario disporre di un accesso sufficiente sui domain controller di Active Directory per creare criteri di

accesso centrali e per creare e applicare gli oggetti Criteri di gruppo ai container che contengono i server CIFS.

- Per eseguire i comandi necessari, è necessario disporre di un accesso amministrativo sufficiente sulla macchina virtuale di storage (SVM).

### A proposito di questa attività

I criteri di accesso centrale vengono definiti e applicati agli oggetti Criteri di gruppo (GPO) in Active Directory. Per istruzioni sulla configurazione dei criteri di accesso centrale e degli oggetti Criteri di gruppo, consultare la Microsoft TechNet Library.

["Microsoft TechNet Library"](#)

### Fasi

1. Attivare Dynamic Access Control (controllo dinamico degli accessi) su SVM se non è già attivato utilizzando `vserver cifs options modify` comando.

```
vserver cifs options modify -vserver vs1 -is-dac-enabled true
```

2. Abilitare gli oggetti Criteri di gruppo (GPO) sul server CIFS se non sono già abilitati mediante `vserver cifs group-policy modify` comando.

```
vserver cifs group-policy modify -vserver vs1 -status enabled
```

3. Creare regole di accesso centrali e policy di accesso centrali in Active Directory.
4. Creare un oggetto Criteri di gruppo (GPO) per implementare i criteri di accesso centrale in Active Directory.
5. Applicare l'oggetto Criteri di gruppo al container in cui si trova l'account del computer del server CIFS.
6. Aggiornare manualmente gli oggetti Criteri di gruppo applicati al server CIFS utilizzando `vserver cifs group-policy update` comando.

```
vserver cifs group-policy update -vserver vs1
```

7. Verificare che il criterio di accesso centrale dell'oggetto Criteri di gruppo sia applicato alle risorse sul server CIFS utilizzando `vserver cifs group-policy show-applied` comando.

L'esempio seguente mostra che il criterio di dominio predefinito dispone di due criteri di accesso centrali applicati al server CIFS:

```
vserver cifs group-policy show-applied
```

```
Vserver: vs1
-----
GPO Name: Default Domain Policy
Level: Domain
Status: enabled
Advanced Audit Settings:
Object Access:
Central Access Policy Staging: failure
Registry Settings:
Refresh Time Interval: 22
```

```
Refresh Random Offset: 8
Hash Publication Mode for BranchCache: per-share
Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
    Audit Logon Events: none
    Audit Object Access: success
    Log Retention Method: overwrite-as-needed
    Max Log Size: 16384
  File Security:
    /vol1/home
    /vol1/dir1
  Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
  Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
  Registry Values:
    Signing Required: false
  Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
  Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
  Policies: cap1
           cap2

  GPO Name: Resultant Set of Policy
  Level: RSOP
Advanced Audit Settings:
  Object Access:
    Central Access Policy Staging: failure
Registry Settings:
  Refresh Time Interval: 22
  Refresh Random Offset: 8
  Hash Publication Mode for BranchCache: per-share
  Hash Version Support for BranchCache: all-versions
Security Settings:
  Event Audit and Event Log:
```

```
Audit Logon Events: none
Audit Object Access: success
Log Retention Method: overwrite-as-needed
Max Log Size: 16384
File Security:
    /vol1/home
    /vol1/dir1
Kerberos:
    Max Clock Skew: 5
    Max Ticket Age: 10
    Max Renew Age: 7
Privilege Rights:
    Take Ownership: usr1, usr2
    Security Privilege: usr1, usr2
    Change Notify: usr1, usr2
Registry Values:
    Signing Required: false
Restrict Anonymous:
    No enumeration of SAM accounts: true
    No enumeration of SAM accounts and shares: false
    Restrict anonymous access to shares and named pipes: true
    Combined restriction for anonymous user: no-access
Restricted Groups:
    gpr1
    gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2
2 entries were displayed.
```

### Informazioni correlate

[Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo](#)

[Visualizzazione di informazioni sui criteri di accesso centrale](#)

[Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale](#)

[Attivazione o disattivazione del controllo dinamico degli accessi](#)

**Visualizza informazioni sulla sicurezza del controllo dinamico degli accessi**

È possibile visualizzare informazioni sulla sicurezza del controllo dinamico degli accessi (DAC) sui volumi NTFS e sui dati con protezione effettiva NTFS su volumi misti di tipo sicurezza. Ciò include informazioni su ACE condizionali, ACE di risorse e ACE di policy di accesso centrale. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

## A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei dati di cui si desidera visualizzare le informazioni di sicurezza relative al file o alla cartella. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

## Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>
Dove viene visualizzato l'output con SID di gruppo e utente	<pre>vserver security file-directory show -vserver vserver_name -path path -lookup-names false</pre>
Informazioni sulla sicurezza di file e directory per file e directory in cui la bit mask esadecimale viene convertita in formato testuale	<pre>vserver security file-directory show -vserver vserver_name -path path -textual-mask true</pre>

## Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni di sicurezza del controllo dinamico degli accessi relative al percorso `/vol1` in SVM `vs1`:

```

cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
      Vserver: vs1
      File Path: /vol1
      File Inode Number: 112
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attribute: -
      Unix User Id: 0
      Unix Group Id: 1
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xbf14
            Owner:CIFS1\Administrator
            Group:CIFS1\Domain Admins
            SACL - ACEs
                  ALL-Everyone-0xf01ff-OI|CI|SA|FA
                  RESOURCE ATTRIBUTE-Everyone-0x0

      ("Department_MS",TS,0x10020,"Finance")
            POLICY ID-All resources - No Write-
0x0-OI|CI
            DACL - ACEs
                  ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                  ALLOW-Everyone-0x1f01ff-OI|CI
                  ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

      ((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)

```

## Informazioni correlate

[Visualizzazione delle informazioni sulle configurazioni dell'oggetto Criteri di gruppo](#)

[Visualizzazione di informazioni sui criteri di accesso centrale](#)

[Visualizzazione delle informazioni sulle regole dei criteri di accesso centrale](#)

## Considerazioni sul revert per il controllo dinamico degli accessi

È necessario essere consapevoli di cosa accade quando si torna a una versione di ONTAP che non supporta il controllo dinamico degli accessi (DAC) e di cosa si deve fare prima e dopo il ripristino.

Se si desidera ripristinare il cluster a una versione di ONTAP che non supporta il controllo dinamico degli accessi e che il controllo dinamico degli accessi sia attivato su una o più macchine virtuali dello storage (SVM), prima di eseguire il ripristino è necessario eseguire le seguenti operazioni:

- È necessario disattivare il controllo dinamico degli accessi su tutte le SVM che lo hanno attivato nel cluster.
- È necessario modificare le configurazioni di controllo del cluster che contengono `cap-staging` tipo di evento per utilizzare solo `file-op` tipo di evento.

È necessario comprendere e agire in base ad alcune importanti considerazioni di revert per file e cartelle con le ACE di controllo dinamico degli accessi:

- Se il cluster viene invertito, le ACE di controllo dinamico degli accessi esistenti non vengono rimosse; tuttavia, verranno ignorate nei controlli di accesso ai file.
- Poiché le ACE di controllo dinamico degli accessi vengono ignorate dopo la revisione, l'accesso ai file cambia nei file con le ACE di controllo dinamico degli accessi.

Ciò potrebbe consentire agli utenti di accedere a file che in precedenza non potevano o che non potevano accedere a file che in precedenza potevano.

- Per ripristinare il livello di protezione precedente, è necessario applicare ACE di controllo degli accessi non dinamici ai file interessati.

Questa operazione può essere eseguita prima del ripristino o immediatamente dopo il completamento della revisione.



Poiché le ACE di controllo dinamico degli accessi vengono ignorate dopo la reversione, non è necessario rimuoverle quando si applicano ACE di controllo degli accessi non dinamici ai file interessati. Tuttavia, se lo si desidera, è possibile rimuoverli manualmente.

**Dove trovare ulteriori informazioni sulla configurazione e l'utilizzo del controllo dinamico degli accessi e delle policy di accesso centrali**

Sono disponibili risorse aggiuntive per la configurazione e l'utilizzo di Dynamic Access Control e policy di accesso centrali.

Nella Microsoft TechNet Library sono disponibili informazioni su come configurare il controllo dinamico degli accessi e i criteri di accesso centrale in Active Directory.

["Microsoft TechNet: Panoramica dello scenario di controllo dinamico degli accessi"](#)

["Microsoft TechNet: Scenario dei criteri di accesso centrale"](#)

I seguenti riferimenti consentono di configurare il server SMB in modo che utilizzi e supporti il controllo dinamico degli accessi e le policy di accesso centrale:

- **Utilizzo di GPO sul server SMB**

[Applicazione di oggetti Criteri di gruppo ai server SMB](#)

- **Configurazione del controllo NAS sul server SMB**

["Controllo SMB e NFS e tracciamento della sicurezza"](#)



## Accesso sicuro alle PMI tramite policy di esportazione

### Come vengono utilizzate le policy di esportazione con l'accesso SMB

Se i criteri di esportazione per l'accesso SMB sono attivati sul server SMB, i criteri di esportazione vengono utilizzati per controllare l'accesso ai volumi SVM da parte dei client SMB. Per accedere ai dati, è possibile creare un criterio di esportazione che consenta l'accesso SMB e associare il criterio ai volumi contenenti condivisioni SMB.

Una policy di esportazione prevede l'applicazione di una o più regole che specificano i client ai quali è consentito l'accesso ai dati e i protocolli di autenticazione supportati per l'accesso in sola lettura e in lettura/scrittura. È possibile configurare i criteri di esportazione per consentire l'accesso tramite SMB a tutti i client, a una subnet di client o a un client specifico e per consentire l'autenticazione utilizzando l'autenticazione Kerberos, l'autenticazione NTLM o l'autenticazione Kerberos e NTLM quando si determina l'accesso di sola lettura e lettura/scrittura ai dati.

Dopo aver elaborato tutte le regole di esportazione applicate ai criteri di esportazione, ONTAP può determinare se al client viene concesso l'accesso e quale livello di accesso viene concesso. Le regole di esportazione si applicano ai computer client, non agli utenti e ai gruppi Windows. Le regole di esportazione non sostituiscono l'autenticazione e l'autorizzazione basate su utenti e gruppi di Windows. Le regole di esportazione offrono un altro livello di sicurezza degli accessi oltre alle autorizzazioni di condivisione e accesso ai file.

Per configurare l'accesso del client al volume, è necessario associare esattamente un criterio di esportazione a ciascun volume. Ogni SVM può contenere più policy di esportazione. Ciò consente di eseguire le seguenti operazioni per le SVM con più volumi:

- Assegnare criteri di esportazione diversi a ciascun volume di SVM per il controllo degli accessi dei singoli client a ciascun volume di SVM.
- Assegnare la stessa policy di esportazione a più volumi di SVM per un identico controllo dell'accesso client senza dover creare una nuova policy di esportazione per ciascun volume.

Ogni SVM dispone di almeno una policy di esportazione chiamata "default", che non contiene regole. Non è possibile eliminare questo criterio di esportazione, ma è possibile rinominarlo o modificarlo. Per impostazione predefinita, ciascun volume della SVM è associato al criterio di esportazione predefinito. Se i criteri di esportazione per l'accesso SMB sono disattivati sulla SVM, la policy di esportazione "default" non ha alcun effetto sull'accesso SMB.

È possibile configurare le regole che forniscono l'accesso agli host NFS e SMB e associare tale regola a un criterio di esportazione, che può quindi essere associato al volume che contiene i dati a cui devono accedere gli host NFS e SMB. In alternativa, se esistono volumi in cui solo i client SMB richiedono l'accesso, è possibile configurare un criterio di esportazione con regole che consentono l'accesso solo utilizzando il protocollo SMB e che utilizzano solo Kerberos o NTLM (o entrambi) per l'autenticazione in sola lettura e in scrittura. Il criterio di esportazione viene quindi associato ai volumi in cui si desidera solo l'accesso SMB.

Se i criteri di esportazione per SMB sono attivati e un client effettua una richiesta di accesso non consentita dalla policy di esportazione applicabile, la richiesta non riesce e viene visualizzato un messaggio di autorizzazione negata. Se un client non corrisponde a nessuna regola nella policy di esportazione del volume, l'accesso viene negato. Se un criterio di esportazione è vuoto, tutti gli accessi vengono implicitamente negati. Ciò è vero anche se le autorizzazioni di condivisione e file consentirebbero altrimenti l'accesso. Ciò significa che è necessario configurare la policy di esportazione in modo da consentire in modo minimo quanto segue sui volumi contenenti condivisioni SMB:

- Consentire l'accesso a tutti i client o al sottoinsieme appropriato di client

- Consentire l'accesso tramite SMB
- Consentire l'accesso di sola lettura e scrittura appropriato utilizzando l'autenticazione Kerberos o NTLM (o entrambe)

Scopri di più ["configurazione e gestione delle policy di esportazione"](#).

### Come funzionano le regole di esportazione

Le regole di esportazione sono gli elementi funzionali di una policy di esportazione. Le regole di esportazione consentono di associare le richieste di accesso client a un volume a parametri specifici configurati per determinare come gestire le richieste di accesso client.

Un criterio di esportazione deve contenere almeno una regola di esportazione per consentire l'accesso ai client. Se un criterio di esportazione contiene più di una regola, le regole vengono elaborate nell'ordine in cui appaiono nel criterio di esportazione. L'ordine delle regole è determinato dal numero di indice delle regole. Se una regola corrisponde a un client, vengono utilizzate le autorizzazioni di tale regola e non vengono elaborate ulteriori regole. Se nessuna regola corrisponde, al client viene negato l'accesso.

È possibile configurare le regole di esportazione per determinare le autorizzazioni di accesso del client utilizzando i seguenti criteri:

- Il protocollo di accesso al file utilizzato dal client che invia la richiesta, ad esempio NFSv4 o SMB.
- Identificatore del client, ad esempio nome host o indirizzo IP.

La dimensione massima di `-clientmatch` il campo è composto da 4096 caratteri.

- Il tipo di protezione utilizzato dal client per autenticare, ad esempio Kerberos v5, NTLM o AUTH\_SYS.

Se una regola specifica più criteri, il client deve corrispondere a tutti i criteri affinché la regola venga applicata.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

La richiesta di accesso client viene inviata utilizzando il protocollo NFSv3 e il client ha l'indirizzo IP 10.1.17.37.

Anche se il protocollo di accesso client corrisponde, l'indirizzo IP del client si trova in una subnet diversa da quella specificata nella regola di esportazione. Pertanto, la corrispondenza dei client non riesce e questa regola non si applica a questo client.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`

- `-rorule any`
- `-rwrule any`

La richiesta di accesso client viene inviata utilizzando il protocollo NFSv4 e il client ha l'indirizzo IP 10.1.16.54.

Il protocollo di accesso client corrisponde e l'indirizzo IP del client si trova nella subnet specificata. Pertanto, la corrispondenza dei client viene eseguita correttamente e questa regola si applica a questo client. Il client ottiene l'accesso in lettura/scrittura indipendentemente dal tipo di protezione.

### Esempio

Il criterio di esportazione contiene una regola di esportazione con i seguenti parametri:

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

Il client n. 1 ha l'indirizzo IP 10.1.16.207, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con Kerberos v5.

Il client n. 2 ha l'indirizzo IP 10.1.16.211, invia una richiesta di accesso utilizzando il protocollo NFSv3 e viene autenticato con AUTH\_SYS.

Il protocollo di accesso client e l'indirizzo IP corrispondono per entrambi i client. Il parametro di sola lettura consente l'accesso in sola lettura a tutti i client, indipendentemente dal tipo di protezione con cui sono stati autenticati. Pertanto, entrambi i client ottengono l'accesso in sola lettura. Tuttavia, solo il client n. 1 ottiene l'accesso in lettura/scrittura perché per l'autenticazione è stato utilizzato il tipo di protezione approvato Kerberos v5. Il client n. 2 non ottiene l'accesso in lettura/scrittura.

### Esempi di regole dei criteri di esportazione che limitano o consentono l'accesso tramite SMB

Gli esempi mostrano come creare regole di policy di esportazione che limitano o consentono l'accesso tramite SMB su una SVM con criteri di esportazione per l'accesso SMB abilitati.

I criteri di esportazione per l'accesso SMB sono disattivati per impostazione predefinita. È necessario configurare le regole dei criteri di esportazione che limitano o consentono l'accesso su SMB solo se sono state attivate le policy di esportazione per l'accesso SMB.

### Regola di esportazione solo per l'accesso SMB

Il seguente comando crea una regola di esportazione sulla SVM denominata "vs1" con la seguente configurazione:

- Nome policy: Cifs1
- Numero indice: 1
- Client match (corrispondenza client): Corrisponde solo ai client sulla rete 192.168.1.0/24
- Protocol (protocollo): Consente solo l'accesso SMB
- Accesso di sola lettura: Ai client che utilizzano l'autenticazione NTLM o Kerberos

- Accesso in lettura/scrittura: Ai client che utilizzano l'autenticazione Kerberos

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

## Regola di esportazione per accesso SMB e NFS

Il seguente comando crea una regola di esportazione sulla SVM denominata "vs1" con la seguente configurazione:

- Nome policy: Cifsnfs1
- Numero indice: 2
- Client match (corrispondenza client): Corrisponde a tutti i client
- Protocollo: Accesso SMB e NFS
- Accesso in sola lettura: A tutti i client
- Accesso in lettura/scrittura: Ai client che utilizzano Kerberos (NFS e SMB) o autenticazione NTLM (SMB)
- Mapping per ID utente UNIX 0 (zero): Mappato all'ID utente 65534 (che in genere viene mappato al nome utente nessuno)
- Accesso SUID e sgid: Consente

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule any
-rwrule krb5,ntlm -anon 65534 -allow-suid true
```

## Regola di esportazione per l'accesso SMB utilizzando solo NTLM

Il seguente comando crea una regola di esportazione sulla SVM denominata "vs1" con la seguente configurazione:

- Nome policy: Ntlm1
- Numero indice: 1
- Client match (corrispondenza client): Corrisponde a tutti i client
- Protocol (protocollo): Consente solo l'accesso SMB
- Accesso di sola lettura: Solo ai client che utilizzano NTLM
- Accesso di lettura/scrittura: Solo ai client che utilizzano NTLM



Se si configura l'opzione di sola lettura o l'opzione di lettura/scrittura per l'accesso solo NTLM, è necessario utilizzare le voci basate sull'indirizzo IP nell'opzione di corrispondenza del client. In caso contrario, ricevi `access denied` errori. Questo perché ONTAP utilizza i nomi principali del servizio Kerberos (SPN) quando si utilizza un nome host per verificare i diritti di accesso del client. L'autenticazione NTLM non supporta i nomi SPN.

```
cluster1::> vservers export-policy rule create -vservers vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

### Attiva o disattiva i criteri di esportazione per l'accesso SMB

È possibile attivare o disattivare le policy di esportazione per l'accesso SMB sulle macchine virtuali di storage (SVM). L'utilizzo di policy di esportazione per controllare l'accesso SMB alle risorse è facoltativo.

#### Prima di iniziare

Di seguito sono riportati i requisiti per l'attivazione delle policy di esportazione per SMB:

- Il client deve disporre di un record "PTR" nel DNS prima di creare le regole di esportazione per tale client.
- Se la SVM fornisce l'accesso ai client NFS e se il nome host che si desidera utilizzare per l'accesso NFS è diverso dal nome del server CIFS, è necessario disporre di un set aggiuntivo di record "A" e "PTR" per i nomi host.

#### A proposito di questa attività

Quando si imposta un nuovo server CIFS su SVM, l'utilizzo dei criteri di esportazione per l'accesso SMB viene disattivato per impostazione predefinita. È possibile attivare i criteri di esportazione per l'accesso SMB se si desidera controllare l'accesso in base al protocollo di autenticazione o agli indirizzi IP o ai nomi host dei client. È possibile attivare o disattivare i criteri di esportazione per l'accesso SMB in qualsiasi momento.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Attivare o disattivare i criteri di esportazione:
  - Abilitare i criteri di esportazione: `vservers cifs options modify -vservers vservers_name -is-exportpolicy-enabled true`
  - Disattiva policy di esportazione: `vservers cifs options modify -vservers vservers_name -is-exportpolicy-enabled false`
3. Tornare al livello di privilegio admin: `set -privilege admin`

#### Esempio

L'esempio seguente consente l'utilizzo di policy di esportazione per controllare l'accesso del client SMB alle risorse su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

## Proteggere l'accesso ai file utilizzando Storage-Level Access Guard

### Proteggere l'accesso ai file utilizzando Storage-Level Access Guard

Oltre a proteggere l'accesso utilizzando la sicurezza nativa a livello di file e di esportazione e condivisione, è possibile configurare la protezione dell'accesso a livello di storage, un terzo livello di sicurezza applicato da ONTAP a livello di volume. Storage-Level Access Guard si applica all'accesso da tutti i protocolli NAS all'oggetto di storage a cui è applicato.

Sono supportate solo le autorizzazioni di accesso NTFS. Affinché ONTAP esegua controlli di sicurezza sugli utenti UNIX per l'accesso ai dati sui volumi per i quali è stato applicato Storage-Level Access Guard, l'utente UNIX deve eseguire il mapping a un utente Windows sulla SVM proprietaria del volume.

### Comportamento di Access Guard a livello di storage

- Storage-Level Access Guard si applica a tutti i file o a tutte le directory di un oggetto di storage.

Poiché tutti i file o le directory di un volume sono soggetti alle impostazioni di Storage-Level Access Guard, non è richiesta l'ereditarietà attraverso la propagazione.

- È possibile configurare Storage-Level Access Guard in modo che si applichi solo ai file, solo alle directory o sia ai file che alle directory all'interno di un volume.

- Sicurezza di file e directory

Si applica a ogni directory e file all'interno dell'oggetto di storage. Questa è l'impostazione predefinita.

- Sicurezza del file

Si applica a tutti i file all'interno dell'oggetto di storage. L'applicazione di questa protezione non influisce sull'accesso o sul controllo delle directory.

- Sicurezza della directory

Si applica a ogni directory all'interno dell'oggetto di storage. L'applicazione di questa protezione non influisce sull'accesso o sul controllo dei file.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

Non assegnerà mai autorizzazioni di accesso aggiuntive.

- Se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, la protezione Storage-Level Access Guard non viene visualizzata.

Viene applicato a livello di oggetto di storage e memorizzato nei metadati utilizzati per determinare le autorizzazioni effettive.

- La sicurezza a livello di storage non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX).

È progettato per essere modificato solo dagli amministratori dello storage.

- È possibile applicare Storage-Level Access Guard a volumi con NTFS o stile di sicurezza misto.
- È possibile applicare Storage-Level Access Guard ai volumi con lo stile di sicurezza UNIX, purché la SVM contenente il volume abbia configurato un server CIFS.
- Quando i volumi sono montati sotto un percorso di giunzione del volume e se Storage-Level Access Guard è presente su tale percorso, non verrà propagata ai volumi montati sotto di esso.
- Il descrittore di sicurezza Storage-Level Access Guard viene replicato con la replica dei dati SnapMirror e con la replica SVM.
- Esiste una dispensazione speciale per i virus scanner.

A questi server è consentito un accesso eccezionale per lo screening di file e directory, anche se Storage-Level Access Guard nega l'accesso all'oggetto.

- Le notifiche FPolicy non vengono inviate se l'accesso viene negato a causa di Storage-Level Access Guard.

## Ordine dei controlli di accesso

L'accesso a un file o a una directory è determinato dall'effetto combinato delle autorizzazioni di esportazione o condivisione, delle autorizzazioni Storage-Level Access Guard impostate sui volumi e delle autorizzazioni native dei file applicate a file e/o directory. Tutti i livelli di sicurezza vengono valutati per determinare le autorizzazioni effettive di un file o di una directory. I controlli di accesso di sicurezza vengono eseguiti nel seguente ordine:

1. Permessi di condivisione SMB o NFS a livello di esportazione
2. Access Guard a livello di storage
3. ACL (Access Control List) file/cartelle NTFS, ACL NFSv4 o bit di modalità UNIX

## Casi di utilizzo di Storage-Level Access Guard

Storage-Level Access Guard offre una sicurezza aggiuntiva a livello di storage, che non è visibile dal lato client; pertanto, non può essere revocata da nessuno degli utenti o degli amministratori dai propri desktop. Esistono alcuni casi di utilizzo in cui la capacità di controllare l'accesso a livello di storage è vantaggiosa.

I casi di utilizzo tipici di questa funzionalità includono i seguenti scenari:

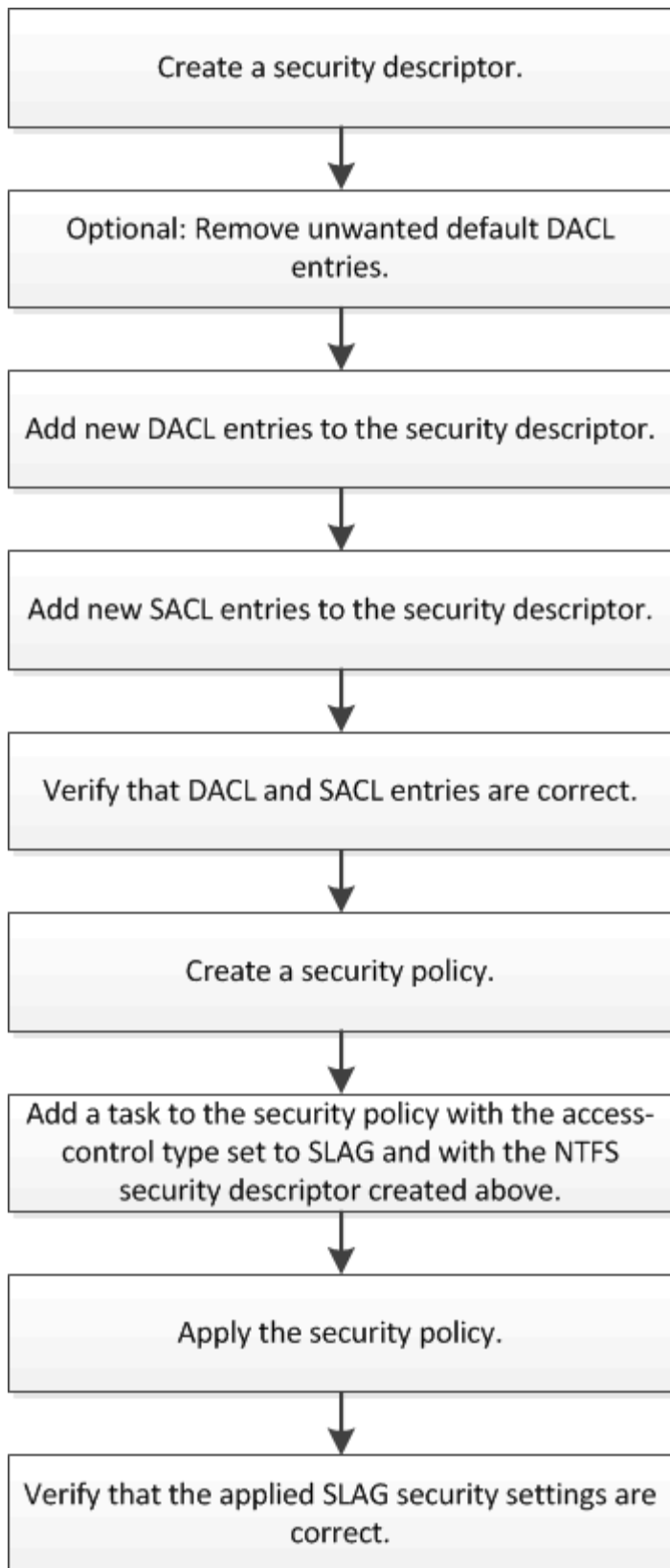
- Protezione della proprietà intellettuale attraverso il controllo e il controllo dell'accesso di tutti gli utenti a livello di storage
- Storage per le società di servizi finanziari, inclusi gruppi bancari e commerciali

- Servizi governativi con storage di file separato per singoli reparti
- Le università proteggono tutti i file degli studenti

#### **Workflow per configurare Storage-Level Access Guard**

Il flusso di lavoro per la configurazione di Storage-Level Access Guard (SLAG) utilizza gli stessi comandi CLI di ONTAP utilizzati per configurare le autorizzazioni dei file NTFS e i criteri di controllo. Invece di configurare l'accesso a file e directory su una destinazione designata, è possibile configurare LO SLAG sul volume SVM (Storage Virtual Machine) designato.





#### Informazioni correlate

[Configurazione di Storage-Level Access Guard](#)

Per configurare Storage-Level Access Guard su un volume o su un qtree, è necessario seguire una serie di passaggi. Storage-Level Access Guard offre un livello di sicurezza degli accessi impostato a livello di storage. Fornisce una sicurezza che si applica a tutti gli accessi da tutti i protocolli NAS all'oggetto di storage a cui è stato applicato.

### Fasi

1. Creare un descrittore di protezione utilizzando `vserver security file-directory ntfs create` comando.

```
vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sdl vserver
security file-directory ntfs show -vserver vs1
```

```
Vserver: vs1
```

NTFS Security Descriptor Name	Owner Name
-----	-----
sdl	-

Viene creato un descrittore di protezione con le seguenti quattro voci di controllo di accesso DACL predefinite:

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sdl
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
BUILTIN\Administrators	allow	full-control	this-folder, sub-folders, files
BUILTIN\Users	allow	full-control	this-folder, sub-folders, files
CREATOR OWNER	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

Se non si desidera utilizzare le voci predefinite durante la configurazione di Storage-Level Access Guard, è possibile rimuoverle prima di creare e aggiungere le proprie ACE al descrittore di protezione.

2. Rimuovere dal descrittore di protezione una delle ACL DACL predefinite che non si desidera configurare con la protezione Storage-Level Access Guard:

- a. Rimuovere eventuali ACL DACL indesiderati utilizzando `vserver security file-directory ntfs dacl remove` comando.

In questo esempio, tre ACL DACL predefiniti vengono rimossi dal descrittore di protezione: BUILTIN/Administrators, BUILTIN/Users e CREATOR OWNER.

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

- b. Verificare che le ACL DACL che non si desidera utilizzare per la protezione Storage-Level Access Guard siano rimosse dal descrittore di protezione utilizzando `vserver security file-directory ntfs dacl show` comando.

In questo esempio, l'output del comando verifica che tre ACL DACL predefinite siano state rimosse dal descrittore di protezione, lasciando solo la voce ACE DACL predefinita di sistema/AUTORITÀ NT:

```
vserver security file-directory ntfs dacl show -vserver vs1
```

Vserver: vs1

NTFS Security Descriptor Name: sd1

Account Name	Access Type	Access Rights	Apply To
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

3. Aggiungere una o più voci DACL a un descrittore di protezione utilizzando `vserver security file-directory ntfs dacl add` comando.

In questo esempio, due ACL DACL vengono aggiunti al descrittore di protezione:

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. Aggiungere una o più voci SACL a un descrittore di protezione utilizzando `vserver security file-directory ntfs sacl add` comando.

In questo esempio, due ACL SACL vengono aggiunti al descrittore di protezione:

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
```

```
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. Verificare che le ACL DACL e SACL siano configurate correttamente utilizzando `vserver security file-directory ntfs dacl show` e `vserver security file-directory ntfs sacl show` comandi, rispettivamente.

In questo esempio, il comando seguente visualizza informazioni sulle voci DACL per il descrittore di protezione “sd1”:

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
EXAMPLE\Domain Users	allow	read	this-folder, sub-folders, files
EXAMPLE\engineering	allow	full-control	this-folder, sub-folders, files
NT AUTHORITY\SYSTEM	allow	full-control	this-folder, sub-folders, files

In questo esempio, il comando seguente visualizza informazioni sulle voci SACL per il descrittore di protezione “sd1”:

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
EXAMPLE\Domain Users	failure	read	this-folder, sub-folders, files
EXAMPLE\engineering	success	full-control	this-folder, sub-folders, files

6. Creare un criterio di protezione utilizzando `vserver security file-directory policy create` comando.

Nell'esempio seguente viene creata una policy denominata "policy1":

```
vserver security file-directory policy create -vserver vs1 -policy-name policy1
```

7. Verificare che il criterio sia configurato correttamente utilizzando `vserver security file-directory policy show` comando.

```
vserver security file-directory policy show
```

Vserver	Policy Name
-----	-----
vs1	policy1

8. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione utilizzando `vserver security file-directory policy task add` con il `-access-control` parametro impostato su `slag`.

Anche se un criterio può contenere più di un'attività Storage-Level Access Guard, non è possibile configurare un criterio in modo che contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

In questo esempio, viene aggiunto un task alla policy denominata "policy1", assegnata al descrittore di sicurezza "sd1". Viene assegnato a. /datavol1 percorso con il tipo di controllo dell'accesso impostato su "slag".

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1
```

9. Verificare che l'attività sia configurata correttamente utilizzando `vserver security file-directory policy task show` comando.

```
vserver security file-directory policy task show -vserver vs1 -policy-name policy1
```

```
Vserver: vs1
Policy: policy1
```

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	Descriptor
Name					
-----	-----	-----	-----	-----	
1	/datavol1	slag	ntfs	propagate	sd1

10. Applicare il criterio di protezione Storage-Level Access Guard utilizzando `vserver security file-directory apply` comando.

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

Il processo di applicazione della policy di sicurezza è pianificato.

11. Verificare che le impostazioni di protezione di Storage-Level Access Guard applicate siano corrette utilizzando `vserver security file-directory show` comando.

In questo esempio, l'output del comando indica che la protezione Storage-Level Access Guard è stata applicata al volume NTFS `/datavol1`. Anche se il DACL predefinito che consente il controllo completo a tutti rimane, la protezione di Storage-Level Access Guard limita (e controlla) l'accesso ai gruppi definiti nelle impostazioni di Storage-Level Access Guard.

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```

        Vserver: vs1
        File Path: /datavol1
File Inode Number: 77
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0x8004
              Owner:BUILTIN\Administrators
              Group:BUILTIN\Administrators
              DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

Storage-Level Access Guard security
SACL (Applies to Directories):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Directories):
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
SACL (Applies to Files):
  AUDIT-EXAMPLE\Domain Users-0x120089-FA
  AUDIT-EXAMPLE\engineering-0x1f01ff-SA
DACL (Applies to Files):
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-EXAMPLE\engineering-0x1f01ff
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

### Informazioni correlate

[Gestione della sicurezza dei file NTFS, delle policy di audit NTFS e di Storage-Level Access Guard su SVM mediante CLI](#)

[Workflow per configurare Storage-Level Access Guard](#)

[Visualizzazione di informazioni su Storage-Level Access Guard](#)

[Rimozione di Storage-Level Access Guard](#)

## Matrice DI SCORIE efficace

È possibile configurare LO SLAG su un volume, un qtree o entrambi. La matrice DELLE SCORIE definisce su quale volume o qtree è la configurazione DELLE SCORIE applicabile in diversi scenari elencati nella tabella.

	<b>SCORIA di volume in un AFS</b>	<b>SCORIE di volume in una copia Snapshot</b>	<b>SCORIE del qtree in un AFS</b>	<b>SCORIE del qtree in una copia Snapshot</b>
Accesso al volume in un file system di accesso (AFS)	Sì	NO	N/A.	N/A.
Accesso al volume in una copia Snapshot	Sì	NO	N/A.	N/A.
Accesso al qtree in un AFS (quando LA SCORIA è presente nel qtree)	NO	NO	Sì	NO
Accesso al qtree in un AFS (quando LA SCORIA non è presente in qtree)	Sì	NO	NO	NO
Accesso al qtree nella copia Snapshot (quando LA SCORIA è presente nel qtree AFS)	NO	NO	Sì	NO
Accesso al qtree nella copia Snapshot (quando LA SCORIA non è presente nel qtree AFS)	Sì	NO	NO	NO

### Visualizza informazioni su Storage-Level Access Guard

Storage-Level Access Guard è un terzo livello di sicurezza applicato a un volume o qtree. Le impostazioni di Storage-Level Access Guard non possono essere visualizzate utilizzando la finestra Proprietà di Windows. È necessario utilizzare l'interfaccia utente di ONTAP per visualizzare informazioni sulla protezione di Access Guard a livello di storage, che è possibile utilizzare per convalidare la configurazione o risolvere i problemi di accesso ai file.



### A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso del volume o del qtree di cui si desidera visualizzare le informazioni di protezione Storage-Level Access Guard. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

### Fase

1. Visualizzare le impostazioni di sicurezza di Storage-Level Access Guard con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i></pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i> -expand-mask true</pre>

### Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni di protezione di Storage-Level Access Guard per il volume di sicurezza NTFS con il percorso `/datavol1` in SVM `vs1`:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
    File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner:BUILTIN\Administrators
          Group:BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

    Storage-Level Access Guard security
    SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

Nell'esempio seguente vengono visualizzate le informazioni di Storage-Level Access Guard relative al volume misto di sicurezza nel percorso /datavol15 In SVM vs1. Il livello superiore di questo volume offre una protezione efficace per UNIX. Il volume dispone della protezione di Storage-Level Access Guard.

```

cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

### Rimuovere Storage-Level Access Guard

È possibile rimuovere Storage-Level Access Guard su un volume o qtree se non si desidera più impostare la sicurezza dell'accesso a livello di storage. La rimozione di Storage-Level Access Guard non modifica o rimuove la normale protezione di file e directory NTFS.

### Fasi

1. Verificare che nel volume o nel qtree sia configurato Storage-Level Access Guard utilizzando `vserver security file-directory show` comando.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```

        Vserver: vs1
        File Path: /datavol2
File Inode Number: 99
        Security Style: ntfs
        Effective Style: ntfs
        DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
              Control:0xbf14
              Owner:BUILTIN\Administrators
              Group:BUILTIN\Administrators
              SACL - ACEs
                AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
              DACL - ACEs
                ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

Storage-Level Access Guard security
DACL (Applies to Directories):
  ALLOW-BUILTIN\Administrators-0x1f01ff
  ALLOW-CREATOR OWNER-0x1f01ff
  ALLOW-EXAMPLE\Domain Admins-0x1f01ff
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
DACL (Applies to Files):
  ALLOW-BUILTIN\Administrators-0x1f01ff
  ALLOW-CREATOR OWNER-0x1f01ff
  ALLOW-EXAMPLE\Domain Admins-0x1f01ff
  ALLOW-EXAMPLE\Domain Users-0x120089
  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

2. Rimuovere Storage-Level Access Guard utilizzando `vserver security file-directory remove-slag` comando.

```
vserver security file-directory remove-slag -vserver vs1 -path /datavol2
```

3. Verificare che Storage-Level Access Guard sia stato rimosso dal volume o dal qtree utilizzando `vserver security file-directory show` comando.

```
vserver security file-directory show -vserver vs1 -path /datavol2
```

```
Vserver: vs1
File Path: /datavol2
File Inode Number: 99
Security Style: ntfs
Effective Style: ntfs
DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
Unix User Id: 0
Unix Group Id: 0
Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
ACLs: NTFS Security Descriptor
Control:0xbf14
Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
SACL - ACEs
AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
DACL - ACEs
ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

## Gestire l'accesso ai file utilizzando SMB

### Utilizzare utenti e gruppi locali per l'autenticazione e l'autorizzazione

Modalità di utilizzo di utenti e gruppi locali da parte di ONTAP

#### Concetti relativi a utenti e gruppi locali

Prima di stabilire se configurare e utilizzare utenti e gruppi locali nel proprio ambiente, è necessario conoscere gli utenti e i gruppi locali e alcune informazioni di base.

- **Utente locale**

Un account utente con un identificatore di protezione univoco (SID) che ha visibilità solo sulla macchina virtuale di storage (SVM) su cui è creato. Gli account utente locali dispongono di una serie di attributi, tra cui nome utente e SID. Un account utente locale esegue l'autenticazione locale sul server CIFS utilizzando l'autenticazione NTLM.

Gli account utente possono essere utilizzati in diversi modi:

- Utilizzato per concedere privilegi di *User Rights Management* a un utente.
- Utilizzato per controllare l'accesso a livello di condivisione e di file alle risorse di file e cartelle di proprietà della SVM.

- **Gruppo locale**

Un gruppo con un SID univoco ha visibilità solo sulla SVM su cui è creato. I gruppi contengono un insieme di membri. I membri possono essere utenti locali, utenti di dominio, gruppi di dominio e account di computer di dominio. I gruppi possono essere creati, modificati o cancellati.

I gruppi hanno diversi utilizzi:

- Utilizzato per concedere privilegi a *User Rights Management* ai propri membri.
- Utilizzato per controllare l'accesso a livello di condivisione e di file alle risorse di file e cartelle di proprietà della SVM.

- **Dominio locale**

Dominio con ambito locale, delimitato dalla SVM. Il nome del dominio locale è il nome del server CIFS. Gli utenti e i gruppi locali sono contenuti all'interno del dominio locale.

- **Identificatore di sicurezza (SID)**

Un SID è un valore numerico di lunghezza variabile che identifica le entità di protezione di tipo Windows. Ad esempio, un SID tipico assume la seguente forma: S-1-5-21-3139654847-1303905135-2517279418-123456.

- **Autenticazione NTLM**

Metodo di protezione Microsoft Windows utilizzato per autenticare gli utenti su un server CIFS.

- **Cluster Replicated Database (RDB)**

Database replicato con un'istanza su ciascun nodo di un cluster. Gli oggetti utente e gruppo locali vengono memorizzati nell'RDB.

## **Motivi per la creazione di utenti locali e gruppi locali**

Esistono diversi motivi per creare utenti locali e gruppi locali sulla macchina virtuale di storage (SVM). Ad esempio, è possibile accedere a un server SMB utilizzando un account utente locale se i controller di dominio (DC) non sono disponibili, se si desidera utilizzare gruppi locali per assegnare privilegi o se il server SMB si trova in un gruppo di lavoro.

È possibile creare uno o più account utente locali per i seguenti motivi:

- Il server SMB si trova in un gruppo di lavoro e gli utenti di dominio non sono disponibili.

Nelle configurazioni dei gruppi di lavoro sono richiesti utenti locali.

- Se i controller di dominio non sono disponibili, si desidera eseguire l'autenticazione e l'accesso al server SMB.

Gli utenti locali possono autenticarsi con il server SMB utilizzando l'autenticazione NTLM quando il controller di dominio non è attivo o quando i problemi di rete impediscono al server SMB di contattare il controller di dominio.

- Si desidera assegnare i privilegi di *User Rights Management* a un utente locale.

*User Rights Management* è la capacità di un amministratore del server SMB di controllare i diritti degli

utenti e dei gruppi sulla SVM. È possibile assegnare i privilegi a un utente assegnando i privilegi all'account dell'utente o facendo in modo che l'utente sia membro di un gruppo locale che dispone di tali privilegi.

È possibile creare uno o più gruppi locali per i seguenti motivi:

- Il server SMB si trova in un gruppo di lavoro e i gruppi di dominio non sono disponibili.

I gruppi locali non sono richiesti nelle configurazioni dei gruppi di lavoro, ma possono essere utili per la gestione dei privilegi di accesso per gli utenti dei gruppi di lavoro locali.

- Si desidera controllare l'accesso alle risorse di file e cartelle utilizzando gruppi locali per il controllo della condivisione e dell'accesso ai file.
- Si desidera creare gruppi locali con privilegi personalizzati di *User Rights Management*.

Alcuni gruppi di utenti integrati dispongono di privilegi predefiniti. Per assegnare un set personalizzato di privilegi, è possibile creare un gruppo locale e assegnare i privilegi necessari a tale gruppo. È quindi possibile aggiungere utenti locali, utenti di dominio e gruppi di dominio al gruppo locale.

## Informazioni correlate

[Come funziona l'autenticazione utente locale](#)

[Elenco dei privilegi supportati](#)

## Come funziona l'autenticazione utente locale

Prima che un utente locale possa accedere ai dati su un server CIFS, l'utente deve creare una sessione autenticata.

Poiché SMB è basato sulla sessione, l'identità dell'utente può essere determinata una sola volta, quando la sessione viene configurata per la prima volta. Il server CIFS utilizza l'autenticazione basata su NTLM per l'autenticazione degli utenti locali. Sono supportati sia NTLMv1 che NTLMv2.

ONTAP utilizza l'autenticazione locale in tre casi di utilizzo. Ogni caso di utilizzo dipende dal fatto che la parte di dominio del nome utente (con il formato DOMINIO/utente) corrisponda al nome di dominio locale del server CIFS (il nome del server CIFS):

- La parte di dominio corrisponde

Gli utenti che forniscono credenziali utente locali quando richiedono l'accesso ai dati vengono autenticati localmente sul server CIFS.

- La porzione di dominio non corrisponde

ONTAP tenta di utilizzare l'autenticazione NTLM con un controller di dominio nel dominio a cui appartiene il server CIFS. Se l'autenticazione ha esito positivo, l'accesso è completo. In caso contrario, ciò che accade in seguito dipende dal motivo per cui l'autenticazione non ha avuto esito positivo.

Ad esempio, se l'utente esiste in Active Directory ma la password non è valida o è scaduta, ONTAP non tenta di utilizzare l'account utente locale corrispondente sul server CIFS. Al contrario, l'autenticazione non riesce. In altri casi, ONTAP utilizza l'account locale corrispondente sul server CIFS, se esistente, per l'autenticazione, anche se i nomi di dominio NetBIOS non corrispondono. Ad esempio, se esiste un account di dominio corrispondente ma è disattivato, ONTAP utilizza l'account locale corrispondente sul

server CIFS per l'autenticazione.

- La porzione di dominio non è specificata

ONTAP tenta innanzitutto l'autenticazione come utente locale. Se l'autenticazione come utente locale non riesce, ONTAP autentica l'utente con un controller di dominio nel dominio a cui appartiene il server CIFS.

Una volta completata correttamente l'autenticazione dell'utente locale o di dominio, ONTAP crea un token di accesso utente completo, che tiene conto dell'appartenenza al gruppo locale e dei privilegi.

Per ulteriori informazioni sull'autenticazione NTLM per gli utenti locali, consultare la documentazione di Microsoft Windows.

## Informazioni correlate

[Attivazione o disattivazione dell'autenticazione utente locale](#)

## Come vengono costruiti i token di accesso degli utenti

Quando un utente mappa una condivisione, viene stabilita una sessione SMB autenticata e viene creato un token di accesso utente che contiene informazioni sull'utente, l'appartenenza al gruppo dell'utente e i privilegi cumulativi e l'utente UNIX mappato.

A meno che la funzionalità non sia disattivata, al token di accesso dell'utente vengono aggiunte anche le informazioni relative all'utente locale e al gruppo. La modalità di creazione dei token di accesso dipende dal fatto che l'accesso sia destinato a un utente locale o a un utente di dominio Active Directory:

- Accesso utente locale

Sebbene gli utenti locali possano essere membri di diversi gruppi locali, i gruppi locali non possono essere membri di altri gruppi locali. Il token di accesso dell'utente locale è composto da un'Unione di tutti i privilegi assegnati ai gruppi a cui è membro un particolare utente locale.

- Login utente di dominio

Quando un utente di dominio effettua l'accesso, ONTAP ottiene un token di accesso utente che contiene il SID e i SID dell'utente per tutti i gruppi di dominio a cui l'utente è membro. ONTAP utilizza l'Unione del token di accesso dell'utente di dominio con il token di accesso fornito dalle appartenenze locali dei gruppi di dominio dell'utente (se presenti), nonché qualsiasi privilegio diretto assegnato all'utente di dominio o a una qualsiasi delle sue appartenenze ai gruppi di dominio.

Per l'accesso dell'utente locale e di dominio, viene impostato anche l'RID del gruppo primario per il token di accesso dell'utente. L'RID predefinito è `Domain Users` (RID 513). Non è possibile modificare l'impostazione predefinita.

Il processo di mappatura dei nomi da Windows a UNIX e da UNIX a Windows segue le stesse regole per gli account locali e di dominio.



Non esiste alcuna mappatura automatica implicita da un utente UNIX a un account locale. Se necessario, è necessario specificare una regola di mappatura esplicita utilizzando i comandi di mappatura dei nomi esistenti.



## Linee guida per l'utilizzo di SnapMirror su SVM che contengono gruppi locali

È necessario conoscere le linee guida per la configurazione di SnapMirror su volumi di proprietà di SVM che contengono gruppi locali.

Non è possibile utilizzare gruppi locali nelle ACE applicate a file, directory o condivisioni replicate da SnapMirror su un'altra SVM. Se si utilizza la funzione SnapMirror per creare un mirror DR su un volume su un altro SVM e il volume dispone di un ACE per un gruppo locale, l'ACE non è valido sul mirror. Se i dati vengono replicati su una SVM diversa, i dati vengono effettivamente trasferiti in un dominio locale diverso. Le autorizzazioni concesse agli utenti e ai gruppi locali sono valide solo nell'ambito della SVM in cui sono stati creati originariamente.

### Cosa accade agli utenti e ai gruppi locali quando si eliminano i server CIFS

Il set predefinito di utenti e gruppi locali viene creato quando viene creato un server CIFS e sono associati alla macchina virtuale di storage (SVM) che ospita il server CIFS. Gli amministratori di SVM possono creare utenti e gruppi locali in qualsiasi momento. È necessario essere consapevoli di ciò che accade agli utenti e ai gruppi locali quando si elimina il server CIFS.

Gli utenti e i gruppi locali sono associati alle SVM; pertanto, non vengono cancellati quando i server CIFS vengono cancellati a causa di considerazioni di sicurezza. Anche se gli utenti e i gruppi locali non vengono cancellati quando il server CIFS viene cancellato, essi sono nascosti. Non è possibile visualizzare o gestire utenti e gruppi locali fino a quando non viene ricreato un server CIFS su SVM.



Lo stato amministrativo del server CIFS non influisce sulla visibilità degli utenti o dei gruppi locali.

### Come utilizzare Microsoft Management Console con utenti e gruppi locali

È possibile visualizzare informazioni su utenti e gruppi locali dalla console di gestione Microsoft. Con questa versione di ONTAP, non è possibile eseguire altre attività di gestione per utenti e gruppi locali dalla console di gestione Microsoft.

### Linee guida per il ripristino

Se si prevede di ripristinare il cluster a una release di ONTAP che non supporta utenti e gruppi locali e utenti e gruppi locali vengono utilizzati per gestire l'accesso ai file o i diritti utente, è necessario tenere presente alcune considerazioni.

- A causa di motivi di sicurezza, le informazioni relative a utenti, gruppi e privilegi locali configurati non vengono eliminate quando ONTAP viene reimpostato su una versione che non supporta la funzionalità di utenti e gruppi locali.
- In caso di ripristino di una versione principale precedente di ONTAP, ONTAP non utilizza utenti e gruppi locali durante l'autenticazione e la creazione delle credenziali.
- Gli utenti e i gruppi locali non vengono rimossi dagli ACL di file e cartelle.
- Le richieste di accesso ai file che dipendono dall'accesso concesso a causa delle autorizzazioni concesse agli utenti o ai gruppi locali vengono negate.

Per consentire l'accesso, è necessario riconfigurare le autorizzazioni dei file in modo da consentire

l'accesso in base agli oggetti di dominio anziché agli oggetti utente e gruppo locali.

## Quali sono i privilegi locali

### Elenco dei privilegi supportati

ONTAP dispone di un set predefinito di privilegi supportati. Per impostazione predefinita, alcuni gruppi locali predefiniti dispongono di alcuni di questi privilegi. È inoltre possibile aggiungere o rimuovere privilegi dai gruppi predefiniti o creare nuovi utenti o gruppi locali e aggiungere privilegi ai gruppi creati o a utenti e gruppi di dominio esistenti.

La seguente tabella elenca i privilegi supportati sulla macchina virtuale di storage (SVM) e fornisce un elenco di gruppi BUILTIN con privilegi assegnati:

Nome privilegio	Impostazione di sicurezza predefinita	Descrizione
SeTcbPrivilege	Nessuno	Agire come parte del sistema operativo
SeBackupPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Eseguire il backup di file e directory, sovrascrivendo eventuali ACL
SeRestorePrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators	Ripristinare file e directory, sovrascrivendo gli ACL, impostare qualsiasi SID utente o gruppo valido come proprietario del file
SeTakeOwnershipPrivilege	BUILTIN\Administrators	Assumere la proprietà di file o altri oggetti
SeSecurityPrivilege	BUILTIN\Administrators	Gestire il controllo  Ciò include la visualizzazione, lo scarico e la cancellazione del registro di protezione.
SeChangeNotifyPrivilege	BUILTIN\Administrators, BUILTIN\Backup Operators, BUILTIN\Power Users, BUILTIN\Users, Everyone	Bypass controllo traversa  Agli utenti con questo privilegio non è richiesto di disporre di autorizzazioni trasversali (x) per attraversare cartelle, collegamenti simbolici o giunzioni.

### Informazioni correlate

- [Assegnare privilegi locali](#)
- [Configurazione del controllo incrociato bypass](#)

## Assegnare privilegi

È possibile assegnare i privilegi direttamente agli utenti locali o agli utenti di dominio. In alternativa, è possibile assegnare utenti a gruppi locali i cui privilegi assegnati corrispondono alle funzionalità desiderate per tali utenti.

- È possibile assegnare un set di privilegi a un gruppo creato.

Quindi, aggiungere un utente al gruppo che dispone dei privilegi che si desidera assegnare a tale utente.

- È inoltre possibile assegnare utenti locali e utenti di dominio a gruppi predefiniti i cui privilegi predefiniti corrispondono ai privilegi che si desidera concedere a tali utenti.

### Informazioni correlate

- [Aggiunta di privilegi a utenti o gruppi locali o di dominio](#)
- [Rimozione dei privilegi da utenti o gruppi locali o di dominio](#)
- [Reimpostazione dei privilegi per utenti e gruppi locali o di dominio](#)
- [Configurazione del controllo incrociato bypass](#)

### Linee guida per l'utilizzo dei gruppi BUILTIN e dell'account amministratore locale

Esistono alcune linee guida da tenere presenti quando si utilizzano i gruppi BUILTIN e l'account amministratore locale. Ad esempio, è possibile rinominare l'account amministratore locale, ma non è possibile eliminarlo.

- L'account Administrator può essere rinominato ma non eliminato.
- Impossibile rimuovere l'account Administrator dal gruppo BUILTIN/Administrators.
- I gruppi INCORPORATI possono essere rinominati ma non eliminati.

Dopo aver rinominato il gruppo BUILTIN, è possibile creare un altro oggetto locale con il nome noto; tuttavia, all'oggetto viene assegnato un nuovo RID.

- Nessun account Guest locale.

### Informazioni correlate

[Gruppi BUILTIN predefiniti e privilegi predefiniti](#)

### Requisiti per le password dell'utente locale

Per impostazione predefinita, le password degli utenti locali devono soddisfare i requisiti di complessità. I requisiti di complessità delle password sono simili ai requisiti definiti nella *policy di sicurezza locale* di Microsoft Windows.

La password deve soddisfare i seguenti criteri:

- Deve essere composto da almeno sei caratteri
- Non deve contenere il nome dell'account utente
- Deve contenere almeno tre caratteri delle seguenti quattro categorie:
  - Caratteri maiuscoli inglesi (Dalla A alla Z)

- Caratteri minuscoli inglesi (da a a z)
- Base 10 cifre (da 0 a 9)
- Caratteri speciali:  
~! @ ` % ^ & \* \_ - + = / | ( ) [ ] : ; " < > , . ? /

Informazioni correlate

[Attivazione o disattivazione della complessità della password richiesta per gli utenti SMB locali](#)

[Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS](#)

[Modifica delle password degli account utente locali](#)

Gruppi BUILTIN predefiniti e privilegi predefiniti

È possibile assegnare l'appartenenza di un utente locale o di un utente di dominio a un set predefinito di gruppi BUILTIN forniti da ONTAP. Ai gruppi predefiniti sono assegnati privilegi predefiniti.

La seguente tabella descrive i gruppi predefiniti:

Gruppo BUILTIN predefinito	Privilegi predefiniti
<p>BUILTIN\AdministratorsRID 544</p> <p>Quando viene creato per la prima volta, il locale Administrator L'account, con un RID di 500, viene automaticamente reso membro di questo gruppo. Quando la macchina virtuale di storage (SVM) viene unita a un dominio, il domain\Domain Admins il gruppo viene aggiunto al gruppo. Se SVM lascia il dominio, il domain\Domain Admins il gruppo viene rimosso dal gruppo.</p>	<ul style="list-style-type: none"> <li>• SeBackupPrivilege</li> <li>• SeRestorePrivilege</li> <li>• SeSecurityPrivilege</li> <li>• SeTakeOwnershipPrivilege</li> <li>• SeChangeNotifyPrivilege</li> </ul>
<p>BUILTIN\Power UsersRID 547</p> <p>Quando viene creato per la prima volta, questo gruppo non ha membri. I membri di questo gruppo hanno le seguenti caratteristiche:</p> <ul style="list-style-type: none"> <li>• Può creare e gestire utenti e gruppi locali.</li> <li>• Impossibile aggiungere se stessi o altri oggetti a BUILTIN\Administrators gruppo.</li> </ul>	<p>SeChangeNotifyPrivilege</p>

Gruppo BUILTIN predefinito	Privilegi predefiniti
BUILTIN\Backup OperatorsRID 551  Quando viene creato per la prima volta, questo gruppo non ha membri. I membri di questo gruppo possono sovrascrivere i permessi di lettura e scrittura su file o cartelle se vengono aperti con finalità di backup.	<ul style="list-style-type: none"> <li>• SeBackupPrivilege</li> <li>• SeRestorePrivilege</li> <li>• SeChangeNotifyPrivilege</li> </ul>
BUILTIN\UsersRID 545  Quando creato per la prima volta, questo gruppo non ha membri (oltre a quelli impliciti Authenticated Users gruppo speciale). Quando la SVM viene unita a un dominio, la domain\Domain Users il gruppo viene aggiunto a questo gruppo. Se SVM lascia il dominio, il domain\Domain Users il gruppo viene rimosso da questo gruppo.	SeChangeNotifyPrivilege
EveryoneSID S-1-1-0  Questo gruppo include tutti gli utenti, inclusi gli utenti guest (ma non gli utenti anonimi). Si tratta di un gruppo implicito con un'appartenenza implicita.	SeChangeNotifyPrivilege

### Informazioni correlate

[Linee guida per l'utilizzo dei gruppi BUILTIN e dell'account amministratore locale](#)

[Elenco dei privilegi supportati](#)

[Configurazione del controllo incrociato bypass](#)

### Attiva o disattiva la funzionalità di utenti e gruppi locali

#### Attivare o disattivare la panoramica delle funzionalità di utenti e gruppi locali

Prima di poter utilizzare utenti e gruppi locali per il controllo dell'accesso ai dati di sicurezza NTFS, è necessario attivare la funzionalità locale di utenti e gruppi. Inoltre, se si desidera utilizzare gli utenti locali per l'autenticazione SMB, è necessario attivare la funzionalità di autenticazione dell'utente locale.

Per impostazione predefinita, le funzionalità degli utenti e dei gruppi locali e l'autenticazione dell'utente locale sono attivate. Se non sono abilitati, è necessario abilitarli prima di poter configurare e utilizzare utenti e gruppi locali. È possibile disattivare la funzionalità di utenti e gruppi locali in qualsiasi momento.

Oltre a disattivare esplicitamente le funzionalità di utenti e gruppi locali, ONTAP disattiva le funzionalità di utenti e gruppi locali se un nodo del cluster viene reimpresso in una release di ONTAP che non supporta tale funzionalità. La funzionalità utente e gruppo locale non viene attivata finché tutti i nodi del cluster non eseguono una versione di ONTAP che la supporta.

## Informazioni correlate

[Modificare gli account utente locali](#)

[Modificare i gruppi locali](#)

[Aggiungere privilegi a utenti o gruppi locali o di dominio](#)

## Attivare o disattivare utenti e gruppi locali

È possibile attivare o disattivare utenti e gruppi locali per l'accesso SMB sulle macchine virtuali di storage (SVM). La funzionalità utenti e gruppi locali è attivata per impostazione predefinita.

### A proposito di questa attività

È possibile utilizzare utenti e gruppi locali durante la configurazione delle autorizzazioni di condivisione SMB e file NTFS e, facoltativamente, utilizzare utenti locali per l'autenticazione quando si crea una connessione SMB. Per utilizzare gli utenti locali per l'autenticazione, è necessario attivare anche l'opzione di autenticazione degli utenti e dei gruppi locali.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera che utenti e gruppi locali siano...	Immettere il comando...
Attivato	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false</code>

3. Tornare al livello di privilegio admin: `set -privilege admin`

### Esempio

L'esempio seguente abilita le funzionalità di utenti e gruppi locali su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

## Informazioni correlate

[Attiva o disattiva l'autenticazione utente locale](#)

[Attivare o disattivare gli account utente locali](#)

### Attiva o disattiva l'autenticazione utente locale

È possibile attivare o disattivare l'autenticazione utente locale per l'accesso SMB sulle macchine virtuali di storage (SVM). L'impostazione predefinita prevede l'autenticazione dell'utente locale, utile quando SVM non è in grado di contattare un controller di dominio o se si sceglie di non utilizzare i controlli di accesso a livello di dominio.

#### Prima di iniziare

La funzionalità di utenti e gruppi locali deve essere attivata sul server CIFS.

#### A proposito di questa attività

È possibile attivare o disattivare l'autenticazione utente locale in qualsiasi momento. Se si desidera utilizzare utenti locali per l'autenticazione durante la creazione di una connessione SMB, è necessario attivare anche l'opzione utenti e gruppi locali del server CIFS.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera che l'autenticazione locale sia...	Immettere il comando...
Attivato	<pre>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled true</pre>
Disattivato	<pre>vserver cifs options modify -vserver vserver_name -is-local-auth-enabled false</pre>

3. Tornare al livello di privilegio admin: `set -privilege admin`

#### Esempio

L'esempio seguente abilita l'autenticazione dell'utente locale su SVM vs1:

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

## Informazioni correlate

[Come funziona l'autenticazione utente locale](#)

[Attivazione o disattivazione di utenti e gruppi locali](#)

**Gestire gli account utente locali**

### Modificare gli account utente locali

È possibile modificare un account utente locale se si desidera modificare il nome completo o la descrizione di un utente esistente e se si desidera attivare o disattivare l'account utente. È inoltre possibile rinominare un account utente locale se il nome dell'utente è compromesso o se è necessario modificare il nome per scopi amministrativi.

Se si desidera...	Immettere il comando...
Modificare il nome completo dell'utente locale	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -full-name text</code> Se il nome completo contiene uno spazio, deve essere racchiuso tra virgolette doppie.
Modificare la descrizione dell'utente locale	<code>vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user -name <i>user_name</i> -description text</code> Se la descrizione contiene uno spazio, deve essere racchiusa tra virgolette doppie.
Attivare o disattivare l'account utente locale	<code>`vserver cifs users-and-groups local-user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is -account-disabled {true</code>
<code>false}`</code>	Rinominare l'account utente locale

### Esempio

Nell'esempio seguente l'utente locale "CIFS\_SERVER` sue" viene rinomina in "CIFS\_SERVER sue\_new" sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:



```
cluster1::> vserver cifs users-and-groups local-user rename -user-name  
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

## Attivare o disattivare gli account utente locali

Attivare un account utente locale se si desidera che l'utente possa accedere ai dati contenuti nella macchina virtuale di storage (SVM) tramite una connessione SMB. È inoltre possibile disattivare un account utente locale se non si desidera che l'utente acceda ai dati SVM tramite SMB.

### A proposito di questa attività

Per abilitare un utente locale, modificare l'account utente.

### Fase

1. Eseguire l'azione appropriata:

Se si desidera...	Immettere il comando...
Attivare l'account utente	<pre>vserver cifs users-and-groups local- user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is-account -disabled false</pre>
Disattivare l'account utente	<pre>vserver cifs users-and-groups local- user modify -vserver <i>vserver_name</i> -user-name <i>user_name</i> -is-account -disabled true</pre>

## Modificare le password dell'account utente locale

È possibile modificare la password dell'account di un utente locale. Ciò può essere utile se la password dell'utente viene compromessa o se l'utente ha dimenticato la password.

### Fase

1. Modificare la password eseguendo l'azione appropriata: 

```
vserver cifs users-and-groups local-  
user set-password -vserver vserver_name -user-name user_name
```

### Esempio

Nell'esempio seguente viene impostata la password per l'utente locale "CIFS\_SERVER\ sue" associato alla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vsserver cifs users-and-groups local-user set-password -user  
-name CIFS_SERVER\sue -vsserver vs1
```

Enter the new password:

Confirm the new password:

## Informazioni correlate

[Attivazione o disattivazione della complessità della password richiesta per gli utenti SMB locali](#)

[Visualizzazione delle informazioni sulle impostazioni di sicurezza del server CIFS](#)

## Visualizza le informazioni sugli utenti locali

È possibile visualizzare un elenco di tutti gli utenti locali in un modulo riepilogativo. Se si desidera determinare quali impostazioni dell'account sono configurate per un utente specifico, è possibile visualizzare informazioni dettagliate sull'account per tale utente, nonché informazioni sull'account per più utenti. Queste informazioni consentono di determinare se è necessario modificare le impostazioni di un utente e risolvere i problemi di autenticazione o di accesso ai file.

## A proposito di questa attività

Le informazioni relative alla password di un utente non vengono mai visualizzate.

## Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Visualizzare le informazioni su tutti gli utenti sulla macchina virtuale per lo storage (SVM)	<code>vsserver cifs users-and-groups local-user show -vsserver vsserver_name</code>
Visualizza informazioni dettagliate sull'account di un utente	<code>vsserver cifs users-and-groups local-user show -instance -vsserver vsserver_name -user-name user_name</code>

Quando si esegue il comando, è possibile scegliere altri parametri opzionali. Per ulteriori informazioni, consulta la pagina man.

## Esempio

Nell'esempio seguente vengono visualizzate informazioni su tutti gli utenti locali su SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                               Full Name      Description
-----  -
vs1      CIFS_SERVER\Administrator      James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue                Sue    Jones
```

### Visualizza le informazioni sulle appartenenze ai gruppi per gli utenti locali

È possibile visualizzare informazioni sui gruppi locali a cui appartiene un utente locale. È possibile utilizzare queste informazioni per determinare l'accesso dell'utente a file e cartelle. Queste informazioni possono essere utili per determinare i diritti di accesso che l'utente deve avere a file e cartelle o per risolvere i problemi di accesso ai file.

#### A proposito di questa attività

È possibile personalizzare il comando per visualizzare solo le informazioni desiderate.

#### Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera...	Immettere il comando...
Visualizza le informazioni di appartenenza dell'utente locale per un utente locale specificato	<code>vserver cifs users-and-groups local-user show-membership -user-name <i>user_name</i></code>
Visualizza le informazioni di appartenenza dell'utente locale per il gruppo locale di cui l'utente locale è membro	<code>vserver cifs users-and-groups local-user show-membership -membership <i>group_name</i></code>
Visualizzazione delle informazioni di appartenenza degli utenti locali associati a una specifica SVM (Storage Virtual Machine)	<code>vserver cifs users-and-groups local-user show-membership -vserver <i>vserver_name</i></code>
Visualizza informazioni dettagliate per tutti gli utenti locali su una SVM specificata	<code>vserver cifs users-and-groups local-user show-membership -instance -vserver <i>vserver_name</i></code>

#### Esempio

Nell'esempio seguente vengono visualizzate le informazioni di appartenenza per tutti gli utenti locali su SVM vs1; l'utente "CIFS\_SERVER` Administrator" è membro del gruppo "BUILTIN`Administrators" e "CIFS\_SERVER` sue" è membro del gruppo "CIFS\_SERVER g1":

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
```

Vserver	User Name	Membership
vs1	CIFS_SERVER\Administrator	BUILTIN\Administrators
	CIFS_SERVER\sue	CIFS_SERVER\g1

## Eliminare gli account utente locali

È possibile eliminare gli account utente locali dalla macchina virtuale di storage (SVM) se non sono più necessari per l'autenticazione SMB locale al server CIFS o per determinare i diritti di accesso ai dati contenuti nella SVM.

### A proposito di questa attività

Quando si eliminano gli utenti locali, tenere presente quanto segue:

- Il file system non viene modificato.

I descrittori di protezione di Windows su file e directory che fanno riferimento a questo utente non vengono modificati.

- Tutti i riferimenti agli utenti locali vengono rimossi dai database di appartenenza e privilegi.
- Gli utenti standard e noti come Administrator non possono essere eliminati.

### Fasi

1. Determinare il nome dell'account utente locale che si desidera eliminare: `vserver cifs users-and-groups local-user show -vserver vserver_name`
2. Eliminare l'utente locale: `vserver cifs users-and-groups local-user delete -vserver vserver_name -user-name username_name`
3. Verificare che l'account utente sia stato eliminato: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Esempio

Nell'esempio seguente viene eliminato l'utente locale "CIFS\_SERVER\ sue" associato a SVM vs1:

```
cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith             Built-in administrator
account
vs1      CIFS_SERVER\sue           Sue    Jones

cluster1::> vsriver cifs users-and-groups local-user delete -vsriver vs1
-user-name CIFS_SERVER\sue

cluster1::> vsriver cifs users-and-groups local-user show -vsriver vs1
Vserver  User Name                Full Name                Description
-----  -
vs1      CIFS_SERVER\Administrator  James Smith             Built-in administrator
account
```

## Gestire i gruppi locali

### Modificare i gruppi locali

È possibile modificare i gruppi locali esistenti modificando la descrizione di un gruppo locale esistente o rinominando il gruppo.

Se si desidera...	Utilizzare il comando...
Modificare la descrizione del gruppo locale	<code>vsriver cifs users-and-groups local-group modify -vsriver vsriver_name -group-name group_name -description text</code> Se la descrizione contiene uno spazio, deve essere racchiusa tra virgolette doppie.
Rinominare il gruppo locale	<code>vsriver cifs users-and-groups local-group rename -vsriver vsriver_name -group-name group_name -new-group-name new_group_name</code>

### Esempi

Nell'esempio seguente il gruppo locale "CIFS\_SERVER` Engineering" viene rinomina in "CIFS\_SERVER Engineering\_New":

```
cluster1::> vsriver cifs users-and-groups local-group rename -vsriver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

Nell'esempio seguente viene modificata la descrizione del gruppo locale "CIFS\_SERVER\ engineering":

```
cluster1::> vsriver cifs users-and-groups local-group modify -vsriver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

**Visualizza informazioni sui gruppi locali**

È possibile visualizzare un elenco di tutti i gruppi locali configurati sul cluster o su una specifica macchina virtuale di storage (SVM). Queste informazioni possono essere utili per la risoluzione dei problemi di accesso ai file dei dati contenuti nella SVM o dei problemi relativi ai diritti utente (privilegi) sulla SVM.

**Fase**

- 1. Eseguire una delle seguenti operazioni:

Se si desidera ottenere informazioni su...	Immettere il comando...
Tutti i gruppi locali del cluster	<code>vsriver cifs users-and-groups local-group show</code>
Tutti i gruppi locali sulla SVM	<code>vsriver cifs users-and-groups local-group show -vsriver vsriver_name</code>

Quando si esegue questo comando, è possibile scegliere altri parametri opzionali. Per ulteriori informazioni, consulta la pagina man.

**Esempio**

Nell'esempio seguente vengono visualizzate informazioni su tutti i gruppi locali su SVM vs1:

```
cluster1::> vsriver cifs users-and-groups local-group show -vsriver vs1
Vserver  Group Name                                Description
-----  -
vs1      BUILTIN\Administrators                    Built-in Administrators group
vs1      BUILTIN\Backup Operators                  Backup Operators group
vs1      BUILTIN\Power Users                       Restricted administrative privileges
vs1      BUILTIN\Users                             All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

**Gestire l'appartenenza al gruppo locale**

È possibile gestire l'appartenenza a un gruppo locale aggiungendo e rimuovendo utenti locali o di dominio oppure aggiungendo e rimuovendo gruppi di dominio. Questa funzione è utile se si desidera controllare l'accesso ai dati in base ai controlli di accesso posizionati nel gruppo o se si desidera che gli utenti dispongano di privilegi associati a

tale gruppo.

**A proposito di questa attività**

Linee guida per l'aggiunta di membri a un gruppo locale:

- Non è possibile aggiungere utenti al gruppo speciale *Everyone*.
- Il gruppo locale deve esistere prima di poter aggiungere un utente.
- L'utente deve esistere prima di poter aggiungere l'utente a un gruppo locale.
- Non è possibile aggiungere un gruppo locale a un altro gruppo locale.
- Per aggiungere un utente o un gruppo di dominio a un gruppo locale, Data ONTAP deve essere in grado di risolvere il nome in un SID.

Linee guida per la rimozione dei membri da un gruppo locale:

- Non puoi rimuovere membri dal gruppo speciale *Everyone*.
- Il gruppo da cui si desidera rimuovere un membro deve esistere.
- ONTAP deve essere in grado di risolvere i nomi dei membri che si desidera rimuovere dal gruppo in un SID corrispondente.

**Fase**

1. Aggiungere o rimuovere un membro di un gruppo.

Se si desidera...	Quindi utilizzare il comando...
Aggiungere un membro a un gruppo	<pre>vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da aggiungere al gruppo locale specificato.</p>
Rimuovere un membro da un gruppo	<pre>vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]</pre> <p>È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da rimuovere dal gruppo locale specificato.</p>

Nell'esempio seguente vengono aggiunti un utente locale "SMB\_SERVER` sue" e un gruppo di domini "ad\_DOM `Sdom\_eng" al gruppo locale "MB\_SERVER engineering" su SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

Nell'esempio seguente vengono rimossi gli utenti locali "SMB\_SERVER` sue" e "SMB\_SERVER `Sjames"

dal gruppo locale "MB\_SERVER engineering" su SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

Informazioni correlate

[Visualizzazione delle informazioni sui membri dei gruppi locali](#)

Visualizza le informazioni sui membri dei gruppi locali

È possibile visualizzare un elenco di tutti i membri dei gruppi locali configurati sul cluster o su una specifica macchina virtuale di storage (SVM). Queste informazioni possono essere utili per la risoluzione dei problemi di accesso ai file o di diritti dell'utente (privilegio).

Fase

- 1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su...	Immettere il comando...
Membri di tutti i gruppi locali del cluster	vserver cifs users-and-groups local-group show-members
Membri di tutti i gruppi locali sulla SVM	vserver cifs users-and-groups local-group show-members -vserver vserver_name

Esempio

Nell'esempio seguente vengono visualizzate informazioni sui membri di tutti i gruppi locali su SVM vs1:

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver      Group Name                Members
-----
vs1          BUILTIN\Administrators    CIFS_SERVER\Administrator
                                     AD_DOMAIN\Domain Admins
                                     AD_DOMAIN\dom_grpl
                                     BUILTIN\Users
                                     AD_DOMAIN\Domain Users
                                     AD_DOMAIN\dom_usr1
                                     CIFS_SERVER\engineering
                                     CIFS_SERVER\james
```



## Eliminare un gruppo locale

È possibile eliminare un gruppo locale dalla macchina virtuale di storage (SVM) se non è più necessario per determinare i diritti di accesso ai dati associati a tale SVM o se non è più necessario per assegnare i diritti utente (privilegi) di SVM ai membri del gruppo.

### A proposito di questa attività

Quando si eliminano gruppi locali, tenere presente quanto segue:

- Il file system non viene modificato.

I descrittori di protezione di Windows su file e directory che fanno riferimento a questo gruppo non vengono modificati.

- Se il gruppo non esiste, viene restituito un errore.
- Impossibile eliminare il gruppo speciale *Everyone*.
- I gruppi incorporati come *BUILTIN/Administrators* *BUILTIN/Users* non possono essere eliminati.

### Fasi

1. Determinare il nome del gruppo locale che si desidera eliminare visualizzando l'elenco dei gruppi locali sulla SVM: `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. Eliminare il gruppo locale: `vserver cifs users-and-groups local-group delete -vserver vserver_name -group-name group_name`
3. Verificare che il gruppo sia stato eliminato: `vserver cifs users-and-groups local-user show -vserver vserver_name`

### Esempio

Nell'esempio seguente viene eliminato il gruppo locale "'CIFS\_SERVER` sales" associato a SVM vs1:

```

cluster1::> vsriver cifs users-and-groups local-group show -vsriver vs1
Vserver      Group Name                Description
-----
vs1          BUILTIN\Administrators    Built-in Administrators group
vs1          BUILTIN\Backup Operators  Backup Operators group
vs1          BUILTIN\Power Users       Restricted administrative
privileges
vs1          BUILTIN\Users             All users
vs1          CIFS_SERVER\engineering
vs1          CIFS_SERVER\sales

cluster1::> vsriver cifs users-and-groups local-group delete -vsriver vs1
-group-name CIFS_SERVER\sales

cluster1::> vsriver cifs users-and-groups local-group show -vsriver vs1
Vserver      Group Name                Description
-----
vs1          BUILTIN\Administrators    Built-in Administrators group
vs1          BUILTIN\Backup Operators  Backup Operators group
vs1          BUILTIN\Power Users       Restricted administrative
privileges
vs1          BUILTIN\Users             All users
vs1          CIFS_SERVER\engineering

```

### Aggiornare i nomi degli utenti e dei gruppi di dominio nei database locali

È possibile aggiungere utenti e gruppi di dominio ai gruppi locali di un server CIFS. Questi oggetti di dominio vengono registrati nei database locali del cluster. Se un oggetto di dominio viene rinominato, i database locali devono essere aggiornati manualmente.

#### A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) su cui si desidera aggiornare i nomi di dominio.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire l'azione appropriata:

Se si desidera aggiornare utenti e gruppi di dominio e...	Utilizzare questo comando...
Visualizza gli utenti e i gruppi di dominio che hanno eseguito l'aggiornamento e che non sono riusciti ad aggiornare	<code>vsriver cifs users-and-groups update-names -vsriver vsriver_name</code>

Se si desidera aggiornare utenti e gruppi di dominio e...	Utilizzare questo comando...
Visualizzare gli utenti e i gruppi di dominio che sono stati aggiornati correttamente	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false</code>
Visualizzare solo gli utenti e i gruppi di dominio che non riescono ad aggiornare	<code>vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true</code>
Elimina tutte le informazioni di stato relative agli aggiornamenti	<code>vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true</code>

3. Tornare al livello di privilegio admin: `set -privilege admin`

### Esempio

Nell'esempio riportato di seguito vengono aggiornati i nomi degli utenti e dei gruppi di dominio associati alla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1. Per l'ultimo aggiornamento, è necessario aggiornare una catena di nomi dipendente:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs users-and-groups update-names -vsserver vs1

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-12345
Domain:           EXAMPLE1
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654322-23456
Domain:           EXAMPLE2
Out-of-date Name: dom_user1
Updated Name:     dom_user2
Status:           Successfully updated

Vserver:          vs1
SID:              S-1-5-21-123456789-234565432-987654321-123456
Domain:           EXAMPLE1
Out-of-date Name: dom_user3
Updated Name:     dom_user4
Status:           Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                  to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                  to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                  to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                  to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin

```

## Gestire i privilegi locali

## Aggiungere privilegi a utenti o gruppi locali o di dominio

È possibile gestire i diritti utente per utenti o gruppi locali o di dominio aggiungendo privilegi. I privilegi aggiunti sovrascrivono i privilegi predefiniti assegnati a uno di questi oggetti. In questo modo è possibile migliorare la sicurezza, consentendo di personalizzare i privilegi di un utente o di un gruppo.

### Prima di iniziare

L'utente o il gruppo locale o di dominio a cui verranno aggiunti i privilegi deve già esistere.

### A proposito di questa attività

L'aggiunta di un privilegio a un oggetto sovrascrive i privilegi predefiniti per quell'utente o gruppo. L'aggiunta di un privilegio non rimuove i privilegi aggiunti in precedenza.

Quando si aggiungono privilegi a utenti o gruppi locali o di dominio, è necessario tenere presente quanto segue:

- È possibile aggiungere uno o più privilegi.
- Quando si aggiungono privilegi a un utente o a un gruppo di dominio, ONTAP può validare l'utente o il gruppo di dominio contattando il controller di dominio.

Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

### Fasi

1. Aggiungere uno o più privilegi a un utente o a un gruppo locale o di dominio: `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. Verificare che i privilegi desiderati siano applicati all'oggetto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Esempio

Nell'esempio seguente vengono aggiunti i privilegi "SeTcbPrivilege" e "SeTakeOwnershipPrivilege" all'utente "CIFS\_SERVER\sue" sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          CIFS_SERVER\sue        SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

## Rimuovere i privilegi da utenti o gruppi locali o di dominio

È possibile gestire i diritti utente per utenti o gruppi locali o di dominio rimuovendo i privilegi. In questo modo è possibile migliorare la sicurezza, consentendo di

personalizzare i privilegi massimi di utenti e gruppi.

### Prima di iniziare

L'utente o il gruppo locale o di dominio da cui verranno rimossi i privilegi deve già esistere.

### A proposito di questa attività

Quando si rimuovono privilegi da utenti o gruppi locali o di dominio, è necessario tenere presente quanto segue:

- È possibile rimuovere uno o più privilegi.
- Quando si rimuovono i privilegi da un utente o gruppo di dominio, ONTAP può validare l'utente o il gruppo di dominio contattando il controller di dominio.

Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

### Fasi

1. Rimuovere uno o più privilegi da un utente o gruppo locale o di dominio: `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. Verificare che i privilegi desiderati siano stati rimossi dall'oggetto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Esempio

Nell'esempio seguente vengono rimossi i privilegi "SeTcbPrivilege" e "SeTakeOwnershipPrivilege" dall'utente "CIFS\_SERVER\sue" sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name    Privileges
-----
vs1        CIFS_SERVER\sue     -
```

### Ripristinare i privilegi per utenti e gruppi locali o di dominio

È possibile reimpostare i privilegi per utenti e gruppi locali o di dominio. Ciò può risultare utile quando si apportano modifiche ai privilegi di un utente o di un gruppo locale o di dominio e tali modifiche non sono più richieste o necessarie.

## A proposito di questa attività

La reimpostazione dei privilegi per un utente o un gruppo locale o di dominio rimuove eventuali voci di privilegio per tale oggetto.

### Fasi

1. Ripristinare i privilegi di un utente o di un gruppo locale o di dominio: `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`
2. Verificare che i privilegi siano ripristinati sull'oggetto: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Esempi

Nell'esempio seguente vengono ripristinati i privilegi dell'utente "CIFS\_SERVER\sue" sulla macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1. Per impostazione predefinita, gli utenti normali non dispongono di privilegi associati ai propri account:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        CIFS_SERVER\sue        SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Nell'esempio riportato di seguito vengono ripristinati i privilegi per il gruppo "BUILTIN\Administrators", rimuovendo in modo efficace la voce di privilegio:

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver    User or Group Name      Privileges
-----
vs1        BUILTIN\Administrators  SeRestorePrivilege
                                SeSecurityPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

Visualizza le informazioni sugli override dei privilegi

È possibile visualizzare informazioni sui privilegi personalizzati assegnati agli account o ai gruppi di utenti locali o di dominio. Queste informazioni consentono di determinare se vengono applicati i diritti utente desiderati.

Fase

- 1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare informazioni su...	Immettere questo comando...
Privilegi personalizzati per tutti gli utenti e i gruppi locali e di dominio sulla macchina virtuale di storage (SVM)	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i></code>
Privilegi personalizzati per un dominio o un utente e gruppo locale specifico sulla SVM	<code>vserver cifs users-and-groups privilege show -vserver <i>vserver_name</i> -user-or-group-name <i>name</i></code>

Quando si esegue questo comando, è possibile scegliere altri parametri opzionali. Per ulteriori informazioni, consulta la pagina man.

Esempio

Il seguente comando visualizza tutti i privilegi esplicitamente associati agli utenti e ai gruppi locali o di dominio per SVM vs1:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver      User or Group Name      Privileges
-----
vs1          BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1          CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

Configurare il controllo incrociato del bypass

Configurare la panoramica del controllo incrociato del bypass

Il controllo incrociato del bypass è un diritto utente (noto anche come *privilegio*) che determina se un utente può attraversare tutte le directory nel percorso verso un file anche se l'utente non dispone delle autorizzazioni per la directory attraversata. È necessario comprendere cosa accade quando si consente o non si consente il controllo incrociato del bypass e come configurare il controllo incrociato del bypass per gli utenti sulle macchine virtuali di storage (SVM).



## Cosa accade quando si consente o si non si consente il controllo incrociato del bypass

- Se consentito, quando un utente tenta di accedere a un file, ONTAP non controlla l'autorizzazione di attraversamento per le directory intermedie quando determina se concedere o negare l'accesso al file.
- Se non consentito, ONTAP controlla l'autorizzazione di traslazione (esecuzione) per tutte le directory nel percorso del file.

Se una qualsiasi delle directory intermedie non dispone di "X" (autorizzazione trasversale), ONTAP nega l'accesso al file.

## Configurare il controllo incrociato del bypass

È possibile configurare il controllo incrociato di bypass utilizzando l'interfaccia utente di ONTAP o configurando i criteri di gruppo di Active Directory con questo diritto utente.

Il `SeChangeNotifyPrivilege` il privilegio controlla se gli utenti sono autorizzati a ignorare il controllo incrociato.

- L'aggiunta a utenti o gruppi SMB locali sulla SVM o a utenti o gruppi di dominio consente di evitare il controllo incrociato.
- La sua rimozione da utenti o gruppi SMB locali sulla SVM o da utenti o gruppi di dominio non consente di ignorare il controllo incrociato.

Per impostazione predefinita, i seguenti gruppi BUILTIN su SVM hanno il diritto di ignorare il controllo incrociato:

- BUILTIN\Administrators
- BUILTIN\Power Users
- BUILTIN\Backup Operators
- BUILTIN\Users
- Everyone

Se non si desidera consentire ai membri di uno di questi gruppi di ignorare il controllo incrociato, è necessario rimuovere questo privilegio dal gruppo.

Durante la configurazione del bypass, è necessario tenere presente quanto segue per gli utenti e i gruppi SMB locali sulla SVM utilizzando la CLI:

- Se si desidera consentire ai membri di un gruppo locale o di dominio personalizzato di ignorare il controllo incrociato, è necessario aggiungere `SeChangeNotifyPrivilege` privilegio per quel gruppo.
- Se si desidera consentire a un singolo utente locale o di dominio di ignorare il controllo incrociato e tale utente non è membro di un gruppo con tale privilegio, è possibile aggiungere `SeChangeNotifyPrivilege` privilegio per l'account utente.
- È possibile disattivare il controllo incrociato bypass per utenti o gruppi locali o di dominio rimuovendo `SeChangeNotifyPrivilege` privilegio in qualsiasi momento.



Per disattivare la funzione di bypass travers per utenti o gruppi locali o di dominio specifici, è necessario rimuovere anche `SeChangeNotifyPrivilege` privilegio di Everyone gruppo.

## Informazioni correlate

[Consenti a utenti o gruppi di ignorare il controllo incrociato della directory](#)

[Non consentire a utenti o gruppi di ignorare il controllo incrociato della directory](#)

[Configurare la mappatura dei caratteri per la conversione dei nomi file SMB sui volumi](#)

[Creare elenchi di controllo degli accessi di condivisione SMB](#)

[Proteggere l'accesso ai file utilizzando Storage-Level Access Guard](#)

[Elenco dei privilegi supportati](#)

[Aggiungere privilegi a utenti o gruppi locali o di dominio](#)

## Consenti a utenti o gruppi di ignorare il controllo incrociato della directory

Se si desidera che un utente sia in grado di attraversare tutte le directory del percorso verso un file anche se non dispone delle autorizzazioni per una directory attraversata, è possibile aggiungere `SeChangeNotifyPrivilege` Privilegio per utenti o gruppi SMB locali su macchine virtuali storage (SVM). Per impostazione predefinita, gli utenti possono ignorare il controllo incrociato della directory.

### Prima di iniziare

- Un server SMB deve essere presente sulla SVM.
- È necessario attivare l'opzione server SMB per utenti e gruppi locali.
- L'utente o il gruppo locale o di dominio in cui si utilizza `SeChangeNotifyPrivilege` il privilegio verrà aggiunto deve essere già esistente.

### A proposito di questa attività

Quando si aggiungono privilegi a un utente o a un gruppo di dominio, ONTAP può validare l'utente o il gruppo di dominio contattando il controller di dominio. Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

### Fasi

1. Abilitare il controllo incrociato bypass aggiungendo `SeChangeNotifyPrivilege` privilegio per un utente o un gruppo locale o di dominio: `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

Il valore di `-user-or-group-name` il parametro è un utente o un gruppo locale o un utente o un gruppo di dominio.

2. Verificare che l'utente o il gruppo specificato abbia attivato il controllo incrociato bypass: `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

### Esempio

Il seguente comando consente agli utenti che appartengono al gruppo "EXAMPLE" di ignorare il controllo incrociato della directory aggiungendo il `SeChangeNotifyPrivilege` privilegio per il gruppo:

```
cluster1::> vservers cifs users-and-groups privilege add-privilege -vservers
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vservers cifs users-and-groups privilege show -vservers vs1
Vservers    User or Group Name      Privileges
-----
vs1         EXAMPLE\eng             SeChangeNotifyPrivilege
```

## Informazioni correlate

[Non consentire a utenti o gruppi di ignorare il controllo incrociato della directory](#)

### Non consentire a utenti o gruppi di ignorare il controllo incrociato della directory

Se non si desidera che un utente attraversi tutte le directory nel percorso di un file perché l'utente non dispone delle autorizzazioni per la directory attraversata, è possibile rimuovere `SeChangeNotifyPrivilege` Privilegio di utenti o gruppi SMB locali su macchine virtuali storage (SVM).

### Prima di iniziare

L'utente o il gruppo locale o di dominio da cui verranno rimossi i privilegi deve già esistere.

### A proposito di questa attività

Quando si rimuovono i privilegi da un utente o gruppo di dominio, ONTAP può validare l'utente o il gruppo di dominio contattando il controller di dominio. Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

### Fasi

1. Non consentire il controllo incrociato del bypass: `vservers cifs users-and-groups privilege remove-privilege -vservers vservers_name -user-or-group-name name -privileges SeChangeNotifyPrivilege`

Il comando rimuove `SeChangeNotifyPrivilege` privilegio dell'utente o del gruppo locale o di dominio specificato con il valore per `-user-or-group-name name` parametro.

2. Verificare che l'utente o il gruppo specificato abbia disattivato il controllo incrociato bypass: `vservers cifs users-and-groups privilege show -vservers vservers_name -user-or-group-name name`

### Esempio

Il seguente comando non consente agli utenti che appartengono al gruppo "EXAMPLE" di ignorare il controllo incrociato della directory:

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name      Privileges
-----
vs1        EXAMPLE\eng              SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name      Privileges
-----
vs1        EXAMPLE\eng              -
```

### Informazioni correlate

[Consentire a utenti o gruppi di ignorare il controllo incrociato della directory](#)

### Visualizza informazioni sulla sicurezza dei file e sulle policy di audit

Visualizza informazioni generali sulla sicurezza dei file e sui criteri di controllo

È possibile visualizzare informazioni sulla sicurezza dei file su file e directory contenuti nei volumi su macchine virtuali di storage (SVM). È possibile visualizzare informazioni sui criteri di controllo sui volumi FlexVol. Se configurato, è possibile visualizzare informazioni sulle impostazioni di protezione accesso a livello di storage e controllo dinamico degli accessi sui volumi FlexVol.

### Visualizzazione delle informazioni sulla sicurezza dei file

È possibile visualizzare le informazioni sulla sicurezza dei file applicate ai dati contenuti nei volumi e nei qtree (per i volumi FlexVol) con i seguenti stili di sicurezza:

- NTFS
- UNIX
- Misto

### Visualizzazione delle informazioni sui criteri di controllo

È possibile visualizzare informazioni sulle policy di audit per il controllo degli eventi di accesso sui volumi FlexVol sui seguenti protocolli NAS:

- SMB (tutte le versioni)
- NFSv4.x

### Visualizzazione di informazioni sulla sicurezza di Storage-Level Access Guard (SLAG)

La protezione degli accessi a livello di storage può essere applicata a volumi FlexVol e oggetti qtree con i seguenti stili di sicurezza:

- NTFS
- Misto
- UNIX (se un server CIFS è configurato sulla SVM che contiene il volume)

## Visualizzazione di informazioni sulla sicurezza del controllo dinamico degli accessi (DAC)

La protezione del controllo dinamico degli accessi può essere applicata a un oggetto all'interno di un volume FlexVol con i seguenti stili di protezione:

- NTFS
- Misto (se l'oggetto dispone di una protezione efficace NTFS)

### Informazioni correlate

[Protezione dell'accesso ai file mediante Storage-Level Access Guard](#)

[Visualizzazione di informazioni su Storage-Level Access Guard](#)

### Visualizza le informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security

È possibile visualizzare informazioni sulla sicurezza di file e directory sui volumi di sicurezza NTFS, inclusi lo stile di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli attributi DOS. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

### A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei dati di cui si desidera visualizzare le informazioni di sicurezza relative al file o alla cartella. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- Poiché i volumi e i qtree di sicurezza NTFS utilizzano solo le autorizzazioni per i file NTFS e gli utenti e i gruppi Windows per determinare i diritti di accesso ai file, i campi di output relativi a UNIX contengono informazioni sulle autorizzazioni per i file UNIX di sola visualizzazione.
- L'output ACL viene visualizzato per file e cartelle con protezione NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata sulla radice del volume o sul qtree, l'output di un volume o percorso del qtree in cui è configurato Storage-Level Access Guard potrebbe visualizzare sia gli ACL dei file normali che gli ACL di Storage-Level Access Guard.
- L'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se il controllo dinamico degli accessi è configurato per il percorso di file o directory specificato.

### Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
Con dettagli più dettagliati	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

## Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/vol4` in SVM `vs1`:

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4
```

```

                Vserver: vs1
                File Path: /vol4
        File Inode Number: 64
                Security Style: ntfs
        Effective Style: ntfs
                DOS Attributes: 10
        DOS Attributes in Text: ----D---
        Expanded Dos Attributes: -
                Unix User Id: 0
                Unix Group Id: 0
                Unix Mode Bits: 777
        Unix Mode Bits in Text: rwxrwxrwx
                ACLs: NTFS Security Descriptor
                        Control:0x8004
                        Owner:BUILTIN\Administrators
                        Group:BUILTIN\Administrators
                        DACL - ACEs
                        ALLOW-Everyone-0x1f01ff
                        ALLOW-Everyone-0x10000000-
```

OI|CI|IO

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza con maschere estese sul percorso `/data/engineering` in SVM `vs1`:

```
cluster::> vserver security file-directory show -vserver vs1 -path -path  
/data/engineering -expand-mask true
```

```

                Vserver: vs1
                File Path: /data/engineering
        File Inode Number: 5544
                Security Style: ntfs
        Effective Style: ntfs
                DOS Attributes: 10
```

```

DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
    Control:0x8004

    1... .... = Self Relative
    .0.. .... = RM Control Valid
    ..0. .... = SACL Protected
    ...0 .... = DACL Protected
    .... 0... .... = SACL Inherited
    .... .0.. .... = DACL Inherited
    .... ..0. .... = SACL Inherit Required
    .... ...0 .... = DACL Inherit Required
    .... .... ..0. .... = SACL Defaulted
    .... .... ...0 .... = SACL Present
    .... .... .... 0... = DACL Defaulted
    .... .... .... .1.. = DACL Present
    .... .... .... ..0. = Group Defaulted
    .... .... .... ...0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
    ALLOW-Everyone-0x1f01ff
    0... .... =
Generic Read
    .0.. .... =
Generic Write
    ..0. .... =
Generic Execute
    ...0 .... =
Generic All
    .... ...0 .... =
System Security

```

Synchronize	.....1.....	=
Write Owner	.....1.....	=
Write DAC	.....1.....	=
Read Control	.....1.....	=
Delete	.....1.....	=
Write Attributes	.....1.....	=
Read Attributes	.....1.....	=
Delete Child	.....1.....	=
Execute	.....1.....	=
Write EA	.....1.....	=
Read EA	.....1.....	=
Append	.....1.....	=
Write	.....1.....	=
Read	.....1.....	=
ALLOW-Everyone-0x10000000-OI CI IO		
Generic Read	0.....	=
Generic Write	.0.....	=
Generic Execute	..0.....	=
Generic All	...1.....	=
System Security	.....0.....	=
Synchronize	.....0.....	=
Write Owner	.....0.....	=
Write DAC	.....0.....	=



Read Control	.....0..... =
Delete	.....0..... =
Write Attributes	.....0..... =
Read Attributes	.....0..... =
Delete Child	.....0..... =
Execute	.....0..... =
Write EA	.....0..... =
Read EA	.....0..... =
Append	.....0..... =
Write	.....0..... =
Read	.....0..... =

Nell'esempio riportato di seguito vengono visualizzate le informazioni di sicurezza, incluse le informazioni di protezione Storage-Level Access Guard, per il volume con il percorso /datavol1 In SVM vs1:

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1
```

```

    Vserver: vs1
    File Path: /datavol1
    File Inode Number: 77
    Security Style: ntfs
    Effective Style: ntfs
    DOS Attributes: 10
    DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
    Unix User Id: 0
    Unix Group Id: 0
    Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
    ACLs: NTFS Security Descriptor
          Control:0x8004
          Owner: BUILTIN\Administrators
          Group: BUILTIN\Administrators
          DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-OI|CI|IO

    Storage-Level Access Guard security
    SACL (Applies to Directories):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Directories):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
    SACL (Applies to Files):
          AUDIT-EXAMPLE\Domain Users-0x120089-FA
          AUDIT-EXAMPLE\engineering-0x1f01ff-SA
    DACL (Applies to Files):
          ALLOW-EXAMPLE\Domain Users-0x120089
          ALLOW-EXAMPLE\engineering-0x1f01ff
          ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

### Informazioni correlate

[Visualizzazione di informazioni sulla sicurezza dei file su volumi misti di tipo sicurezza](#)

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi UNIX di tipo Security](#)

È possibile visualizzare informazioni sulla sicurezza di file e directory su volumi misti di sicurezza, inclusi lo stile di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sui proprietari e sui gruppi UNIX. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

### A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei dati di cui si desidera visualizzare le informazioni di sicurezza relative al file o alla cartella. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree misti di sicurezza possono contenere alcuni file e cartelle che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.
- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS.
- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

Questo campo è vuoto per i file e le directory che utilizzano la protezione UNIX e che hanno solo autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia le autorizzazioni dei file UNIX che gli ACL Storage-Level Access Guard.
- Se il percorso immesso nel comando riguarda i dati con protezione effettiva NTFS, l'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se è configurato Dynamic Access Control per il percorso di file o directory specificato.

### Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<pre>vserver security file-directory show -vserver vserver_name -path path</pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</pre>

### Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/projects` in SVM `vs1` in forma di maschera espansa. Questo percorso misto in stile di sicurezza offre una sicurezza efficace per UNIX.

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true
```

```

        Vserver: vs1
        File Path: /projects
    File Inode Number: 78
        Security Style: mixed
    Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ....0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
        ACLs: -
```

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso /data In SVM vs1. Questo percorso misto di sicurezza ha una protezione efficace NTFS.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data
```

```

        Vserver: vs1
        File Path: /data
    File Inode Number: 544
        Security Style: mixed
        Effective Style: ntfs
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 777
    Unix Mode Bits in Text: rwxrwxrwx
        ACLs: NTFS Security Descriptor
            Control:0x8004
            Owner:BUILTIN\Administrators
            Group:BUILTIN\Administrators
            DACL - ACEs
                ALLOW-Everyone-0x1f01ff
                ALLOW-Everyone-0x10000000-
```

OI|CI|IO

Nell'esempio riportato di seguito vengono visualizzate le informazioni di sicurezza relative al volume nel percorso /datavol5 in SVM vs1. Il livello superiore di questo volume misto di sicurezza offre una protezione efficace per UNIX. Il volume dispone della protezione di Storage-Level Access Guard.

```
cluster1::> vserver security file-directory show -vserver vs1 -path /datavol5
```

```
      Vserver: vs1
      File Path: /datavol5
      File Inode Number: 3374
      Security Style: mixed
      Effective Style: unix
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 755
      Unix Mode Bits in Text: rwxr-xr-x
      ACLs: Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
        AUDIT-EXAMPLE\market-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-BUILTIN\Administrators-0x1f01ff
        ALLOW-CREATOR OWNER-0x1f01ff
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-EXAMPLE\market-0x1f01ff
```

### Informazioni correlate

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security](#)

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi UNIX di tipo Security](#)

**Visualizza informazioni sulla sicurezza dei file su volumi UNIX di tipo Security**

È possibile visualizzare informazioni sulla sicurezza di file e directory sui volumi UNIX di tipo Security, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sui proprietari e sui gruppi UNIX. È possibile utilizzare i risultati

per convalidare la configurazione di sicurezza o per risolvere i problemi di accesso ai file.

### A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei dati di cui si desidera visualizzare le informazioni di sicurezza relative al file o alla directory. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree UNIX di sicurezza utilizzano solo le autorizzazioni dei file UNIX, ovvero i bit di modalità o gli ACL NFSv4 per determinare i diritti di accesso ai file.
- L'output ACL viene visualizzato solo per file e cartelle con protezione NFSv4.

Questo campo è vuoto per i file e le directory che utilizzano la protezione UNIX e che hanno solo autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi di output del proprietario e del gruppo nell'output ACL non sono validi nel caso dei descrittori di protezione NFSv4.

Sono significativi solo per i descrittori di protezione NTFS.

- Poiché la protezione Storage-Level Access Guard è supportata su un volume o qtree UNIX se un server CIFS è configurato su SVM, l'output potrebbe contenere informazioni sulla protezione Storage-Level Access Guard applicata al volume o al qtree specificato in `-path` parametro.

### Fase

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i></pre>
Con dettagli più dettagliati	<pre>vserver security file-directory show -vserver <i>vserver_name</i> -path <i>path</i> -expand-mask true</pre>

### Esempi

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/home` in SVM `vs1`:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
```

```

        Vserver: vs1
        File Path: /home
    File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
                ACLs: -
```

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso /home in SVM vs1 sotto forma di maschera espansa:

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true
```

```

        Vserver: vs1
        File Path: /home
    File Inode Number: 9590
        Security Style: unix
        Effective Style: unix
        DOS Attributes: 10
    DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
        Unix User Id: 0
        Unix Group Id: 1
        Unix Mode Bits: 700
    Unix Mode Bits in Text: rwx-----
                ACLs: -
```



## Informazioni correlate

[Visualizzazione delle informazioni sulla sicurezza dei file sui volumi NTFS di tipo Security](#)

[Visualizzazione di informazioni sulla sicurezza dei file su volumi misti di tipo sicurezza](#)

**Visualizza informazioni sui criteri di audit NTFS sui volumi FlexVol utilizzando l'interfaccia CLI**

È possibile visualizzare informazioni sui criteri di controllo NTFS sui volumi FlexVol, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo degli accessi al sistema. È possibile utilizzare i risultati per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

### A proposito di questa attività

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle cartelle di cui si desidera visualizzare le informazioni di audit. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree di sicurezza NTFS utilizzano solo SACL (System Access Control List) NTFS per i criteri di controllo.
- I file e le cartelle in un volume misto di sicurezza con protezione efficace NTFS possono applicare criteri di controllo NTFS.

I volumi misti di sicurezza e le qtree possono contenere alcuni file e directory che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.

- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS e potrebbe contenere o meno SACL NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, l'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia SACL NFSv4 di file e cartelle standard che SACL NTFS di Storage-Level Access Guard.
- Se il percorso immesso nel comando è relativo ai dati con protezione effettiva NTFS, l'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se Dynamic Access Control è configurato per il percorso di file o directory specificato.
- Quando si visualizzano informazioni di sicurezza su file e cartelle con protezione efficace NTFS, i campi di output relativi a UNIX contengono informazioni di autorizzazione file UNIX di sola visualizzazione.

I file e le cartelle di sicurezza NTFS utilizzano solo le autorizzazioni per i file NTFS e gli utenti e i gruppi Windows per determinare i diritti di accesso ai file.

- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

Questo campo è vuoto per i file e le cartelle che utilizzano la protezione UNIX e che dispongono solo delle autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.

### Fase

1. Visualizzare le impostazioni dei criteri di controllo di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Come elenco dettagliato	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

## Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/corp` in SVM vs1. Il percorso offre una protezione efficace con NTFS. Il descrittore di protezione NTFS contiene sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA.

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0x8014
      Owner:DOMAIN\Administrator
      Group:BUILTIN\Administrators
      SACL - ACEs
      ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
      SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
      DACL - ACEs
      ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
      ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
      ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
      ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/datavol1` in SVM vs1. Il percorso contiene SACL di file e cartelle e SACL Storage-Level Access Guard.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
                  AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
                  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                  ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

**Visualizza informazioni sui criteri di audit NFSv4 sui volumi FlexVol utilizzando la CLI**

È possibile visualizzare informazioni sui criteri di controllo di NFSv4 sui volumi FlexVol utilizzando l'interfaccia CLI di ONTAP, inclusi gli stili di sicurezza e gli stili di sicurezza

effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo dell'accesso al sistema (SACL). È possibile utilizzare i risultati per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

**A proposito di questa attività**

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle directory di cui si desidera visualizzare le informazioni di audit. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree UNIX di sicurezza utilizzano solo SACL NFSv4 per le policy di controllo.
  - I file e le directory di un volume misto di sicurezza con stile UNIX possono applicare criteri di controllo NFSv4.
- I volumi misti di sicurezza e le qtree possono contenere alcuni file e directory che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.
- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS e potrebbe contenere o meno SACL NFSv4.
  - L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

Questo campo è vuoto per i file e le cartelle che utilizzano la protezione UNIX e che dispongono solo delle autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.
- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia SACL normali di file NFSv4, directory e SACL NTFS di Storage-Level Access Guard.
- Poiché la protezione Storage-Level Access Guard è supportata su un volume o qtree UNIX se un server CIFS è configurato su SVM, l'output potrebbe contenere informazioni sulla protezione Storage-Level Access Guard applicata al volume o al qtree specificato in `-path` parametro.

**Fasi**

1. Visualizzare le impostazioni di sicurezza di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Con dettagli più dettagliati	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

**Esempi**

Nell'esempio seguente vengono visualizzate le informazioni di sicurezza relative al percorso `/lab` in SVM `vs1`. Questo percorso di sicurezza UNIX ha un SACL NFSv4.

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab
```

```

    Vserver: vs1
    File Path: /lab
    File Inode Number: 288
    Security Style: unix
    Effective Style: unix
    DOS Attributes: 11
    DOS Attributes in Text: ----D--R
    Expanded Dos Attributes: -
        Unix User Id: 0
        Unix Group Id: 0
        Unix Mode Bits: 0
    Unix Mode Bits in Text: -----
        ACLs: NFSV4 Security Descriptor
            Control:0x8014
            SACL - ACEs
                SUCCESSFUL-S-1-520-0-0xf01ff-SA
                FAILED-S-1-520-0-0xf01ff-FA
            DACL - ACEs
                ALLOW-S-1-520-1-0xf01ff
```

#### Modi per visualizzare informazioni sulla sicurezza dei file e sulle policy di audit

È possibile utilizzare il carattere jolly (\*) per visualizzare informazioni sulla sicurezza dei file e sulle policy di controllo di tutti i file e le directory in un determinato percorso o volume root.

Il carattere jolly (\*) **può essere utilizzato come ultimo sottocomponente di un determinato percorso di directory al di sotto del quale si desidera visualizzare le informazioni di tutti i file e le directory. Se si desidera visualizzare le informazioni di un particolare file o directory denominata "", è necessario fornire il percorso completo tra virgolette doppie ("").**

#### Esempio

Il seguente comando con il carattere jolly visualizza le informazioni su tutti i file e le directory sotto il percorso /1/ Di SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

Il seguente comando visualizza le informazioni di un file denominato "" sotto il percorso /vol1/a Di SVM vs1. Il percorso è racchiuso tra virgolette doppie (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path  
"/vol1/a/*"
```

```
        Vserver: vs1  
        File Path: "/vol1/a/*"  
        Security Style: mixed  
        Effective Style: unix  
        DOS Attributes: 10  
        DOS Attributes in Text: ----D---  
        Expanded Dos Attributes: -  
            Unix User Id: 1002  
            Unix Group Id: 65533  
            Unix Mode Bits: 755  
        Unix Mode Bits in Text: rwxr-xr-x  
        ACLs: NFSV4 Security Descriptor  
            Control:0x8014  
            SACL - ACEs  
                AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
            DACL - ACEs  
                ALLOW-EVERYONE@-0x1f00a9-FI|DI  
                ALLOW-OWNER@-0x1f01ff-FI|DI  
                ALLOW-GROUP@-0x1200a9-IG
```

## **Gestire la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su SVM utilizzando la CLI**

**Gestisci la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su SVM utilizzando la panoramica CLI**

È possibile gestire la sicurezza dei file NTFS, le policy di audit NTFS e Storage-Level Access Guard su macchine virtuali storage (SVM) utilizzando la CLI.

È possibile gestire la sicurezza dei file NTFS e le policy di controllo dai client SMB o utilizzando la CLI. Tuttavia, l'utilizzo della CLI per configurare le policy di controllo e sicurezza dei file elimina la necessità di utilizzare un client remoto per gestire la sicurezza dei file. L'utilizzo della CLI può ridurre significativamente il tempo necessario per applicare la protezione a molti file e cartelle utilizzando un singolo comando.

È possibile configurare Access Guard a livello di storage, un altro livello di sicurezza applicato da ONTAP ai volumi SVM. Storage-Level Access Guard si applica agli accessi da tutti i protocolli NAS all'oggetto storage a cui è applicato Storage-Level Access Guard.

Access Guard a livello di storage può essere configurato e gestito solo dalla CLI di ONTAP. Non è possibile gestire le impostazioni di Storage-Level Access Guard dai client SMB. Inoltre, se si visualizzano le impostazioni di sicurezza su un file o una directory da un client NFS o SMB, non viene visualizzata la protezione Storage-Level Access Guard. La protezione di Storage-Level Access Guard non può essere revocata da un client, nemmeno da un amministratore di sistema (Windows o UNIX). Pertanto, Storage-Level Access Guard offre un ulteriore livello di sicurezza per l'accesso ai dati, impostato e gestito in modo indipendente dall'amministratore dello storage.



Anche se sono supportate solo le autorizzazioni di accesso NTFS per Storage-Level Access Guard, ONTAP può eseguire controlli di sicurezza per l'accesso via NFS ai dati sui volumi in cui viene applicato Storage-Level Access Guard se l'utente UNIX esegue il mapping a un utente Windows sulla SVM proprietaria del volume.

## Volumi NTFS di tipo Security

Tutti i file e le cartelle contenuti nei volumi e nei qtree di sicurezza NTFS dispongono di un'efficace protezione NTFS. È possibile utilizzare `vserver security file-directory` Famiglia di comandi per implementare i seguenti tipi di protezione sui volumi NTFS di tipo Security:

- Permessi dei file e policy di controllo per file e cartelle contenuti nel volume
- Protezione degli accessi a livello di storage sui volumi

## Volumi misti di sicurezza

I volumi e i qtree misti in stile di sicurezza possono contenere alcuni file e cartelle con una protezione efficace UNIX e che utilizzano autorizzazioni per i file UNIX, i criteri di controllo Mbit di modalità o ACL NFSv4.x e NFSv4.x, nonché alcuni file e cartelle con una protezione effettiva NTFS e che utilizzano le autorizzazioni per i file NTFS e i criteri di controllo. È possibile utilizzare `vserver security file-directory` famiglia di comandi per applicare i seguenti tipi di protezione a dati misti di tipo sicurezza:

- Permessi dei file e policy di controllo per file e cartelle con NTFS efficace in stile di sicurezza nel volume misto o nel qtree
- Access Guard a livello di storage per i volumi con sicurezza efficace NTFS e UNIX

## Volumi UNIX di tipo Security

I volumi e le qtree UNIX di sicurezza contengono file e cartelle con protezione efficace UNIX (ovvero i bit di modalità o gli ACL NFSv4.x). Se si desidera utilizzare il, tenere presente quanto segue `vserver security file-directory` Famiglia di comandi per implementare la sicurezza su volumi UNIX di tipo Security:

- Il `vserver security file-directory` La famiglia di comandi non può essere utilizzata per gestire la sicurezza dei file UNIX e le policy di controllo su qtree e volumi di sicurezza UNIX.
- È possibile utilizzare `vserver security file-directory` Famiglia di comandi per configurare Storage-Level Access Guard su volumi UNIX di tipo Security, a condizione che SVM con il volume di destinazione contenga un server CIFS.

## Informazioni correlate

[Visualizza informazioni sulla sicurezza dei file e sulle policy di audit](#)

[Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI](#)

[Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la CLI](#)

[Proteggere l'accesso ai file utilizzando Storage-Level Access Guard](#)

## Casi di utilizzo dell'interfaccia CLI per impostare la sicurezza di file e cartelle

Poiché è possibile applicare e gestire la sicurezza di file e cartelle in locale senza il coinvolgimento di un client remoto, è possibile ridurre significativamente il tempo necessario per impostare la protezione in blocco su un gran numero di file o cartelle.



È possibile utilizzare la CLI per impostare la sicurezza di file e cartelle nei seguenti casi di utilizzo:

- Storage di file in ambienti aziendali di grandi dimensioni, ad esempio lo storage di file nelle home directory
- Migrazione dei dati
- Modifica del dominio Windows
- Standardizzazione delle policy di controllo e sicurezza dei file nei file system NTFS

#### **Limiti di utilizzo della CLI per impostare la sicurezza di file e cartelle**

È necessario conoscere alcuni limiti quando si utilizza la CLI per impostare la sicurezza di file e cartelle.

- Il `vserver security file-directory` La famiglia di comandi non supporta l'impostazione degli ACL NFSv4.

È possibile applicare i descrittori di protezione NTFS solo a file e cartelle NTFS.

#### **Come vengono utilizzati i descrittori di protezione per applicare la sicurezza di file e cartelle**

I descrittori di protezione contengono gli elenchi di controllo degli accessi che determinano le azioni che un utente può eseguire su file e cartelle e le operazioni controllate quando un utente accede a file e cartelle.

- **Autorizzazioni**

Le autorizzazioni sono consentite o negate dal proprietario di un oggetto e determinano le azioni che un oggetto (utenti, gruppi o oggetti computer) può eseguire su file o cartelle specifici.

- **Descrittori di sicurezza**

I descrittori di protezione sono strutture di dati che contengono informazioni di sicurezza che definiscono le autorizzazioni associate a un file o a una cartella.

- **ACL (Access Control List)**

Gli elenchi di controllo degli accessi sono gli elenchi contenuti in un descrittore di protezione che contengono informazioni sulle azioni che gli utenti, i gruppi o gli oggetti computer possono eseguire nel file o nella cartella a cui è applicato il descrittore di protezione. Il descrittore di protezione può contenere i seguenti due tipi di ACL:

- DACL (Discretionary Access Control List)
- SACL (System Access Control List)

- **Elenchi di controllo degli accessi discrezionali (DACL)**

I DACL contengono l'elenco dei SIDS per gli utenti, i gruppi e gli oggetti computer ai quali è consentito o negato l'accesso per eseguire azioni su file o cartelle. I DACL contengono zero o più voci di controllo degli accessi (ACE).

- **System access control list (SACL)**

I SACL contengono l'elenco di SIDS per gli utenti, i gruppi e gli oggetti computer per i quali vengono

registrati eventi di controllo riusciti o non riusciti. I SACL contengono zero o più voci di controllo degli accessi (ACE).

- **Voci di controllo di accesso (ACE)**

Gli assi sono singole voci in DACL o SACL:

- Una voce di controllo dell'accesso DACL specifica i diritti di accesso consentiti o negati per determinati utenti, gruppi o oggetti computer.
- Una voce di controllo dell'accesso SACL specifica gli eventi di successo o di errore da registrare quando si controllano le azioni specifiche eseguite da utenti, gruppi o oggetti computer specifici.

- **Ereditarietà delle autorizzazioni**

L'ereditarietà delle autorizzazioni descrive il modo in cui le autorizzazioni definite nei descrittori di protezione vengono propagate a un oggetto da un oggetto padre. Solo le autorizzazioni ereditabili vengono ereditate dagli oggetti figlio. Quando si impostano le autorizzazioni sull'oggetto padre, è possibile decidere se cartelle, sottocartelle e file possono ereditare tali autorizzazioni con "applicabile a. this-folder, sub-folders`e `files".

## **Informazioni correlate**

["Controllo SMB e NFS e tracciamento della sicurezza"](#)

[Configurazione e applicazione dei criteri di controllo a file e cartelle NTFS mediante l'interfaccia CLI](#)

**Linee guida per l'applicazione di policy di directory di file che utilizzano utenti o gruppi locali sulla destinazione di disaster recovery SVM**

Prima di applicare i criteri di directory dei file alla destinazione di disaster recovery SVM (Storage Virtual Machine) in una configurazione di eliminazione dell'ID, è necessario tenere presenti alcune linee guida se la configurazione dei criteri di directory dei file utilizza utenti o gruppi locali nel descrittore di protezione o nelle voci DACL o SACL.

È possibile configurare una configurazione di disaster recovery per una SVM in cui la SVM di origine sul cluster di origine replica i dati e la configurazione dalla SVM di origine a una SVM di destinazione su un cluster di destinazione.

È possibile configurare uno dei due tipi di disaster recovery SVM:

- **Identità preservata**

Con questa configurazione, l'identità di SVM e del server CIFS viene preservata.

- **Identità scartata**

Con questa configurazione, l'identità di SVM e del server CIFS non viene preservata. In questo scenario, il nome di SVM e del server CIFS sulla SVM di destinazione è diverso da SVM e dal nome del server CIFS sulla SVM di origine.

## **Linee guida per le configurazioni di identità scartate**

In una configurazione con eliminazione dell'identità, per un'origine SVM che contiene configurazioni di utente, gruppo e privilegi locali, il nome del dominio locale (nome del server CIFS locale) deve essere modificato in modo che corrisponda al nome del server CIFS sulla destinazione SVM. Ad esempio, se il nome SVM di

origine è "vs1" e il nome del server CIFS è "CIFS1" e il nome SVM di destinazione è "vs1\_dst" e il nome del server CIFS è "CIFS1\_DST", il nome del dominio locale di un utente locale denominato "CIFS1` user1" viene automaticamente modificato in "`CIFST\_DVM\_1".

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1	CIFS1\Administrator		Built-in
vs1	CIFS1\user1	-	-

```
cluster1dst::> vserver cifs users-and-groups local-user show -vserver vs1_dst
```

Vserver	User Name	Full Name	Description
vs1_dst	CIFS1_DST\Administrator		Built-in
vs1_dst	CIFS1_DST\user1	-	-

Anche se i nomi degli utenti e dei gruppi locali vengono modificati automaticamente nei database degli utenti e dei gruppi locali, i nomi degli utenti o dei gruppi locali non vengono modificati automaticamente nelle configurazioni dei criteri delle directory dei file (criteri configurati sulla CLI tramite `vserver security file-directory` famiglia di comandi).

Ad esempio, per "vs1", se è stata configurata una voce DACL in cui si trova `-account` Il parametro è impostato su "`CIFS1` user1", l'impostazione non viene modificata automaticamente sulla SVM di destinazione per riflettere il nome del server CIFS di destinazione.

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
CIFS1\user1	allow	full-control	this-folder

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1_dst
```

```
Vserver: vs1_dst
```

```
NTFS Security Descriptor Name: sd1
```

Account Name	Access Type	Access Rights	Apply To
-----	-----	-----	-----
**CIFS1**\user1	allow	full-control	this-folder

È necessario utilizzare `vserver security file-directory modify` Comandi per modificare manualmente il nome del server CIFS nel nome del server CIFS di destinazione.

### Componenti di configurazione dei criteri di directory dei file che contengono parametri dell'account

Esistono tre componenti di configurazione dei criteri di directory dei file che possono utilizzare le impostazioni dei parametri che possono contenere utenti o gruppi locali:

- Descrittore di sicurezza

È possibile specificare il proprietario del descrittore di protezione e il gruppo primario del proprietario del descrittore di protezione. Se il descrittore di protezione utilizza un utente o un gruppo locale per le voci del proprietario e del gruppo primario, è necessario modificare il descrittore di protezione per utilizzare la SVM di destinazione nel nome dell'account. È possibile utilizzare `vserver security file-directory ntfs modify` per apportare le modifiche necessarie ai nomi degli account.

- Voci DACL

Ogni voce DACL deve essere associata a un account. Per utilizzare il nome SVM di destinazione, è necessario modificare tutti i DACL che utilizzano account utente o di gruppo locali. Poiché non è possibile modificare il nome dell'account per le voci DACL esistenti, è necessario rimuovere eventuali voci DACL con utenti o gruppi locali dai descrittori di protezione, creare nuove voci DACL con i nomi account di destinazione corretti e associare queste nuove voci DACL ai descrittori di protezione appropriati.

- Voci SACL

Ogni voce SACL deve essere associata a un account. Per utilizzare il nome SVM di destinazione, è necessario modificare tutti i SACL che utilizzano account utente o di gruppo locali. Poiché non è possibile modificare il nome dell'account per le voci SACL esistenti, è necessario rimuovere eventuali voci SACL con

utenti o gruppi locali dai descrittori di protezione, creare nuove voci SACL con i nomi account di destinazione corretti e associare queste nuove voci SACL ai descrittori di protezione appropriati.

Prima di applicare il criterio, è necessario apportare le modifiche necessarie agli utenti o ai gruppi locali utilizzati nella configurazione del criterio della directory dei file; in caso contrario, il processo di applicazione non riesce.

**Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI**

### **Creare un descrittore di protezione NTFS**

La creazione di un descrittore di sicurezza NTFS (policy di sicurezza dei file) è il primo passo nella configurazione e nell'applicazione degli elenchi di controllo degli accessi NTFS (ACL) a file e cartelle che risiedono nelle macchine virtuali di storage (SVM). È possibile associare il descrittore di protezione al percorso di file o cartelle in un'attività di policy.

#### **A proposito di questa attività**

È possibile creare descrittori di protezione NTFS per file e cartelle che risiedono all'interno di volumi di sicurezza NTFS o per file e cartelle che risiedono su volumi misti di tipo sicurezza.

Per impostazione predefinita, quando viene creato un descrittore di protezione, vengono aggiunte quattro voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) a tale descrittore di protezione. Le quattro ACE predefinite sono le seguenti:

Oggetto	Tipo di accesso	Diritti di accesso	Dove applicare le autorizzazioni
BUILTIN/amministratori	Consentire	Controllo completo	questa-cartella, sottocartelle, file
BUILTIN/utenti	Consentire	Controllo completo	questa-cartella, sottocartelle, file
PROPRIETARIO DEL CREATOR	Consentire	Controllo completo	questa-cartella, sottocartelle, file
AUTORITÀ/SISTEMA NT	Consentire	Controllo completo	questa-cartella, sottocartelle, file

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Proprietario del descrittore di protezione
- Gruppo primario del proprietario
- Flag di controllo raw

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

## Aggiungere le voci di controllo dell'accesso DACL NTFS al descrittore di protezione NTFS

L'aggiunta di voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) al descrittore di protezione NTFS è il secondo passo nella configurazione e nell'applicazione di ACL NTFS a un file o a una cartella. Ciascuna voce identifica l'oggetto a cui è consentito o negato l'accesso e definisce le operazioni che l'oggetto può o non può eseguire nei file o nelle cartelle definiti nell'ACE.

### A proposito di questa attività

È possibile aggiungere uno o più ACE al DACL del descrittore di protezione.

Se il descrittore di protezione contiene un DACL con ACE esistenti, il comando aggiunge il nuovo ACE al DACL. Se il descrittore di protezione non contiene un DACL, il comando crea il DACL e aggiunge il nuovo ACE.

È possibile personalizzare le voci DACL specificando i diritti che si desidera consentire o negare per l'account specificato in `-account` parametro. Esistono tre metodi di esclusione reciproca per specificare i diritti:

- Diritti
- Diritti avanzati
- Diritti raw (privilegio avanzato)



Se non si specificano i diritti per la voce DACL, l'impostazione predefinita è impostare i diritti su `Full Control`.

È possibile personalizzare le voci DACL specificando come applicare l'ereditarietà.

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine `man`.

### Fasi

1. Aggiungere una voce DACL a un descrittore di protezione: `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID optional_parameters`

```
vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Verificare che la voce DACL sia corretta: `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
  Allow or Deny: deny
    Account Name or SID: DOMAIN\joe
      Access Rights: full-control
Advanced Access Rights: -
  Apply To: this-folder
    Access Rights: full-control
```

## Creare policy di sicurezza

La creazione di una policy di sicurezza dei file per le SVM è la terza fase della configurazione e dell'applicazione degli ACL a un file o a una cartella. Un criterio agisce come un contenitore per varie attività, in cui ogni attività è una singola voce che può essere applicata a file o cartelle. È possibile aggiungere attività al criterio di protezione in un secondo momento.

### A proposito di questa attività

Le attività aggiunte a un criterio di protezione contengono associazioni tra il descrittore di protezione NTFS e i percorsi di file o cartelle. Pertanto, è necessario associare i criteri di protezione a ogni SVM (contenente volumi di sicurezza NTFS o volumi di sicurezza misti).

### Fasi

1. Creare una policy di sicurezza: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```

2. Verificare la policy di sicurezza: `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver      Policy Name
-----
vs1          policy1
```

## Aggiungere un'attività alla policy di sicurezza

La creazione e l'aggiunta di un'attività di policy a un criterio di sicurezza è la quarta fase della configurazione e dell'applicazione degli ACL a file o cartelle in SVM. Quando si crea l'attività relativa ai criteri, l'attività viene associata a un criterio di protezione. È possibile aggiungere una o più voci di attività a un criterio di protezione.

### A proposito di questa attività

La policy di sicurezza è un container per un'attività. Un'attività si riferisce a una singola operazione che può

essere eseguita da un criterio di protezione a file o cartelle con NTFS o protezione mista (o a un oggetto volume se si configura Storage-Level Access Guard).

Esistono due tipi di attività:

- Attività di file e directory

Consente di specificare le attività che applicano i descrittori di protezione a file e cartelle specifici. Gli ACL applicati attraverso le attività di file e directory possono essere gestiti con client SMB o CLI ONTAP.

- Attività di Access Guard a livello di storage

Consente di specificare le attività che applicano i descrittori di protezione di Storage-Level Access Guard a un volume specificato. Gli ACL applicati tramite le attività di Access Guard a livello di storage possono essere gestiti solo tramite l'interfaccia utente di ONTAP.

Un'attività contiene le definizioni per la configurazione di sicurezza di un file (o di una cartella) o di un set di file (o di cartelle). Ogni attività di una policy è identificata in modo univoco dal percorso. Un'unica attività per percorso può essere presente all'interno di un singolo criterio. Un criterio non può avere voci di attività duplicate.

Linee guida per l'aggiunta di un'attività a un criterio:

- È possibile includere un massimo di 10,000 voci di attività per policy.
- Un criterio può contenere una o più attività.

Anche se un criterio può contenere più attività, non è possibile configurare un criterio in modo che contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

Non assegnerà mai autorizzazioni di accesso aggiuntive.

Quando si aggiungono attività ai criteri di protezione, è necessario specificare i seguenti quattro parametri richiesti:

- Nome SVM
- Nome policy
- Percorso
- Descrittore di sicurezza da associare al percorso

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Tipo di sicurezza
- Modalità di propagazione
- Posizione dell'indice
- Tipo di controllo dell'accesso

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori



informazioni, consulta le pagine man.

**Fasi**

- 1. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` è il valore predefinito di `-access-control` parametro. La specifica del tipo di controllo dell'accesso durante la configurazione delle attività di accesso a file e directory è facoltativa.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

- 2. Verificare la configurazione dell'attività del criterio: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

Vserver: vs1  
Policy: policy1

Index	File/Folder	Access	Security	NTFS	NTFS
	Path	Control	Type	Mode	
Descriptor Name					
-----	-----	-----	-----	-----	
-----					
1	/home/dir1	file-directory	ntfs	propagate	sd2

**Applicare le policy di sicurezza**

L'applicazione di una policy di sicurezza dei file alle SVM è l'ultimo passo nella creazione e nell'applicazione di ACL NTFS a file o cartelle.

**A proposito di questa attività**

È possibile applicare le impostazioni di protezione definite nel criterio di protezione ai file e alle cartelle NTFS che risiedono nei volumi FlexVol (NTFS o stile di protezione misto).



Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Quando vengono applicati un criterio di protezione e i DACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

**Fase**

- 1. Applicare una policy di sicurezza: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

Il processo di applicazione della policy viene pianificato e viene restituito l'ID lavoro.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

## Monitorare il processo di policy di sicurezza

Quando si applica la policy di sicurezza alle macchine virtuali di storage (SVM), è possibile monitorare l'avanzamento dell'attività monitorando il processo di policy di sicurezza. Ciò è utile se si desidera verificare che l'applicazione del criterio di protezione sia riuscita. Questo è utile anche se si dispone di un processo a esecuzione prolungata in cui si applica la protezione in blocco a un gran numero di file e cartelle.

### A proposito di questa attività

Per visualizzare informazioni dettagliate su un processo di policy di sicurezza, utilizzare `-instance` parametro.

### Fase

1. Monitorare il processo di policy di sicurezza: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

## Verificare la sicurezza del file applicata

È possibile verificare le impostazioni di sicurezza del file per confermare che i file o le cartelle sulla macchina virtuale di storage (SVM) a cui è stato applicato il criterio di protezione abbiano le impostazioni desiderate.

### A proposito di questa attività

Specificare il nome della SVM contenente i dati e il percorso del file e delle cartelle in cui si desidera verificare le impostazioni di sicurezza. È possibile utilizzare il opzionale `-expand-mask` per visualizzare informazioni dettagliate sulle impostazioni di sicurezza.

### Fase

1. Visualizzare le impostazioni di sicurezza di file e cartelle: `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

```
vserver security file-directory show -vserver vs1 -path /data/engineering
```

-expand-mask true

```
Vserver: vs1
      File Path: /data/engineering
File Inode Number: 5544
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
    ...0 .... = Offline
    .... ..0. .... = Sparse
    .... .... 0... .... = Normal
    .... .... ..0. .... = Archive
    .... .... ...1 .... = Directory
    .... .... .... .0.. = System
    .... .... .... ..0. = Hidden
    .... .... .... ...0 = Read Only
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
      Control:0x8004

1... .... = Self Relative
.0.. .... = RM Control Valid
..0. .... = SACL Protected
...0 .... = DACL Protected
.... 0... .... = SACL Inherited
.... .0.. .... = DACL Inherited
.... ..0. .... = SACL Inherit Required
.... ...0 .... = DACL Inherit Required
.... .... ..0. .... = SACL Defaulted
.... .... ...0 .... = SACL Present
.... .... .... 0... = DACL Defaulted
.... .... .... .1.. = DACL Present
.... .... .... ..0. = Group Defaulted
.... .... .... ...0 = Owner Defaulted

Owner:BUILTIN\Administrators
Group:BUILTIN\Administrators
DACL - ACEs
      ALLOW-Everyone-0x1f01ff
      0... .... =

Generic Read
```

Generic Write	.0.. .....	=
Generic Execute	..0. ....	=
Generic All	...0 .....	=
System Security	.... ..0 .....	=
Synchronize	.... ....1 .....	=
Write Owner	.... ....1... .....	=
Write DAC	.... ....1.. .....	=
Read Control	.... ....1. ....	=
Delete	.... ....1 .....	=
Write Attributes	.... ....1 .....	=
Read Attributes	.... ....1... .....	=
Delete Child	.... ....1.. ....	=
Execute	.... ....1. ....	=
Write EA	.... ....1 .....	=
Read EA	.... ....1... .....	=
Append	.... ....1.. ....	=
Write	.... ....1. ....	=
Read	.... ....1 =	
ALLOW-Everyone-0x10000000-OI CI IO		
Generic Read	0... .....	=
Generic Write	.0.. .....	=
Generic Execute	..0. ....	=
Generic All	...1 .....	=

	.....0.....	=
System Security		
	.....0.....	=
Synchronize		
	.....0.....	=
Write Owner		
	.....0.....	=
Write DAC		
	.....0.....	=
Read Control		
	.....0.....	=
Delete		
	.....0.....	=
Write Attributes		
	.....0.....	=
Read Attributes		
	.....0.....	=
Delete Child		
	.....0.....	=
Execute		
	.....0.....	=
Write EA		
	.....0.....	=
Read EA		
	.....0.....	=
Append		
	.....0.....	=
Write		
	.....0.....	=
Read		

**Configurare e applicare i criteri di controllo ai file e alle cartelle NTFS utilizzando la panoramica CLI**

È necessario eseguire diversi passaggi per applicare i criteri di controllo a file e cartelle NTFS quando si utilizza l'interfaccia utente di ONTAP. Innanzitutto, si crea un descrittore di protezione NTFS e si aggiungono SACL al descrittore di protezione. Quindi, creare una policy di sicurezza e aggiungere attività di policy. Quindi, applicare il criterio di protezione a una macchina virtuale di storage (SVM).

**A proposito di questa attività**

Dopo aver applicato il criterio di protezione, è possibile monitorare il processo di criteri di protezione e verificare le impostazioni per il criterio di controllo applicato.



Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

## Informazioni correlate

[Protezione dell'accesso ai file mediante Storage-Level Access Guard](#)

[Limiti di utilizzo della CLI per impostare la sicurezza di file e cartelle](#)

[Come vengono utilizzati i descrittori di protezione per applicare la sicurezza di file e cartelle](#)

["Controllo SMB e NFS e tracciamento della sicurezza"](#)

[Configurare e applicare la protezione dei file su file e cartelle NTFS utilizzando l'interfaccia CLI](#)

## Creare un descrittore di protezione NTFS

La creazione di un criterio di audit del descrittore di protezione NTFS è il primo passo nella configurazione e nell'applicazione degli elenchi di controllo di accesso (ACL) NTFS a file e cartelle che risiedono all'interno delle SVM. Il descrittore di protezione verrà associato al percorso del file o della cartella in un'attività di policy.

### A proposito di questa attività

È possibile creare descrittori di protezione NTFS per file e cartelle che risiedono all'interno di volumi di sicurezza NTFS o per file e cartelle che risiedono su volumi misti di tipo sicurezza.

Per impostazione predefinita, quando viene creato un descrittore di protezione, vengono aggiunte quattro voci di controllo di accesso (ACE) DACL (Discretionary Access Control List) a tale descrittore di protezione. Le quattro ACE predefinite sono le seguenti:

Oggetto	Tipo di accesso	Diritti di accesso	Dove applicare le autorizzazioni
BUILTIN/amministratori	Consentire	Controllo completo	questa-cartella, sottocartelle, file
BUILTIN/utenti	Consentire	Controllo completo	questa-cartella, sottocartelle, file
PROPRIETARIO DEL CREATOR	Consentire	Controllo completo	questa-cartella, sottocartelle, file
AUTORITÀ/SISTEMA NT	Consentire	Controllo completo	questa-cartella, sottocartelle, file

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Proprietario del descrittore di protezione
- Gruppo primario del proprietario
- Flag di controllo raw

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

## Fasi

1. Se si desidera utilizzare i parametri avanzati, impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Creare un descrittore di sicurezza: `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_name optional_parameters`

```
vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe
```

3. Verificare che la configurazione del descrittore di protezione sia corretta: `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

```
vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
Security Descriptor Name: sd1
Owner of the Security Descriptor: DOMAIN\joe
```

4. Se si è nel livello di privilegio avanzato, tornare al livello di privilegio admin: `set -privilege admin`

## Aggiungere le voci di controllo dell'accesso NTFS SACL al descrittore di protezione NTFS

L'aggiunta di voci di controllo di accesso (ACE) SACL (elenco di controllo di accesso al sistema) al descrittore di protezione NTFS è la seconda fase della creazione di criteri di controllo NTFS per file o cartelle in SVM. Ogni voce identifica l'utente o il gruppo che si desidera controllare. La voce SACL definisce se si desidera controllare i tentativi di accesso riusciti o non riusciti.

### A proposito di questa attività

È possibile aggiungere uno o più ACE al SACL del descrittore di protezione.

Se il descrittore di protezione contiene un SACL con ACE esistenti, il comando aggiunge il nuovo ACE al SACL. Se il descrittore di protezione non contiene un SACL, il comando crea il SACL e aggiunge il nuovo ACE.

È possibile configurare le voci SACL specificando i diritti da controllare per gli eventi di successo o di errore per l'account specificato in `-account` parametro. Esistono tre metodi di esclusione reciproca per specificare i diritti:

- Diritti
- Diritti avanzati
- Diritti raw (privilegio avanzato)



Se non si specificano i diritti per la voce SACL, l'impostazione predefinita è `Full Control`.

È possibile personalizzare le voci SACL specificando come applicare l'ereditarietà con `apply to` parametro.

Se non si specifica questo parametro, l'impostazione predefinita prevede l'applicazione di questa voce SACL a questa cartella, sottocartelle e file.

## Fasi

1. Aggiungere una voce SACL a un descrittore di protezione: `vserver security file-directory ntfs sac1 add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs sac1 add -ntfs-sd sd1 -access-type failure -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. Verificare che la voce SACL sia corretta: `vserver security file-directory ntfs sac1 show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sac1 show -vserver vs1 -ntfs-sd sd1 -access-type deny -account domain\joe
```

```
Vserver: vs1
Security Descriptor Name: sd1
Access type for Specified Access Rights: failure
Account Name or SID: DOMAIN\joe
Access Rights: full-control
Advanced Access Rights: -
Apply To: this-folder
Access Rights: full-control
```

## Creare policy di sicurezza

La creazione di un criterio di audit per le macchine virtuali di storage (SVM) è la terza fase della configurazione e dell'applicazione degli ACL a un file o a una cartella. Un criterio agisce come un contenitore per varie attività, in cui ogni attività è una singola voce che può essere applicata a file o cartelle. È possibile aggiungere attività al criterio di protezione in un secondo momento.

### A proposito di questa attività

Le attività aggiunte a un criterio di protezione contengono associazioni tra il descrittore di protezione NTFS e i percorsi di file o cartelle. Pertanto, è necessario associare la policy di sicurezza a ciascuna macchina virtuale di storage (SVM) (contenente volumi di sicurezza NTFS o volumi misti di sicurezza).

## Fasi

1. Creare una policy di sicurezza: `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver vs1
```



## 2. Verificare la policy di sicurezza: `vserver security file-directory policy show`

```
vserver security file-directory policy show
Vserver          Policy Name
-----
vs1              policy1
```

### Aggiungere un'attività alla policy di sicurezza

La creazione e l'aggiunta di un'attività di policy a un criterio di sicurezza è la quarta fase della configurazione e dell'applicazione degli ACL a file o cartelle in SVM. Quando si crea l'attività relativa ai criteri, l'attività viene associata a un criterio di protezione. È possibile aggiungere una o più voci di attività a un criterio di protezione.

#### A proposito di questa attività

La policy di sicurezza è un container per un'attività. Un'attività si riferisce a una singola operazione che può essere eseguita da un criterio di protezione a file o cartelle con NTFS o protezione mista (o a un oggetto volume se si configura Storage-Level Access Guard).

Esistono due tipi di attività:

- Attività di file e directory

Consente di specificare le attività che applicano i descrittori di protezione a file e cartelle specifici. Gli ACL applicati attraverso le attività di file e directory possono essere gestiti con client SMB o CLI ONTAP.

- Attività di Access Guard a livello di storage

Consente di specificare le attività che applicano i descrittori di protezione di Storage-Level Access Guard a un volume specificato. Gli ACL applicati tramite le attività di Access Guard a livello di storage possono essere gestiti solo tramite l'interfaccia utente di ONTAP.

Un'attività contiene le definizioni per la configurazione di sicurezza di un file (o di una cartella) o di un set di file (o di cartelle). Ogni attività di una policy è identificata in modo univoco dal percorso. Un'unica attività per percorso può essere presente all'interno di un singolo criterio. Un criterio non può avere voci di attività duplicate.

Linee guida per l'aggiunta di un'attività a un criterio:

- È possibile includere un massimo di 10,000 voci di attività per policy.
- Un criterio può contenere una o più attività.

Anche se un criterio può contenere più attività, non è possibile configurare un criterio in modo che contenga sia le attività file-directory che Storage-Level Access Guard. Un criterio deve contenere tutte le attività Storage-Level Access Guard o tutte le attività di file-directory.

- Storage-Level Access Guard viene utilizzato per limitare le autorizzazioni.

Non assegnerà mai autorizzazioni di accesso aggiuntive.

È possibile personalizzare la configurazione del descrittore di protezione utilizzando i seguenti parametri opzionali:

- Tipo di sicurezza
- Modalità di propagazione
- Posizione dell'indice
- Tipo di controllo dell'accesso

Il valore di qualsiasi parametro opzionale viene ignorato per Storage-Level Access Guard. Per ulteriori informazioni, consulta le pagine man.

**Fasi**

1. Aggiungere un'attività con un descrittore di protezione associato al criterio di protezione: `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

`file-directory` è il valore predefinito di `-access-control` parametro. La specifica del tipo di controllo dell'accesso durante la configurazione delle attività di accesso a file e directory è facoltativa.

```
vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
```

2. Verificare la configurazione dell'attività del criterio: `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

Vserver: vs1  
Policy: policy1

Index	File/Folder	Access	Security	NTFS	NTFS
Security	Path	Control	Type	Mode	
Descriptor Name					
-----	-----	-----	-----	-----	
-----					
1	/home/dir1	file-directory	ntfs	propagate	sd2

**Applicare le policy di sicurezza**

L'applicazione di un criterio di audit alle SVM è l'ultimo passo nella creazione e nell'applicazione di ACL NTFS a file o cartelle.

**A proposito di questa attività**

È possibile applicare le impostazioni di protezione definite nel criterio di protezione ai file e alle cartelle NTFS che risiedono nei volumi FlexVol (NTFS o stile di protezione misto).



Quando vengono applicati un criterio di audit e i SACL associati, tutti i DACL esistenti vengono sovrascritti. Quando vengono applicati un criterio di protezione e i DACL associati, tutti i DACL esistenti vengono sovrascritti. Prima di crearne e applicarne di nuovi, è necessario rivedere le policy di sicurezza esistenti.

## Fase

1. Applicare una policy di sicurezza: `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

Il processo di applicazione della policy viene pianificato e viene restituito l'ID lavoro.

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
```

## Monitorare il processo di policy di sicurezza

Quando si applica la policy di sicurezza alle macchine virtuali di storage (SVM), è possibile monitorare l'avanzamento dell'attività monitorando il processo di policy di sicurezza. Ciò è utile se si desidera verificare che l'applicazione del criterio di protezione sia riuscita. Questo è utile anche se si dispone di un processo a esecuzione prolungata in cui si applica la protezione in blocco a un gran numero di file e cartelle.

### A proposito di questa attività

Per visualizzare informazioni dettagliate su un processo di policy di sicurezza, utilizzare `-instance` parametro.

## Fase

1. Monitorare il processo di policy di sicurezza: `vserver security file-directory job show -vserver vserver_name`

```
vserver security file-directory job show -vserver vs1
```

Job ID	Name	Vserver	Node	State
53322	Fsecurity Apply	vs1	node1	Success
Description: File Directory Security Apply Job				

## Verificare la policy di audit applicata

È possibile verificare il criterio di controllo per confermare che i file o le cartelle sulla macchina virtuale di storage (SVM) a cui è stato applicato il criterio di protezione dispongano delle impostazioni di sicurezza di controllo desiderate.

## A proposito di questa attività

Si utilizza `vserver security file-directory show` comando per visualizzare le informazioni sui criteri di controllo. Specificare il nome della SVM che contiene i dati e il percorso dei dati di cui si desidera visualizzare le informazioni sui criteri di controllo del file o della cartella.

### Fase

1. Visualizzare le impostazioni dei criteri di controllo: `vserver security file-directory show -vserver vserver_name -path path`

### Esempio

Il seguente comando visualizza le informazioni di policy di audit applicate al percorso “/corp” in SVM vs1. Il percorso ha applicato sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA:

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

      Vserver: vs1
      File Path: /corp
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

### Considerazioni per la gestione dei processi di policy di sicurezza

Se esiste un processo di policy di sicurezza, in determinate circostanze non è possibile modificare tale policy o le attività assegnate a tale policy. È necessario comprendere in quali condizioni è possibile o meno modificare le policy di sicurezza in modo che i tentativi di modifica vengano eseguiti correttamente. Le modifiche al criterio includono l'aggiunta, la rimozione o la modifica delle attività assegnate al criterio e l'eliminazione o

la modifica del criterio.

Non è possibile modificare un criterio di protezione o un'attività assegnata a tale criterio se esiste un processo per tale criterio e tale processo si trova nei seguenti stati:

- Il lavoro è in esecuzione o in corso.
- Il processo viene messo in pausa.
- Il lavoro viene ripreso e si trova in esecuzione.
- Se il processo è in attesa di eseguire il failover su un altro nodo.

Nei seguenti casi, se esiste un processo per un criterio di protezione, è possibile modificare correttamente tale criterio di protezione o un'attività assegnata a tale criterio:

- Il processo di policy viene arrestato.
- Il processo di policy è stato completato correttamente.

#### Comandi per la gestione dei descrittori di sicurezza NTFS

Esistono comandi ONTAP specifici per la gestione dei descrittori di protezione. È possibile creare, modificare, eliminare e visualizzare informazioni sui descrittori di protezione.

Se si desidera...	Utilizzare questo comando...
Creare descrittori di protezione NTFS	<code>vserver security file-directory ntfs create</code>
Modificare i descrittori di protezione NTFS esistenti	<code>vserver security file-directory ntfs modify</code>
Visualizza informazioni sui descrittori di protezione NTFS esistenti	<code>vserver security file-directory ntfs show</code>
Eliminare i descrittori di protezione NTFS	<code>vserver security file-directory ntfs delete</code>

Vedere le pagine man per `vserver security file-directory ntfs` per ulteriori informazioni.

#### Comandi per la gestione delle voci di controllo degli accessi NTFS DACL

Esistono comandi ONTAP specifici per la gestione delle voci di controllo degli accessi DACL (Access Control). È possibile aggiungere ACE ai DACL NTFS in qualsiasi momento. È inoltre possibile gestire i DACL NTFS esistenti modificando, eliminando e visualizzando le informazioni relative agli ACE nei DACL.

Se si desidera...	Utilizzare questo comando...
Creare ACE e aggiungerli ai DACL NTFS	<code>vserver security file-directory ntfs dacl add</code>
Modificare gli ACE esistenti nei DACL NTFS	<code>vserver security file-directory ntfs dacl modify</code>
Visualizza le informazioni sugli ACE esistenti nei DACL NTFS	<code>vserver security file-directory ntfs dacl show</code>
Rimuovere gli ACE esistenti dai DACL NTFS	<code>vserver security file-directory ntfs dacl remove</code>

Vedere le pagine man per `vserver security file-directory ntfs dacl` per ulteriori informazioni.

#### Comandi per la gestione delle voci di controllo degli accessi NTFS SACL

Esistono comandi ONTAP specifici per la gestione delle voci di controllo degli accessi SACL (ACE). È possibile aggiungere ACE ai SACL NTFS in qualsiasi momento. È inoltre possibile gestire i SACL NTFS esistenti modificando, eliminando e visualizzando le informazioni relative agli ACE nei SACL.

Se si desidera...	Utilizzare questo comando...
Creare ACE e aggiungerli ai SACL NTFS	<code>vserver security file-directory ntfs sacl add</code>
Modificare gli ACE esistenti nei SACL NTFS	<code>vserver security file-directory ntfs sacl modify</code>
Visualizza le informazioni sugli ACE esistenti nei SACL NTFS	<code>vserver security file-directory ntfs sacl show</code>
Rimuovere gli ACE esistenti dai SACL NTFS	<code>vserver security file-directory ntfs sacl remove</code>

Vedere le pagine man per `vserver security file-directory ntfs sacl` per ulteriori informazioni.

#### Comandi per la gestione delle policy di sicurezza

Esistono comandi ONTAP specifici per la gestione delle policy di sicurezza. È possibile visualizzare informazioni sui criteri ed eliminare i criteri. Non è possibile modificare un criterio di protezione.

Se si desidera...	Utilizzare questo comando...
Creare policy di sicurezza	<code>vserver security file-directory policy create</code>
Visualizzare informazioni sulle policy di sicurezza	<code>vserver security file-directory policy show</code>
Eliminare le policy di sicurezza	<code>vserver security file-directory policy delete</code>

Vedere le pagine man per `vserver security file-directory policy` per ulteriori informazioni.

#### Comandi per la gestione delle attività dei criteri di protezione

Sono disponibili comandi ONTAP per aggiungere, modificare, rimuovere e visualizzare informazioni sulle attività dei criteri di protezione.

Se si desidera...	Utilizzare questo comando...
Aggiungere attività di policy di sicurezza	<code>vserver security file-directory policy task add</code>
Modificare le attività dei criteri di protezione	<code>vserver security file-directory policy task modify</code>
Visualizza informazioni sulle attività dei criteri di protezione	<code>vserver security file-directory policy task show</code>
Rimuovere le attività dei criteri di protezione	<code>vserver security file-directory policy task remove</code>

Vedere le pagine man per `vserver security file-directory policy task` per ulteriori informazioni.

#### Comandi per la gestione dei processi di policy di sicurezza

Sono disponibili comandi ONTAP per mettere in pausa, riprendere, arrestare e visualizzare informazioni sui processi relativi ai criteri di protezione.

Se si desidera...	Utilizzare questo comando...
Sospendere i processi di policy di sicurezza	<code>vserver security file-directory job pause -vserver vserver_name -id integer</code>
Riprendere i processi di policy di sicurezza	<code>vserver security file-directory job resume -vserver vserver_name -id integer</code>

Se si desidera...	Utilizzare questo comando...
Visualizza informazioni sui processi di policy di sicurezza	<code>vserver security file-directory job show -vserver vserver_name</code> È possibile determinare l'ID lavoro di un lavoro utilizzando questo comando.
Arrestare i processi di policy di sicurezza	<code>vserver security file-directory job stop -vserver vserver_name -id integer</code>

Vedere le pagine man per `vserver security file-directory job` per ulteriori informazioni.

## Configurare la cache dei metadati per le condivisioni SMB

### Come funziona il caching dei metadati SMB

Il caching dei metadati consente il caching degli attributi dei file sui client SMB 1.0 per fornire un accesso più rapido agli attributi di file e cartelle. È possibile attivare o disattivare il caching degli attributi in base alla condivisione. È inoltre possibile configurare il time-to-live per le voci memorizzate nella cache se è attivata la cache dei metadati. La configurazione del caching dei metadati non è necessaria se i client si connettono alle condivisioni tramite SMB 2.x o SMB 3.0.

Quando questa opzione è attivata, la cache dei metadati SMB memorizza i dati di attributi di percorso e file per un periodo di tempo limitato. Ciò può migliorare le performance delle PMI per i client SMB 1.0 con carichi di lavoro comuni.

Per alcune attività, SMB crea una quantità significativa di traffico che può includere più query identiche per i metadati di percorso e file. È possibile ridurre il numero di query ridondanti e migliorare le performance per i client SMB 1.0 utilizzando il caching dei metadati SMB per recuperare le informazioni dalla cache.



Sebbene improbabile, è possibile che la cache dei metadati serva informazioni obsolete ai client SMB 1.0. Se il tuo ambiente non può permettersi questo rischio, non dovresti attivare questa funzionalità.

### Attivare la cache dei metadati SMB

È possibile migliorare le performance SMB per i client SMB 1.0 attivando la cache dei metadati SMB. Per impostazione predefinita, il caching dei metadati SMB è disattivato.

#### Fase

1. Eseguire l'azione desiderata:

Se si desidera...	Immettere il comando...
Attiva il caching dei metadati SMB quando crei una condivisione	<code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties attributecache</code>



Se si desidera...	Immettere il comando...
Abilitare il caching dei metadati SMB su una condivisione esistente	<pre>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties attributecache</pre>

## Informazioni correlate

[Configurazione della durata delle voci della cache dei metadati SMB](#)

[Aggiunta o rimozione delle proprietà di condivisione su una condivisione SMB esistente](#)

## Configurare la durata delle voci della cache dei metadati SMB

È possibile configurare la durata delle voci della cache dei metadati SMB per ottimizzare le prestazioni della cache dei metadati SMB nel proprio ambiente. L'impostazione predefinita è 10 secondi.

## Prima di iniziare

È necessario aver attivato la funzione cache dei metadati SMB. Se il caching dei metadati SMB non è attivato, l'impostazione TTL della cache SMB non viene utilizzata.

## Fase

1. Eseguire l'azione desiderata:

Se si desidera configurare la durata delle voci della cache dei metadati SMB quando...	Immettere il comando...
Creare una condivisione	<pre>vserver cifs share -create -vserver vserver_name -share-name share_name -path path -attribute-cache-ttl [integerh][integerm][integers]</pre>
Modificare una condivisione esistente	<pre>vserver cifs share -modify -vserver vserver_name -share-name share_name -attribute-cache-ttl [integerh][integerm][integers]</pre>

È possibile specificare ulteriori proprietà e opzioni di configurazione della condivisione quando si creano o modificano le condivisioni. Per ulteriori informazioni, consulta le pagine man.

## Gestire i blocchi dei file

### Informazioni sul blocco dei file tra protocolli

Il blocco dei file è un metodo utilizzato dalle applicazioni client per impedire a un utente di accedere a un file precedentemente aperto da un altro utente. Il modo in cui ONTAP blocca i file dipende dal protocollo del client.

Se il client è un client NFS, i blocchi sono avvisi; se il client è un client SMB, i blocchi sono obbligatori.

A causa delle differenze tra i blocchi di file NFS e SMB, un client NFS potrebbe non riuscire ad accedere a un file precedentemente aperto da un'applicazione SMB.

Quando un client NFS tenta di accedere a un file bloccato da un'applicazione SMB, si verifica quanto segue:

- In volumi misti o NTFS, operazioni di manipolazione dei file come `rm`, `rmdir`, e `mv` Può causare il malfunzionamento dell'applicazione NFS.
- Le operazioni di lettura e scrittura NFS sono negate rispettivamente dalle modalità aperta di negazione-lettura e di negazione-scrittura di SMB.
- Le operazioni di scrittura NFS non riescono quando l'intervallo scritto del file è bloccato con un esclusivo bytelock SMB.

- **Scollega**

- Per i file system NTFS, sono supportate operazioni di eliminazione SMB e CIFS.

Il file verrà rimosso dopo l'ultima chiusura.

- Le operazioni di scollegamento NFS non sono supportate.

Non è supportato perché sono necessarie semantiche NTFS e SMB e l'ultima operazione Delete-on-Close non è supportata per NFS.

- Per i filesystem UNIX, è supportata l'operazione di scollegamento.

È supportato perché sono richieste semantiche NFS e UNIX.

- **Rinominare**

- Per i file system NTFS, se il file di destinazione viene aperto da SMB o CIFS, il file di destinazione può essere rinominato.
  - La ridenominazione NFS non è supportata.

Non è supportato perché sono necessarie semantiche NTFS e SMB.

Nei volumi UNIX di sicurezza, le operazioni di sconnessione e ridenominazione NFS ignorano lo stato di blocco SMB e consentono l'accesso al file. Tutte le altre operazioni NFS sui volumi UNIX di sicurezza rispettano lo stato di blocco SMB.

#### **Come ONTAP tratta i bit di sola lettura**

Il bit di sola lettura viene impostato file per file per indicare se un file è scrivibile (disattivato) o di sola lettura (abilitato).

I client SMB che utilizzano Windows possono impostare un bit di sola lettura per ogni file. I client NFS non impostano un bit di sola lettura per ogni file perché i client NFS non eseguono operazioni di protocollo che utilizzano un bit di sola lettura per ogni file.

ONTAP può impostare un bit di sola lettura su un file quando un client SMB che utilizza Windows crea tale file. ONTAP può anche impostare un bit di sola lettura quando un file viene condiviso tra client NFS e client SMB. Alcuni software, se utilizzati dai client NFS e dai client SMB, richiedono l'abilitazione del bit di sola lettura.

Affinché ONTAP mantenga le autorizzazioni di lettura e scrittura appropriate su un file condiviso tra client NFS

e client SMB, tratta il bit di sola lettura in base alle seguenti regole:

- NFS considera qualsiasi file con il bit di sola lettura abilitato come se non abbia alcun bit di permesso di scrittura abilitato.
- Se un client NFS disattiva tutti i bit di permesso di scrittura e almeno uno di questi bit era stato precedentemente attivato, ONTAP attiva il bit di sola lettura per quel file.
- Se un client NFS attiva qualsiasi bit di autorizzazione di scrittura, ONTAP disattiva il bit di sola lettura per quel file.
- Se il bit di sola lettura per un file è attivato e un client NFS tenta di rilevare le autorizzazioni per il file, i bit di autorizzazione per il file non vengono inviati al client NFS; invece, ONTAP invia i bit di autorizzazione al client NFS con i bit di autorizzazione di scrittura mascherati.
- Se il bit di sola lettura per un file è attivato e un client SMB disattiva il bit di sola lettura, ONTAP attiva il bit di autorizzazione di scrittura del proprietario per il file.
- I file con il bit di sola lettura abilitato sono scrivibili solo da root.



Le modifiche alle autorizzazioni dei file hanno effetto immediato sui client SMB, ma potrebbero non avere effetto immediato sui client NFS se il client NFS attiva il caching degli attributi.

#### In che modo ONTAP si differenzia da Windows per la gestione dei blocchi sui componenti del percorso di condivisione

A differenza di Windows, ONTAP non blocca ogni componente del percorso di un file aperto mentre il file è aperto. Questo comportamento influisce anche sui percorsi di condivisione SMB.

Poiché ONTAP non blocca ogni componente del percorso, è possibile rinominare un componente del percorso sopra il file aperto o la condivisione, che può causare problemi per alcune applicazioni o causare l'invalidità del percorso di condivisione nella configurazione SMB. Questo può rendere la condivisione inaccessibile.

Per evitare problemi causati dalla ridenominazione dei componenti del percorso, è possibile applicare impostazioni di sicurezza che impediscono agli utenti o alle applicazioni di rinominare le directory critiche.

#### Visualizza informazioni sui blocchi

È possibile visualizzare informazioni sui blocchi di file correnti, inclusi i tipi di blocchi che vengono conservati e lo stato di blocco, i dettagli sui blocchi dell'intervallo di byte, le modalità sharelock, i blocchi di delega e i blocchi opportunistici e se i blocchi vengono aperti con handle durevoli o persistenti.

#### A proposito di questa attività

L'indirizzo IP del client non può essere visualizzato per i blocchi stabiliti tramite NFSv4 o NFSv4.1.

Per impostazione predefinita, il comando visualizza le informazioni relative a tutti i blocchi. È possibile utilizzare i parametri dei comandi per visualizzare informazioni sui blocchi di una specifica macchina virtuale di storage (SVM) o per filtrare l'output del comando in base ad altri criteri.

Il `vserver locks show` il comando visualizza informazioni su quattro tipi di blocchi:

- Blocchi byte-range, che bloccano solo una parte di un file.
- Blocchi di condivisione che bloccano i file aperti.

- Blocchi opportunistici, che controllano il caching lato client su SMB.
- Deleghe, che controllano il caching lato client su NFSv4.x.

Specificando i parametri opzionali, è possibile determinare informazioni importanti su ciascun tipo di blocco. Per ulteriori informazioni, vedere la pagina man per il comando.

## Fase

1. Visualizzare le informazioni sui blocchi utilizzando `vserver locks show` comando.

## Esempi

Nell'esempio riportato di seguito vengono visualizzate informazioni riepilogative per un blocco NFSv4 su un file con il percorso `/vol1/file1`. La modalità di accesso sharelock è `write-deny_none` e il blocco è stato concesso con delega di scrittura:

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path          LIF          Protocol  Lock Type  Client
-----
-----
vol1    /vol1/file1               lif1         nfsv4     share-level -
                                     Sharelock Mode: write-deny_none
                                     delegation  -
                                     Delegation Type: write
```

Nell'esempio riportato di seguito vengono visualizzate informazioni dettagliate sull'oplock e sullo sharlock relative al blocco SMB in un file con il percorso `/data2/data2_2/intro.pptx`. Un handle durevole viene concesso sul file con una modalità di accesso con blocco della condivisione `write-deny_none` a un client con un indirizzo IP 10.3.1.3. Un oplock di leasing viene concesso con un livello di oplock batch:

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

Vserver: vs1
Volume: data2_2
Logical Interface: lif2
Object Path: /data2/data2_2/intro.pptx
Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
Lock Protocol: cifs
Lock Type: share-level
Node Holding Lock State: node3
Lock State: granted
Bytelock Starting Offset: -
Number of Bytes Locked: -
Bytelock is Mandatory: -
Bytelock is Exclusive: -
Bytelock is Superlock: -
```

```

    Bytelock is Soft: -
        Oplock Level: -
Shared Lock Access Mode: write-deny_none
    Shared Lock is Soft: false
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: durable
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

        Vserver: vs1
            Volume: data2_2
Logical Interface: lif2
    Object Path: /data2/data2_2/test.pptx
        Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
            Lock Protocol: cifs
                Lock Type: op-lock
Node Holding Lock State: node3
    Lock State: granted
Bytelock Starting Offset: -
    Number of Bytes Locked: -
        Bytelock is Mandatory: -
        Bytelock is Exclusive: -
        Bytelock is Superlock: -
            Bytelock is Soft: -
                Oplock Level: batch
Shared Lock Access Mode: -
    Shared Lock is Soft: -
        Delegation Type: -
            Client Address: 10.3.1.3
                SMB Open Type: -
                    SMB Connect State: connected
SMB Expiration Time (Secs): -
    SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

```

### Blocchi di interruzione

Quando i blocchi di file impediscono l'accesso dei client ai file, è possibile visualizzare le informazioni sui blocchi attualmente in attesa e quindi interrompere blocchi specifici. Esempi di scenari in cui potrebbe essere necessario interrompere i blocchi includono il debug delle applicazioni.

### A proposito di questa attività

Il `vserver locks break` il comando è disponibile solo a un livello di privilegio avanzato e superiore. La pagina man del comando contiene informazioni dettagliate.

## Fasi

1. Per trovare le informazioni necessarie per interrompere un blocco, utilizzare `vserver locks show` comando.

La pagina man del comando contiene informazioni dettagliate.

2. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
3. Eseguire una delle seguenti operazioni:

Se si desidera interrompere un blocco specificando...	Immettere il comando...
Il nome SVM, il nome del volume, il nome LIF e il percorso del file	<code>vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif</code>
L'ID blocco	<code>vserver locks break -lockid UUID</code>

4. Tornare al livello di privilegio admin: `set -privilege admin`

## Monitorare l'attività delle PMI

### Visualizzare le informazioni sulla sessione SMB

È possibile visualizzare informazioni sulle sessioni SMB stabilite, tra cui la connessione SMB, l'ID della sessione e l'indirizzo IP della workstation che utilizza la sessione. È possibile visualizzare informazioni sulla versione del protocollo SMB della sessione e sul livello di protezione continuamente disponibile, per identificare se la sessione supporta operazioni senza interruzioni.

### A proposito di questa attività

È possibile visualizzare le informazioni relative a tutte le sessioni della SVM in forma di riepilogo. Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali:

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output relativo ai campi scelti.

È possibile immettere `-fields ?` per determinare quali campi è possibile utilizzare.

- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sulle sessioni SMB stabilite.
- È possibile utilizzare `-fields` o il `-instance` parametro da solo o in combinazione con altri parametri opzionali.

## Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le informazioni sulla sessione SMB...	Immettere il seguente comando...
Per tutte le sessioni su SVM in forma di riepilogo	<code>vserver cifs session show -vserver vserver_name</code>
Su un ID di connessione specificato	<code>vserver cifs session show -vserver vserver_name -connection-id integer</code>
Da un indirizzo IP della workstation specificato	<code>vserver cifs session show -vserver vserver_name -address workstation_IP_address</code>
Su un indirizzo IP LIF specificato	<code>vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address</code>
Su un nodo specificato	<code>`vserver cifs session show -vserver vserver_name -node {node_name</code>
local}`	Da un utente Windows specificato
<code>vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name</code>	Con un meccanismo di autenticazione specificato
<code>`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1</code>	NTLMv2
Kerberos	Anonymous}`
Con una versione del protocollo specificata	<code>`vserver cifs session show -vserver vserver_name -protocol-version {SMB1</code>
SMB2	SMB2_1
SMB3	SMB3_1}`
	<p>[NOTE]</p> <p>====</p> <p>La protezione a disponibilità continua e SMB Multichannel sono disponibili solo su SMB 3.0 e sessioni successive. Per visualizzarne lo stato in tutte le sessioni qualificanti, specificare questo parametro con il valore impostato su SMB3 o versioni successive.</p> <p>====</p>

Se si desidera visualizzare le informazioni sulla sessione SMB...	Immettere il seguente comando...
Con un livello specifico di protezione a disponibilità continua	<code>`vserver cifs session show -vserver vserver_name -continuously-available {No</code>
Yes	<code>Partial}`</code>  <b>[NOTE]</b> ===== <p>Se lo stato di disponibilità continua è <code>Partial</code>, questo significa che la sessione contiene almeno un file aperto a disponibilità continua, ma la sessione ha alcuni file che non sono aperti con una protezione continuamente disponibile. È possibile utilizzare <code>vserver cifs sessions file show</code> comando per determinare quali file della sessione stabilita non sono aperti con una protezione continuamente disponibile.</p> =====
Con uno stato di sessione SMB Signing specificato	<code>`vserver cifs session show -vserver vserver_name -is-session-signed {true</code>

## Esempi

Il seguente comando visualizza le informazioni sulla sessione per le sessioni su SVM vs1 stabilite da una workstation con indirizzo IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID      Workstation    Windows User    Open      Idle
-----
3151272279,
3151272280,
3151272281  1      10.1.1.1      DOMAIN\joe      2         23s
```

Il seguente comando visualizza informazioni dettagliate sulla sessione per le sessioni con protezione continuamente disponibile su SVM vs1. La connessione è stata effettuata utilizzando l'account di dominio.



```
cluster1::> vserver cifs session show -instance -continuously-available  
Yes
```

```
Node: node1  
Vserver: vs1  
Session ID: 1  
Connection ID: 3151274158  
Incoming Data LIF IP Address: 10.2.1.1  
Workstation IP address: 10.1.1.2  
Authentication Mechanism: Kerberos  
Windows User: DOMAIN\SERVER1$  
UNIX User: pcuser  
Open Shares: 1  
Open Files: 1  
Open Other: 0  
Connected Time: 10m 43s  
Idle Time: 1m 19s  
Protocol Version: SMB3  
Continuously Available: Yes  
Is Session Signed: false  
User Authenticated as: domain-user  
NetBIOS Name: -  
SMB Encryption Status: Unencrypted
```

Il seguente comando visualizza le informazioni di sessione su una sessione che utilizza SMB 3.0 e SMB Multichannel su SVM vs1. Nell'esempio, l'utente si è connesso a questa condivisione da un client SMB 3.0 utilizzando l'indirizzo IP LIF; pertanto, il meccanismo di autenticazione è stato impostato su NTLMv2 per impostazione predefinita. La connessione deve essere effettuata utilizzando l'autenticazione Kerberos per connettersi con la protezione continuamente disponibile.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3
```

```

    Node: node1
    Vserver: vs1
    Session ID: 1
    **Connection IDs: 3151272607,31512726078,3151272609
    Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
    Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
        Windows User: DOMAIN\administrator
        UNIX User: pcuser
    Open Shares: 1
    Open Files: 0
    Open Other: 0
    Connected Time: 6m 22s
    Idle Time: 5m 42s
    Protocol Version: SMB3
    Continuously Available: No
    Is Session Signed: false
    User Authenticated as: domain-user
    NetBIOS Name: -
    SMB Encryption Status: Unencrypted
```

## Informazioni correlate

[Visualizzazione delle informazioni sui file SMB aperti](#)

### Visualizzare le informazioni sui file SMB aperti

È possibile visualizzare informazioni sui file SMB aperti, tra cui la connessione SMB e l'ID sessione, il volume di hosting, il nome della condivisione e il percorso di condivisione. È possibile visualizzare informazioni sul livello di protezione continuamente disponibile di un file, utile per determinare se un file aperto si trova in uno stato che supporta operazioni senza interruzioni.

### A proposito di questa attività

È possibile visualizzare informazioni sui file aperti in una sessione SMB stabilita. Le informazioni visualizzate sono utili quando è necessario determinare le informazioni della sessione SMB per determinati file all'interno di una sessione SMB.

Ad esempio, se si dispone di una sessione SMB in cui alcuni dei file aperti sono aperti con una protezione continuamente disponibile e alcuni non sono aperti con una protezione continuamente disponibile (il valore per `-continuously-available` campo in `vserver cifs session show` l'output del comando è `Partial`), è possibile determinare quali file non sono continuamente disponibili utilizzando questo comando.

È possibile visualizzare le informazioni relative a tutti i file aperti nelle sessioni SMB stabilite sulle macchine virtuali di storage (SVM) in forma riepilogativa utilizzando `vserver cifs session file show` senza

parametri opzionali.

Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali. Ciò può essere utile quando si desidera visualizzare informazioni solo per un piccolo sottoinsieme di file aperti.

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output nei campi scelti.  
È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.
- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sui file SMB aperti.  
È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.

## Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare i file SMB aperti...	Immettere il seguente comando...
Sul modulo SVM in forma di riepilogo	<code>vserver cifs session file show -vserver vserver_name</code>
Su un nodo specificato	<code>`vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}`</code>	Su un ID file specificato
<code>vserver cifs session file show -vserver vserver_name -file-id integer</code>	Su un ID connessione SMB specificato
<code>vserver cifs session file show -vserver vserver_name -connection-id integer</code>	Su un ID sessione SMB specificato
<code>vserver cifs session file show -vserver vserver_name -session-id integer</code>	Sull'aggregato di hosting specificato
<code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code>	Sul volume specificato
<code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code>	Sulla condivisione SMB specificata

Se si desidera visualizzare i file SMB aperti...	Immettere il seguente comando...
<code>vserver cifs session file show -vserver vserver_name -share share_name</code>	Sul percorso SMB specificato
<code>vserver cifs session file show -vserver vserver_name -path path</code>	Con il livello specificato di protezione a disponibilità continua
<code>`vserver cifs session file show -vserver vserver_name -continuously-available {No</code>	Yes}  [NOTE] ==== Se lo stato di disponibilità continua è No, questo significa che questi file aperti non sono in grado di eseguire il ripristino senza interruzioni dal takeover e dal giveback. Inoltre, non possono essere ripristinati dal trasferimento generale di aggregati tra partner in una relazione ad alta disponibilità.  ====
Con lo stato di riconnessione specificato	<code>`vserver cifs session file show -vserver vserver_name -reconnected {No</code>

Sono disponibili ulteriori parametri opzionali che è possibile utilizzare per perfezionare i risultati di output. Per ulteriori informazioni, consulta la pagina [man](#).

## Esempi

Nell'esempio seguente vengono visualizzate informazioni sui file aperti su SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:    1
File      File      Open Hosting      Continuously
ID        Type        Mode Volume      Share      Available
-----
41        Regular    r    data      data      Yes
Path: \mytest.rtf
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate sui file SMB aperti con ID file 82 su SVM vs1:

```
cluster1::> vsriver cifs session file show -vsriver vs1 -file-id 82
-instance
```

```
Node: node1
Vserver: vs1
File ID: 82
Connection ID: 104617
Session ID: 1
File Type: Regular
Open Mode: rw
Aggregate Hosting File: aggr1
Volume Hosting File: data1
CIFS Share: data1
Path from CIFS Share: windows\win8\test\test.txt
Share Mode: rw
Range Locks: 1
Continuously Available: Yes
Reconnected: No
```

## Informazioni correlate

[Visualizzazione delle informazioni sulla sessione SMB](#)

### Determinare quali oggetti e contatori statistici sono disponibili

Prima di ottenere informazioni su CIFS, SMB, audit e statistiche hash BranchCache e monitorare le performance, è necessario sapere quali oggetti e contatori sono disponibili per ottenere i dati.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera determinare...	Inserisci...
Quali oggetti sono disponibili	<code>statistics catalog object show</code>
Oggetti specifici disponibili	<code>statistics catalog object show object object_name</code>
Quali contatori sono disponibili	<code>statistics catalog counter show object object_name</code>

Per ulteriori informazioni sugli oggetti e i contatori disponibili, consultare le pagine man.

3. Tornare al livello di privilegio admin: `set -privilege admin`

## Esempi

Il seguente comando visualizza le descrizioni degli oggetti statistici selezionati relativi all'accesso CIFS e SMB nel cluster, come si vede al livello di privilegio avanzato:

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them only  
when directed to do so by support personnel.
```

```
Do you want to continue? {y|n}: y
```

```
cluster1::*> statistics catalog object show -object audit  
    audit_ng                CM object for exporting audit_ng  
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs  
    cifs                    The CIFS object reports activity of the  
                           Common Internet File System protocol  
                           ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs  
    nblade_cifs            The Common Internet File System (CIFS)  
                           protocol is an implementation of the  
Server  
                           ...
```

```
cluster1::*> statistics catalog object show -object smb1  
    smb1                   These counters report activity from the  
SMB  
                           revision of the protocol. For information  
                           ...
```

```
cluster1::*> statistics catalog object show -object smb2  
    smb2                   These counters report activity from the  
                           SMB2/SMB3 revision of the protocol. For  
                           ...
```

```
cluster1::*> statistics catalog object show -object hashd  
    hashd                  The hashd object provides counters to  
measure  
                           the performance of the BranchCache hash  
daemon.
```

```
cluster1::*> set -privilege admin
```

Il seguente comando visualizza informazioni su alcuni contatori di `cifs` oggetto visto a livello di privilegi avanzati:



In questo esempio non vengono visualizzati tutti i contatori disponibili per `cifs` oggetto; l'output è troncato.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

## Informazioni correlate

[Visualizzazione delle statistiche](#)

### Visualizzare le statistiche

È possibile visualizzare varie statistiche, tra cui statistiche su CIFS e SMB, audit e hash di BranchCache, per monitorare le performance e diagnosticare i problemi.

### Prima di iniziare

È necessario aver raccolto campioni di dati utilizzando `statistics start` e `statistics stop` prima di poter visualizzare informazioni sugli oggetti.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le statistiche per...	Inserisci...
Tutte le versioni di SMB	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x e SMB 3.0	<code>statistics show -object smb2</code>
Sottosistema CIFS del nodo	<code>statistics show -object nblade_cifs</code>
Audit multiprotocollo	<code>statistics show -object audit_ng</code>
Servizio hash BranchCache	<code>statistics show -object hashd</code>
DNS dinamico	<code>statistics show -object ddns_update</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

3. Tornare al livello di privilegio admin: `set -privilege admin`

## Informazioni correlate

[Determinazione degli oggetti e dei contatori delle statistiche disponibili](#)

[Monitoraggio delle statistiche delle sessioni firmate SMB](#)

[Visualizzazione delle statistiche di BranchCache](#)

[Utilizzo delle statistiche per monitorare l'attività di riferimento automatico del nodo](#)

["Configurazione SMB per Microsoft Hyper-V e SQL Server"](#)

["Configurazione del monitoraggio delle performance"](#)



## Implementare servizi basati su client SMB

### Utilizzare i file offline per consentire il caching dei file per l'utilizzo offline

#### Utilizzare i file offline per consentire il caching dei file per la panoramica dell'utilizzo offline

ONTAP supporta la funzione Microsoft Offline Files, o *caching lato client*, che consente di memorizzare i file nella cache dell'host locale per l'utilizzo offline. Gli utenti possono utilizzare la funzionalità offline Files per continuare a lavorare sui file anche quando sono disconnessi dalla rete.

È possibile specificare se i documenti utente e i programmi Windows vengono automaticamente memorizzati nella cache di una condivisione o se i file devono essere selezionati manualmente per il caching. Il caching manuale è attivato per impostazione predefinita per le nuove condivisioni. I file resi disponibili offline vengono sincronizzati sul disco locale del client Windows. La sincronizzazione si verifica quando viene ripristinata la connettività di rete a una specifica condivisione del sistema di storage.

Poiché i file e le cartelle offline mantengono le stesse autorizzazioni di accesso della versione dei file e delle cartelle salvati sul server CIFS, l'utente deve disporre di autorizzazioni sufficienti per i file e le cartelle salvati sul server CIFS per eseguire azioni sui file e sulle cartelle offline.

Quando l'utente e un altro utente della rete apportano modifiche allo stesso file, l'utente può salvare la versione locale del file nella rete, conservare l'altra versione o salvare entrambe. Se l'utente mantiene entrambe le versioni, un nuovo file con le modifiche dell'utente locale viene salvato localmente e il file memorizzato nella cache viene sovrascritto con le modifiche della versione del file salvato sul server CIFS.

È possibile configurare i file offline in base alla condivisione utilizzando le impostazioni di configurazione della condivisione. È possibile scegliere una delle quattro configurazioni di cartelle offline quando si creano o modificano le condivisioni:

- Nessun caching

Disattiva il caching lato client per la condivisione. I file e le cartelle non vengono automaticamente memorizzati nella cache locale sui client e gli utenti non possono scegliere di memorizzare nella cache i file o le cartelle localmente.

- Caching manuale

Consente la selezione manuale dei file da memorizzare nella cache della condivisione. Questa è l'impostazione predefinita. Per impostazione predefinita, nessun file o cartella viene memorizzato nella cache del client locale. Gli utenti possono scegliere i file e le cartelle da memorizzare nella cache locale per l'utilizzo offline.

- Caching automatico dei documenti

Consente di memorizzare automaticamente i documenti utente nella cache della condivisione. Solo i file e le cartelle a cui si accede vengono memorizzati nella cache locale.

- Caching automatico dei programmi

Consente ai programmi e ai documenti utente di essere automaticamente memorizzati nella cache della condivisione. Solo i file, le cartelle e i programmi a cui si accede vengono memorizzati nella cache locale. Inoltre, questa impostazione consente al client di eseguire file eseguibili memorizzati nella cache locale anche quando è connesso alla rete.

Per ulteriori informazioni sulla configurazione dei file offline su server e client Windows, consultare la Microsoft TechNet Library.

### Informazioni correlate

[Utilizzo di profili roaming per memorizzare i profili utente centralmente su un server CIFS associato a SVM](#)

[Utilizzo del reindirizzamento delle cartelle per memorizzare i dati su un server CIFS](#)

[Utilizzo di BranchCache per memorizzare nella cache SMB i contenuti vengono condivisi in una filiale](#)

["Microsoft TechNet Library: technet.microsoft.com/en-us/library/"](#)

### Requisiti per l'utilizzo di file offline

Prima di poter utilizzare la funzionalità file offline di Microsoft con il server CIFS, è necessario sapere quali versioni di ONTAP e SMB e quali client Windows supportano tale funzionalità.

### Requisiti di versione di ONTAP

Le release di ONTAP supportano i file offline.

### Requisiti di versione del protocollo SMB

Per le macchine virtuali di storage (SVM), ONTAP supporta i file offline su tutte le versioni di SMB.

### Requisiti del client Windows

Il client Windows deve supportare i file offline.

Per informazioni aggiornate sui client Windows che supportano la funzionalità file offline, vedere la matrice di interoperabilità.

["mysupport.netapp.com/matrix"](#)

### Linee guida per la distribuzione di file offline

Esistono alcune importanti linee guida da comprendere quando si distribuiscono file offline nelle condivisioni home directory che dispongono di `showsnapshot` proprietà di condivisione impostata nelle home directory.

Se il `showsnapshot` La proprietà Share viene impostata su una condivisione home directory con file offline configurati, i client Windows memorizzano nella cache tutte le copie Snapshot in `~snapshot` nella home directory dell'utente.

I client Windows memorizzano nella cache tutte le copie Snapshot nella home directory se si verifica una delle seguenti condizioni:

- L'utente rende la home directory disponibile offline dal client.

Il contenuto di `~snapshot` la cartella nella home directory viene inclusa e resa disponibile offline.

- L'utente configura il reindirizzamento delle cartelle per reindirizzare una cartella come `My Documents` Alla

directory principale di una home directory che risiede nella condivisione del server CIFS.

Alcuni client Windows potrebbero rendere automaticamente disponibile la cartella reindirizzata offline. Se la cartella viene reindirizzata alla directory principale della home directory, il `~snapshot` la cartella è inclusa nel contenuto offline memorizzato nella cache.



Implementazioni di file offline in cui `~snapshot` la cartella è inclusa nei file offline dovrebbe essere evitata. Le copie Snapshot in `~snapshot` La cartella contiene tutti i dati sul volume nel punto in cui ONTAP ha creato la copia Snapshot. Pertanto, è necessario creare una copia offline di `~snapshot` la cartella consuma un notevole storage locale sul client, consuma la larghezza di banda della rete durante la sincronizzazione dei file offline e aumenta il tempo necessario per la sincronizzazione dei file offline.

#### Configurare il supporto dei file offline sulle condivisioni SMB utilizzando la CLI

È possibile configurare il supporto dei file offline utilizzando l'interfaccia utente di ONTAP specificando una delle quattro impostazioni offline quando si creano condivisioni SMB o in qualsiasi momento modificando le condivisioni SMB esistenti. Il supporto manuale dei file offline è l'impostazione predefinita.

#### A proposito di questa attività

Quando si configura il supporto per i file offline, è possibile scegliere una delle seguenti quattro impostazioni per i file offline:

Impostazione	Descrizione
<code>none</code>	Non consente ai client Windows di memorizzare nella cache i file presenti in questa condivisione.
<code>manual</code>	Consente agli utenti sui client Windows di selezionare manualmente i file da memorizzare nella cache.
<code>documents</code>	Consente ai client Windows di memorizzare nella cache i documenti utente utilizzati dall'utente per l'accesso offline.
<code>programs</code>	Consente ai client Windows di memorizzare nella cache i programmi utilizzati dall'utente per l'accesso offline. I client possono utilizzare i file di programma memorizzati nella cache in modalità offline anche se la condivisione è disponibile.

È possibile scegliere una sola impostazione di file offline. Se si modifica un'impostazione dei file offline su una condivisione SMB esistente, la nuova impostazione dei file offline sostituisce l'impostazione originale. Le altre impostazioni di configurazione della condivisione SMB e le proprietà di condivisione esistenti non vengono rimosse o sostituite. Rimangono in vigore fino a quando non vengono esplicitamente rimossi o modificati.

#### Fasi

1. Eseguire l'azione appropriata:

Se si desidera configurare i file offline su...	Immettere il comando...
Una nuova condivisione SMB	<code>`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none</code>
manual	documents
programs}`	Una condivisione SMB esistente
<code>`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none</code>	manual
documents	programs}`

2. Verificare che la configurazione della condivisione SMB sia corretta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

### Esempio

Il seguente comando crea una condivisione SMB denominata “data1” con i file offline impostati su documents:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: Offline files
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: documents
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

Il seguente comando modifica una condivisione SMB esistente denominata “data1” modificando l'impostazione

dei file offline su `manual` e aggiungendo i valori per la maschera di creazione della modalità file e directory:

```
cluster1::> vsserver cifs share modify -vsserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data1
-instance
```

```

                Vserver: vs1
                Share: data1
    CIFS Server NetBIOS Name: VS1
                Path: /data1
        Share Properties: oplocks
                        browsable
                        changenotify
    Symlink Properties: enable
    File Mode Creation Mask: 644
    Directory Mode Creation Mask: 777
        Share Comment: Offline files
        Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                Volume Name: -
        Offline Files: manual
    Vscan File-Operations Profile: standard
    Maximum Tree Connections on Share: 4294967295
        UNIX Group for File Create: -
```

### Informazioni correlate

[Aggiunta o rimozione delle proprietà di condivisione su una condivisione SMB esistente](#)

**Configurare il supporto dei file offline sulle condivisioni SMB utilizzando la MMC Gestione computer**

Se si desidera consentire agli utenti di memorizzare i file nella cache locale per l'utilizzo offline, è possibile configurare il supporto dei file offline utilizzando la console MMC Gestione computer (Microsoft Management Console).

### Fasi

1. Per aprire MMC sul server Windows, in Esplora risorse fare clic con il pulsante destro del mouse sull'icona del computer locale, quindi selezionare **Gestisci**.
2. Nel pannello di sinistra, selezionare **Gestione computer**.
3. Selezionare **azione > connessione a un altro computer**.

Viene visualizzata la finestra di dialogo Select computer (Seleziona computer).

4. Digitare il nome del server CIFS o fare clic su **Browse** (Sfoglia) per individuare il server CIFS.

Se il nome del server CIFS corrisponde al nome host della macchina virtuale di storage (SVM), digitare il

nome SVM. Se il nome del server CIFS è diverso dal nome host SVM, digitare il nome del server CIFS.

5. Fare clic su **OK**.
6. Nella struttura della console, fare clic su **System Tools > Shared Folders**.
7. Fare clic su **shares**.
8. Nel riquadro dei risultati, fare clic con il pulsante destro del mouse sulla condivisione.
9. Fare clic su **Proprietà**.

Vengono visualizzate le proprietà della condivisione selezionata.

10. Nella scheda **Generale**, fare clic su **Impostazioni offline**.

Viene visualizzata la finestra di dialogo Offline Settings (Impostazioni offline).

11. Configurare le opzioni di disponibilità offline in base alle esigenze.
12. Fare clic su **OK**.

## **Utilizzare i profili roaming per memorizzare i profili utente centralmente su un server SMB associato a SVM**

Utilizza i profili di roaming per memorizzare i profili utente centralmente su un server SMB associato alla panoramica SVM

ONTAP supporta la memorizzazione dei profili di roaming Windows su un server CIFS associato alla macchina virtuale di storage (SVM). La configurazione dei profili di roaming degli utenti offre vantaggi all'utente, ad esempio la disponibilità automatica delle risorse, indipendentemente dalla posizione di accesso dell'utente. I profili roaming semplificano inoltre l'amministrazione e la gestione dei profili utente.

I profili utente comuni presentano i seguenti vantaggi:

- Disponibilità automatica delle risorse

Il profilo univoco di un utente è automaticamente disponibile quando l'utente accede a qualsiasi computer della rete che esegue Windows 8, Windows 7, Windows 2000 o Windows XP. Gli utenti non devono creare un profilo su ciascun computer in rete.

- Sostituzione semplificata del computer

Poiché tutte le informazioni del profilo dell'utente vengono conservate separatamente sulla rete, è possibile scaricare facilmente il profilo dell'utente su un nuovo computer sostitutivo. Quando l'utente accede al nuovo computer per la prima volta, la copia del profilo dell'utente sul server viene copiata nel nuovo computer.

### **Informazioni correlate**

[Utilizzo di file offline per consentire il caching dei file per l'utilizzo offline](#)

[Utilizzo del reindirizzamento delle cartelle per memorizzare i dati su un server CIFS](#)

## Requisiti per l'utilizzo dei profili di roaming

Prima di poter utilizzare i profili di roaming di Microsoft con il server CIFS, è necessario sapere quali versioni di ONTAP e SMB e quali client Windows supportano la funzionalità.

### Requisiti di versione di ONTAP

ONTAP supporta i profili di roaming.

### Requisiti di versione del protocollo SMB

Per le macchine virtuali di storage (SVM), ONTAP supporta i profili di roaming su tutte le versioni di SMB.

### Requisiti del client Windows

Prima che un utente possa utilizzare i profili di roaming, il client Windows deve supportare la funzione.

Per informazioni aggiornate sui client Windows che supportano i profili di roaming, consultare la matrice di interoperabilità.

["Tool di matrice di interoperabilità NetApp"](#)

## Configurare i profili di roaming

Se si desidera rendere automaticamente disponibile il profilo di un utente quando quest'ultimo effettua l'accesso a un computer della rete, è possibile configurare i profili di roaming tramite lo snap-in MMC utenti e computer di Active Directory. Se si configurano profili comuni su Windows Server, è possibile utilizzare il Centro di amministrazione di Active Directory.

### Fasi

1. Sul server Windows, aprire la MMC utenti e computer di Active Directory (o Active Directory Administration Center sui server Windows).
2. Individuare l'utente per cui si desidera configurare un profilo di roaming.
3. Fare clic con il pulsante destro del mouse sull'utente e fare clic su **Proprietà**.
4. Nella scheda **Profilo**, immettere il percorso del profilo per la condivisione in cui si desidera memorizzare il profilo di roaming dell'utente, seguito da %username%.

Ad esempio, il percorso di un profilo potrebbe essere il seguente:

\\vs1.example.com\profiles\%username%. La prima volta che un utente effettua l'accesso, %username% viene sostituito con il nome dell'utente.



Nel percorso \\vs1.example.com\profiles\%username%, profiles È il nome di condivisione di una condivisione su SVM (Storage Virtual Machine) vs1 con diritti di controllo completo per tutti.

5. Fare clic su **OK**.

## Utilizzare il reindirizzamento delle cartelle per memorizzare i dati su un server SMB

### Utilizzare il reindirizzamento delle cartelle per memorizzare i dati su una panoramica del server SMB

ONTAP supporta il reindirizzamento delle cartelle Microsoft, che consente agli utenti o agli amministratori di reindirizzare il percorso di una cartella locale a una posizione sul server CIFS. Sembra che le cartelle reindirizzate siano memorizzate sul client Windows locale, anche se i dati sono memorizzati in una condivisione SMB.

Il reindirizzamento delle cartelle è destinato principalmente alle organizzazioni che hanno già implementato le home directory e che desiderano mantenere la compatibilità con l'ambiente di home directory esistente.

- Documents, Desktop, e Start Menu sono esempi di cartelle che è possibile reindirizzare.
- Gli utenti possono reindirizzare le cartelle dal client Windows.
- Gli amministratori possono configurare e gestire centralmente il reindirizzamento delle cartelle configurando gli oggetti Criteri di gruppo in Active Directory.
- Se gli amministratori hanno configurato i profili di roaming, il reindirizzamento delle cartelle consente agli amministratori di dividere i dati degli utenti dai dati del profilo.
- Gli amministratori possono utilizzare il reindirizzamento delle cartelle e i file offline insieme per reindirizzare lo storage dei dati per le cartelle locali al server CIFS, consentendo allo stesso tempo agli utenti di memorizzare il contenuto nella cache locale.

### Informazioni correlate

[Utilizzo di file offline per consentire il caching dei file per l'utilizzo offline](#)

[Utilizzo di profili roaming per memorizzare i profili utente centralmente su un server CIFS associato a SVM](#)

### Requisiti per l'utilizzo del reindirizzamento delle cartelle

Prima di poter utilizzare il reindirizzamento delle cartelle Microsoft con il server CIFS, è necessario sapere quali versioni di ONTAP e SMB e quali client Windows supportano la funzionalità.

### Requisiti di versione di ONTAP

ONTAP supporta il reindirizzamento delle cartelle Microsoft.

### Requisiti di versione del protocollo SMB

Per le macchine virtuali di storage (SVM), ONTAP supporta il reindirizzamento delle cartelle Microsoft su tutte le versioni di SMB.

### Requisiti del client Windows

Prima che un utente possa utilizzare il reindirizzamento delle cartelle di Microsoft, il client Windows deve supportare questa funzionalità.

Per informazioni aggiornate sui client Windows che supportano il reindirizzamento delle cartelle, consultare la matrice di interoperabilità.

["mysupport.netapp.com/matrix"](https://mysupport.netapp.com/matrix)



## Configurare il reindirizzamento delle cartelle

È possibile configurare il reindirizzamento delle cartelle utilizzando la finestra Proprietà di Windows. Il vantaggio di utilizzare questo metodo consiste nel fatto che l'utente Windows può configurare il reindirizzamento delle cartelle senza l'assistenza dell'amministratore di SVM.

### Fasi

1. In Esplora risorse, fare clic con il pulsante destro del mouse sulla cartella che si desidera reindirizzare a una condivisione di rete.
2. Fare clic su **Proprietà**.

Vengono visualizzate le proprietà della condivisione selezionata.

3. Nella scheda **scelta rapida**, fare clic su **destinazione** e specificare il percorso di rete in cui si desidera reindirizzare la cartella selezionata.

Ad esempio, se si desidera reindirizzare una cartella a data in una home directory mappata a Q:\, specificare Q:\data come destinazione.

4. Fare clic su **OK**.

Per ulteriori informazioni sulla configurazione delle cartelle offline, consultare la Microsoft TechNet Library.

### Informazioni correlate

"Microsoft TechNet Library: [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)"

### Accedere alla directory ~snapshot dai client Windows utilizzando SMB 2.x.

Il metodo utilizzato per accedere a. ~snapshot La directory dei client Windows che utilizzano SMB 2.x differisce dal metodo utilizzato per SMB 1.0. È necessario conoscere le modalità di accesso a ~snapshot Directory quando si utilizzano connessioni SMB 2.x per accedere correttamente ai dati memorizzati nelle copie Snapshot.

L'amministratore di SVM controlla se gli utenti sui client Windows possono visualizzare e accedere a. ~snapshot directory su una condivisione attivando o disattivando showsnapshot condividere la proprietà utilizzando i comandi delle famiglie di proprietà di condivisione di vserver cifs.

Quando il showsnapshot La proprietà Share è disattivata, un utente su un client Windows che utilizza SMB 2.x non può visualizzare ~snapshot E non possono accedere alle copie Snapshot in ~snapshot directory, anche quando si immette manualmente il percorso di ~snapshot Directory o a copie Snapshot specifiche all'interno della directory.

Quando il showsnapshot La proprietà Share è attivata, un utente su un client Windows che utilizza SMB 2.x non può ancora visualizzare ~snapshot directory nella directory principale della condivisione o all'interno di qualsiasi giunzione o directory sotto la directory principale della condivisione. Tuttavia, dopo la connessione a una condivisione, l'utente può accedere a nascosto ~snapshot directory aggiungendo manualmente \~snapshot alla fine del percorso di condivisione. Il nascosto ~snapshot la directory è accessibile da due punti di ingresso:

- Alla radice della condivisione

- In ogni punto di giunzione nello spazio di condivisione

Il nascosto `~snapshot` la directory non è accessibile dalle sottodirectory non di giunzione all'interno della condivisione.

### Esempio

Con la configurazione illustrata nell'esempio seguente, un utente su un client Windows con una connessione SMB 2.x alla condivisione "eng" può accedere a `~snapshot` directory aggiungendo manualmente `~snapshot` al percorso di condivisione alla radice della condivisione e in ogni punto di giunzione del percorso. Il nascosto `~snapshot` la directory è accessibile dai tre percorsi seguenti:

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume          junction-path
-----
vs1      vs1_root        /
vs1      vs1_vol1        /eng
vs1      vs1_vol2        /eng/projects1
vs1      vs1_vol3        /eng/projects2

cluster1::> vsserver cifs share show
Vserver  Share  Path    Properties      Comment  ACL
-----
vs1      eng    /eng    oplocks         -        Everyone / Full Control
          chngenotify
          browsable
          showsnapshot
```

## Ripristinare file e cartelle utilizzando le versioni precedenti

### Panoramica sul ripristino di file e cartelle utilizzando le versioni precedenti

La possibilità di utilizzare le versioni precedenti di Microsoft è applicabile ai file system che supportano le copie Snapshot in qualche forma e le hanno attivate. La tecnologia Snapshot è parte integrante di ONTAP. Gli utenti possono ripristinare file e cartelle dalle copie Snapshot dal client Windows utilizzando la funzionalità delle versioni precedenti di Microsoft.

La funzionalità delle versioni precedenti offre agli utenti un metodo per sfogliare le copie Snapshot o per ripristinare i dati da una copia Snapshot senza l'intervento di un amministratore dello storage. Le versioni precedenti non sono configurabili. È sempre attivato. Se l'amministratore dello storage ha reso disponibili copie Snapshot in una condivisione, l'utente può utilizzare le versioni precedenti per eseguire le seguenti attività:

- Recuperare i file cancellati accidentalmente.

- Ripristino della sovrascrittura accidentale di un file.
- Confronta le versioni del file mentre lavori.

I dati memorizzati nelle copie Snapshot sono di sola lettura. Gli utenti devono salvare una copia di un file in un'altra posizione per apportare eventuali modifiche al file. Le copie Snapshot vengono periodicamente eliminate; pertanto, gli utenti devono creare copie dei file contenuti nelle versioni precedenti se desiderano conservare una versione precedente di un file a tempo indeterminato.

#### **Requisiti per l'utilizzo delle versioni precedenti di Microsoft**

Prima di poter utilizzare le versioni precedenti con il server CIFS, è necessario conoscere le versioni di ONTAP e SMB e i client Windows che lo supportano. È inoltre necessario conoscere il requisito di impostazione della copia Snapshot.

#### **Requisiti di versione di ONTAP**

Supporta le versioni precedenti.

#### **Requisiti di versione del protocollo SMB**

Per le macchine virtuali di storage (SVM), ONTAP supporta le versioni precedenti su tutte le versioni di SMB.

#### **Requisiti del client Windows**

Prima che un utente possa utilizzare le versioni precedenti per accedere ai dati nelle copie Snapshot, il client Windows deve supportare questa funzione.

Per informazioni aggiornate sui client Windows che supportano le versioni precedenti, consultare la matrice di interoperabilità.

["Tool di matrice di interoperabilità NetApp"](#)

#### **Requisiti per le impostazioni di copia Snapshot**

Per utilizzare le versioni precedenti per accedere ai dati nelle copie Snapshot, al volume contenente i dati deve essere associata una policy Snapshot attivata, i client devono poter accedere ai dati Snapshot e devono esistere copie Snapshot.

#### **Utilizzare la scheda versioni precedenti per visualizzare e gestire i dati di copia Snapshot**

Gli utenti sulle macchine client Windows possono utilizzare la scheda versioni precedenti della finestra Proprietà di Windows per ripristinare i dati memorizzati nelle copie Snapshot senza richiedere l'intervento dell'amministratore della macchina virtuale di storage (SVM).

#### **A proposito di questa attività**

È possibile utilizzare la scheda versioni precedenti solo per visualizzare e gestire i dati nelle copie Snapshot dei dati memorizzati sulla SVM se l'amministratore ha attivato le copie Snapshot sul volume contenente la condivisione e se l'amministratore configura la condivisione in modo che visualizzi le copie Snapshot.

#### **Fasi**

1. In Esplora risorse, visualizzare il contenuto dell'unità mappata dei dati memorizzati nel server CIFS.

2. Fare clic con il pulsante destro del mouse sul file o sulla cartella nell'unità di rete mappata di cui si desidera visualizzare o gestire le copie Snapshot.

3. Fare clic su **Proprietà**.

Vengono visualizzate le proprietà del file o della cartella selezionata.

4. Fare clic sulla scheda **versioni precedenti**.

Nella casella Folder Versions: (Versioni cartella) viene visualizzato un elenco di copie Snapshot disponibili del file o della cartella selezionata. Le copie Snapshot elencate sono identificate dal prefisso del nome della copia Snapshot e dall'indicatore data e ora di creazione.

5. Nella casella **versioni cartella**:, fare clic con il pulsante destro del mouse sulla copia del file o della cartella che si desidera gestire.

6. Eseguire l'azione appropriata:

Se si desidera...	Effettuare le seguenti operazioni...
Visualizzare i dati della copia Snapshot	Fare clic su <b>Apri</b> .
Creare una copia dei dati da tale copia Snapshot	Fare clic su <b>Copy</b> (Copia).

I dati nelle copie Snapshot sono di sola lettura. Se si desidera apportare modifiche ai file e alle cartelle elencati nella scheda versioni precedenti, è necessario salvare una copia dei file e delle cartelle che si desidera modificare in una posizione scrivibile e apportare modifiche alle copie.

7. Una volta terminata la gestione dei dati Snapshot, chiudere la finestra di dialogo **Proprietà** facendo clic su **OK**.

Per ulteriori informazioni sull'utilizzo della scheda versioni precedenti per visualizzare e gestire i dati Snapshot, consultare la Microsoft TechNet Library.

## Informazioni correlate

"Microsoft TechNet Library: [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)"

### Determinare se le copie Snapshot sono disponibili per le versioni precedenti

È possibile visualizzare le copie Snapshot dalla scheda versioni precedenti solo se al volume contenente la condivisione viene applicato un criterio Snapshot attivato e se la configurazione del volume consente l'accesso alle copie Snapshot. Determinare la disponibilità delle copie Snapshot è utile quando si assiste un utente con l'accesso alle versioni precedenti.

## Fasi

1. Determinare se nel volume in cui risiedono i dati di condivisione sono attivate le copie Snapshot automatiche e se i client hanno accesso alle directory Snapshot: `volume show -vserver vservice-name -volume volume-name -fields vservice,volume,snapdir-access,snapshot-policy,snapshot-count`

L'output visualizza il criterio Snapshot associato al volume, se l'accesso alla directory Snapshot del client è attivato e il numero di copie Snapshot disponibili.

2. Determinare se la policy Snapshot associata è attivata: `volume snapshot policy show -policy policy-name`
3. Elencare le copie Snapshot disponibili: `volume snapshot show -volume volume_name`

Per ulteriori informazioni sulla configurazione e la gestione delle policy Snapshot e delle pianificazioni Snapshot, vedere ["Protezione dei dati"](#).

### Esempio

Nell'esempio seguente vengono visualizzate informazioni sulle policy Snapshot associate al volume denominato "data1" che contiene i dati condivisi e le copie Snapshot disponibili su "data1".

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-----
vs1      data1  true                default                10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
Number of Is
Policy Name      Schedules Enabled Comment
-----
default          3 true      Default policy with hourly, daily &
weekly schedules.
Schedule      Count      Prefix      SnapMirror Label
-----
hourly         6      hourly      -
daily          2      daily       daily
weekly         2      weekly      weekly

cluster1::> volume snapshot show -volume data1
Vserver  Volume  Snapshot      State      Size  Total%  Used%
-----
vs1      data1
weekly.2012-12-16_0015  valid      408KB    0%    1%
daily.2012-12-22_0010  valid      420KB    0%    1%
daily.2012-12-23_0010  valid      192KB    0%    0%
weekly.2012-12-23_0015  valid      360KB    0%    1%
hourly.2012-12-23_1405  valid      196KB    0%    0%
hourly.2012-12-23_1505  valid      196KB    0%    0%
hourly.2012-12-23_1605  valid      212KB    0%    0%
hourly.2012-12-23_1705  valid      136KB    0%    0%
hourly.2012-12-23_1805  valid      200KB    0%    0%
hourly.2012-12-23_1905  valid      184KB    0%    0%
```

## Informazioni correlate

[Creazione di una configurazione Snapshot per consentire l'accesso alle versioni precedenti](#)

["Protezione dei dati"](#)

### Creare una configurazione Snapshot per consentire l'accesso alle versioni precedenti

La funzionalità delle versioni precedenti è sempre disponibile, a condizione che l'accesso client alle copie Snapshot sia attivato e che esistano copie Snapshot. Se la configurazione della copia Snapshot non soddisfa questi requisiti, è possibile creare una configurazione della copia Snapshot.

#### Fasi

1. Se il volume contenente la condivisione a cui si desidera consentire l'accesso alle versioni precedenti non dispone di un criterio Snapshot associato, associare un criterio Snapshot al volume e attivarlo utilizzando `volume modify` comando.

Per ulteriori informazioni sull'utilizzo di `volume modify` vedere le pagine man.

2. Abilitare l'accesso alle copie Snapshot utilizzando `volume modify` per impostare `-snap-dir` opzione a `true`.

Per ulteriori informazioni sull'utilizzo di `volume modify` vedere le pagine man.

3. Verificare che i criteri Snapshot siano attivati e che l'accesso alle directory Snapshot sia attivato utilizzando `volume show` e `volume snapshot policy show` comandi.

Per ulteriori informazioni sull'utilizzo di `volume show` e `volume snapshot policy show` comandi, vedere le pagine man.

Per ulteriori informazioni sulla configurazione e la gestione delle policy Snapshot e delle pianificazioni Snapshot, vedere ["Protezione dei dati"](#).

## Informazioni correlate

["Protezione dei dati"](#)

### Linee guida per il ripristino di directory che contengono giunzioni

Esistono alcune linee guida da tenere presenti quando si utilizzano versioni precedenti per ripristinare le cartelle che contengono punti di giunzione.

Quando si utilizzano le versioni precedenti per ripristinare le cartelle con cartelle figlio che sono punti di giunzione, il ripristino potrebbe non riuscire con un `Access Denied` errore.

È possibile determinare se la cartella che si sta tentando di ripristinare contiene una giunzione utilizzando `vol show` con il `-parent` opzione. È inoltre possibile utilizzare `vserver security trace` comandi per creare log dettagliati sui problemi di accesso a file e cartelle.

## Informazioni correlate

[Creazione e gestione di volumi di dati negli spazi dei nomi NAS](#)

# Implementare servizi basati su server SMB

## Gestire le home directory

In che modo ONTAP abilita le home directory dinamiche

Le home directory di ONTAP consentono di configurare una condivisione SMB che viene mappata a diverse directory in base all'utente che si connette ad essa e a una serie di variabili. Invece di creare condivisioni separate per ciascun utente, è possibile configurare una condivisione con alcuni parametri della home directory per definire la relazione di un utente tra un punto di ingresso (la condivisione) e la home directory (una directory sulla SVM).

Un utente che ha effettuato l'accesso come utente ospite non dispone di una home directory e non può accedere alle home directory di altri utenti. Esistono quattro variabili che determinano il modo in cui un utente viene mappato a una directory:

- **Nome condivisione**

Si tratta del nome della condivisione creata a cui l'utente si connette. È necessario impostare la proprietà home directory per questa condivisione.

Il nome della condivisione può utilizzare i seguenti nomi dinamici:

- %w (Il nome utente Windows dell'utente)
- %d (Il nome di dominio Windows dell'utente)
- %u (Il nome utente UNIX mappato dell'utente) per rendere unico il nome di condivisione in tutte le home directory, il nome di condivisione deve contenere %w o il %u variabile. Il nome della condivisione può contenere entrambi %d e a./%w variabile (ad esempio, %d/%w), oppure il nome della condivisione può contenere una porzione statica e una porzione variabile (ad esempio, home\_/%w).

- **Percorso di condivisione**

Si tratta del percorso relativo, definito dalla condivisione e quindi associato a uno dei nomi di condivisione, che viene aggiunto a ciascun percorso di ricerca per generare l'intero percorso della home directory dell'utente dalla directory principale della SVM. Può essere statico (ad esempio, home), dinamico (ad esempio, %w), o una combinazione dei due (ad esempio, eng/%w).

- **Percorsi di ricerca**

Questo è l'insieme di percorsi assoluti dalla directory principale di SVM che si specifica che dirige la ricerca di home directory in ONTAP. È possibile specificare uno o più percorsi di ricerca utilizzando `vserver cifs home-directory search-path add` comando. Se si specificano più percorsi di ricerca, ONTAP li prova nell'ordine specificato fino a trovare un percorso valido.

- **Directory**

Questa è la home directory dell'utente creata per l'utente. Il nome della directory è generalmente il nome dell'utente. È necessario creare la home directory in una delle directory definite dai percorsi di ricerca.

Ad esempio, considerare la seguente configurazione:

- Utente: John Smith
- Dominio utente: acme
- Nome utente: Jsmith
- Nome SVM: vs1
- Nome di condivisione della home directory n. 1: home\_ %w - percorso di condivisione: %w
- Nome condivisione home directory n. 2: %w - percorso di condivisione: %d/%w
- Percorso di ricerca n. 1: /vol0home/home
- Percorso di ricerca n. 2: /vol1home/home
- Percorso di ricerca n. 3: /vol2home/home
- Home directory: /vol1home/home/jsmith

Scenario 1: L'utente si connette a. \\vs1\home\_jsmith. Corrisponde al primo nome di condivisione della home directory e genera il relativo percorso jsmith. ONTAP ricerca ora una directory denominata jsmith selezionando ciascun percorso di ricerca nell'ordine indicato:

- /vol0home/home/jsmith non esiste; passaggio al percorso di ricerca n. 2.
- /vol1home/home/jsmith esiste; pertanto, il percorso di ricerca n. 3 non è selezionato; l'utente è ora connesso alla propria home directory.

Scenario 2: L'utente si connette a. \\vs1\jsmith. Corrisponde al secondo nome di condivisione della home directory e genera il relativo percorso acme/jsmith. ONTAP ricerca ora una directory denominata acme/jsmith selezionando ciascun percorso di ricerca nell'ordine indicato:

- /vol0home/home/acme/jsmith non esiste; passaggio al percorso di ricerca n. 2.
- /vol1home/home/acme/jsmith non esiste; passaggio al percorso di ricerca n. 3.
- /vol2home/home/acme/jsmith non esiste; la home directory non esiste; pertanto, la connessione non riesce.

## Condivisioni home directory

### Aggiungere una condivisione della home directory

Se si desidera utilizzare la funzione home directory SMB, è necessario aggiungere almeno una condivisione con la proprietà home directory inclusa nelle proprietà di condivisione.

#### A proposito di questa attività

È possibile creare una condivisione home directory al momento della creazione della condivisione utilizzando `vserver cifs share create` in alternativa, è possibile modificare una condivisione esistente in una condivisione della home directory in qualsiasi momento utilizzando `vserver cifs share modify` comando.

Per creare una condivisione della home directory, è necessario includere `homedirectory` valore in `-share -properties` quando si crea o si modifica una condivisione. È possibile specificare il nome della condivisione e il percorso di condivisione utilizzando variabili espandibili dinamicamente quando gli utenti si connettono alle proprie home directory. Le variabili disponibili che è possibile utilizzare nel percorso sono %w,



%d, e. %u, Corrispondenti rispettivamente al nome utente, al dominio e al nome utente UNIX mappato di Windows.

## Fasi

### 1. Aggiungere una condivisione home directory:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties homedirectory[,...]
```

`-vserver vserver` Specifica la SVM (Storage Virtual Machine) abilitata per CIFS su cui aggiungere il percorso di ricerca.

`-share-name share-name` specifica il nome di condivisione della home directory.

Oltre a contenere una delle variabili richieste, se il nome della condivisione contiene una delle stringhe letterali %w, %u, o. %d, È necessario precedere la stringa letterale con un carattere % (percentuale) per impedire a ONTAP di trattare la stringa letterale come una variabile (ad esempio, %%w).

- Il nome della condivisione deve contenere %w o il %u variabile.
- Il nome della condivisione può contenere anche %d variabile (ad esempio, %d/%w) o una parte statica nel nome della condivisione (ad esempio, home1\_/%w).
- Se la condivisione viene utilizzata dagli amministratori per connettersi alle home directory di altri utenti o per consentire agli utenti di connettersi alle home directory di altri utenti, il modello dinamico di nome della condivisione deve essere preceduto da una tilde (~).

Il `vserver cifs home-directory modify` viene utilizzato per abilitare questo accesso impostando `-is-home-dirs-access-for-admin-enabled` opzione a. true) o impostando l'opzione avanzata `-is-home-dirs-access-for-public-enabled` a. true.

`-path path` specifica il percorso relativo alla home directory.

`-share-properties homedirectory[,...]` specifica le proprietà di condivisione per tale condivisione. Specificare `homedirectory` valore. È possibile specificare ulteriori proprietà di condivisione utilizzando un elenco delimitato da virgole.

### 1. Verificare che la condivisione della home directory sia stata aggiunta correttamente utilizzando `vserver cifs share show` comando.

## Esempio

Il seguente comando crea una condivisione della home directory denominata %w. Il `oplocks`, `browsable`, e. `changenotify` oltre all'impostazione di, vengono impostate le proprietà di condivisione `homedirectory` condividere la proprietà.



Questo esempio non visualizza l'output per tutte le condivisioni sulla SVM. L'output viene troncato.

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w  
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
vs1::> vserver cifs share show -vserver vs1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1	%w	%w	oplocks	-	Everyone / Full
Control			browsable changenotify homedirectory		

## Informazioni correlate

[Aggiunta di un percorso di ricerca della home directory](#)

[Requisiti e linee guida per l'utilizzo dei riferimenti automatici ai nodi](#)

[Gestione dell'accessibilità alle home directory degli utenti](#)

## Le condivisioni della home directory richiedono nomi utente univoci

Fare attenzione a assegnare nomi utente univoci quando si creano condivisioni home directory utilizzando %w (Nome utente Windows) o. %u (Nome utente UNIX) variabili per generare condivisioni in modo dinamico. Il nome della condivisione viene associato al nome utente.

Quando il nome di una condivisione statica e il nome di un utente sono identici, possono verificarsi due problemi:

- Quando l'utente elenca le condivisioni su un cluster utilizzando `net view` vengono visualizzate due condivisioni con lo stesso nome utente.
- Quando l'utente si connette a tale nome di condivisione, l'utente è sempre connesso alla condivisione statica e non può accedere alla condivisione della home directory con lo stesso nome.

Ad esempio, esiste una condivisione denominata "Administrator" e si dispone di un nome utente Windows "Administrator". Se si crea una condivisione home directory e ci si connette a tale condivisione, si viene connessi alla condivisione statica "Administrator" e non alla condivisione home directory "Administrator".

Per risolvere il problema relativo ai nomi di condivisione duplicati, procedere come segue:

- Ridenominazione della condivisione statica in modo che non sia più in conflitto con la condivisione della home directory dell'utente.
- Assegnare all'utente un nuovo nome utente in modo che non sia più in conflitto con il nome di condivisione statico.
- Creazione di una condivisione della home directory CIFS con un nome statico come "home" invece di utilizzare %w per evitare conflitti con i nomi di condivisione.

## Cosa accade ai nomi di condivisione della home directory statica dopo l'aggiornamento

I nomi di condivisione della home directory devono contenere `%w` o il `%u` variabile dinamica. Dopo l'aggiornamento a una versione di ONTAP con il nuovo requisito, dovresti essere consapevole di ciò che accade ai nomi di condivisione della home directory statica esistenti.

Se la configurazione della home directory contiene nomi di condivisione statici e si esegue l'aggiornamento a ONTAP, i nomi di condivisione della home directory statica non vengono modificati e sono ancora validi. Tuttavia, non è possibile creare nuove condivisioni della home directory che non contengono `%w` oppure `%u` variabile.

La richiesta di includere una di queste variabili nel nome di condivisione della home directory dell'utente garantisce che ogni nome di condivisione sia univoco nella configurazione della home directory. Se lo si desidera, è possibile modificare i nomi di condivisione della home directory statica in nomi che contengono `%w` oppure `%u` variabile.

### Aggiungere un percorso di ricerca della home directory

Se si desidera utilizzare le home directory SMB di ONTAP, è necessario aggiungere almeno un percorso di ricerca della home directory.

#### A proposito di questa attività

È possibile aggiungere un percorso di ricerca della home directory utilizzando `vserver cifs home-directory search-path add` comando.

Il `vserver cifs home-directory search-path add` il comando verifica il percorso specificato in `-path` durante l'esecuzione del comando. Se il percorso specificato non esiste, il comando genera un messaggio che richiede se si desidera continuare. Scegli tu `y` oppure `n`. Se si sceglie `y` Per continuare, ONTAP crea il percorso di ricerca. Tuttavia, è necessario creare la struttura di directory prima di poter utilizzare il percorso di ricerca nella configurazione della home directory. Se si sceglie di non continuare, il comando non riesce; il percorso di ricerca non viene creato. È quindi possibile creare la struttura della directory dei percorsi ed eseguire di nuovo il `vserver cifs home-directory search-path add` comando.

#### Fasi

1. Aggiungere un percorso di ricerca della home directory: `vserver cifs home-directory search-path add -vserver vserver -path path`
2. Verificare di aver aggiunto correttamente il percorso di ricerca utilizzando `vserver cifs home-directory search-path show` comando.

#### Esempio

Nell'esempio seguente viene aggiunto il percorso `/home1` Alla configurazione della home directory su SVM `vs1`.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home1

vs1::> vserver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1      /home1
```

Nell'esempio seguente viene tentato di aggiungere il percorso `/home2` Alla configurazione della home directory su SVM vs1. Il percorso non esiste. La scelta è fatta per non continuare.

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path /home2
Warning: The specified path "/home2" does not exist in the namespace
        belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

## Informazioni correlate

[Aggiunta di una condivisione della home directory](#)

**Creare una configurazione della home directory utilizzando le variabili `%w` e `%d`.**

È possibile creare una configurazione della home directory utilizzando `%w` e `%d` variabili. Gli utenti possono quindi connettersi alla propria home share utilizzando condivisioni create dinamicamente.

## Fasi

1. Creare un qtree per contenere le home directory dell'utente: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verificare che il qtree utilizzi lo stile di protezione corretto: `volume qtree show`
3. Se qtree non utilizza lo stile di protezione desiderato, modificare lo stile di protezione utilizzando `volume qtree security` comando.
4. Aggiunta di una condivisione home directory: `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`  
  
`-vserver vserver` Specifica la SVM (Storage Virtual Machine) abilitata per CIFS su cui aggiungere il percorso di ricerca.  
  
`-share-name %w` specifica il nome di condivisione della home directory. ONTAP crea dinamicamente il nome di condivisione quando ogni utente si connette alla propria home directory. Il nome della condivisione avrà il formato *Windows\_User\_NAME*.  
  
`-path %d/%w` specifica il percorso relativo alla home directory. Il percorso relativo viene creato dinamicamente quando ciascun utente si connette alla propria home directory e avrà la forma *domain/Windows\_user\_name*.

`-share-properties homedirectory[,...]` specifica le proprietà di condivisione per tale condivisione. Specificare `homedirectory` valore. È possibile specificare ulteriori proprietà di condivisione utilizzando un elenco delimitato da virgole.

5. Verificare che la condivisione abbia la configurazione desiderata utilizzando `vserver cifs share show` comando.

6. Aggiungere un percorso di ricerca della home directory: `vserver cifs home-directory search-path add -vserver vserver -path path`

`-vserver vserver-name` Specifica la SVM abilitata per CIFS su cui aggiungere il percorso di ricerca.

`-path path` specifica il percorso assoluto della directory per il percorso di ricerca.

7. Verificare di aver aggiunto correttamente il percorso di ricerca utilizzando `vserver cifs home-directory search-path show` comando.

8. Per gli utenti con una home directory, creare una directory corrispondente nel qtree o nel volume designato per contenere home directory.

Ad esempio, se è stato creato un qtree con il percorso di `/vol/vol1/users` e il nome utente di cui si desidera creare la directory è `mydomain.user1`, si crea una directory con il seguente percorso:  
`/vol/vol1/users/mydomain/user1`.

Se è stato creato un volume denominato "home1" montato in `/home1`, creare una directory con il seguente percorso: `/home1/mydomain/user1`.

9. Verificare che un utente possa connettersi correttamente alla home share mappando un disco o connettendosi utilizzando il percorso UNC.

Ad esempio, se l'utente `mydomain/user1` desidera connettersi alla directory creata nella fase 8 che si trova su SVM `vs1`, l'utente 1 si connette utilizzando il percorso UNC `\\vs1\user1`.

## Esempio

I comandi dell'esempio seguente creano una configurazione della home directory con le seguenti impostazioni:

- Il nome della condivisione è `%w`.
- Il percorso relativo della home directory è `%d/%W`.
- Il percorso di ricerca utilizzato per contenere le home directory, `/home1`, È un volume configurato con lo stile di protezione NTFS.
- La configurazione viene creata su SVM `vs1`.

È possibile utilizzare questo tipo di configurazione della home directory quando gli utenti accedono alle home directory dagli host Windows. È possibile utilizzare questo tipo di configurazione anche quando gli utenti accedono alle proprie home directory da host Windows e UNIX e l'amministratore del file system utilizza utenti e gruppi basati su Windows per controllare l'accesso al file system.

```

cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vsriver cifs share show -vsriver vs1 -share-name %w

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %d/%w
                Share Properties: oplocks
                                browsable
                                changenotify
                                homedirectory
                Symlink Properties: enable
                File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                Share Comment: -
                Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1

cluster::> vsriver cifs home-directory search-path show
Vserver      Position Path
-----
vs1          1         /home1

```

## Informazioni correlate

[Configurazione delle home directory utilizzando la variabile %u](#)

[Configurazioni aggiuntive della home directory](#)

[Visualizzazione delle informazioni sul percorso home directory di un utente SMB](#)

## Configurare le home directory utilizzando la variabile %u

È possibile creare una configurazione della home directory in cui designare il nome della condivisione utilizzando %w variabile ma si utilizza %u variabile per indicare il percorso relativo alla condivisione della home directory. Gli utenti possono quindi connettersi alla propria home share utilizzando condivisioni create dinamicamente utilizzando il proprio nome utente Windows senza conoscere il nome o il percorso effettivo della home directory.

## Fasi

1. Creare un qtree per contenere le home directory dell'utente: `volume qtree create -vserver vserver_name -qtree-path qtree_path`
2. Verificare che il qtree utilizzi lo stile di protezione corretto: `volume qtree show`
3. Se qtree non utilizza lo stile di protezione desiderato, modificare lo stile di protezione utilizzando `volume qtree security` comando.
4. Aggiunta di una condivisione home directory: `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

`-vserver vserver` Specifica la SVM (Storage Virtual Machine) abilitata per CIFS su cui aggiungere il percorso di ricerca.

`-share-name %w` specifica il nome di condivisione della home directory. Il nome della condivisione viene creato in modo dinamico quando ciascun utente si connette alla propria home directory e ha la forma *Windows\_User\_NAME*.



È inoltre possibile utilizzare `%u` variabile per `-share-name` opzione. In questo modo viene creato un percorso di condivisione relativo che utilizza il nome utente UNIX mappato.

`-path %u` specifica il percorso relativo alla home directory. Il percorso relativo viene creato in modo dinamico quando ciascun utente si connette alla propria home directory ed è del tipo *mapped\_UNIX\_user\_name*.



Il valore di questa opzione può contenere anche elementi statici. Ad esempio, `eng/%u`.

`-share-properties homedirectory\[,...\]` specifica le proprietà di condivisione per tale condivisione. Specificare `homedirectory` valore. È possibile specificare ulteriori proprietà di condivisione utilizzando un elenco delimitato da virgole.

5. Verificare che la condivisione abbia la configurazione desiderata utilizzando `vserver cifs share show` comando.
6. Aggiungere un percorso di ricerca della home directory: `vserver cifs home-directory search-path add -vserver vserver -path path`  
  
`-vserver vserver` Specifica la SVM abilitata per CIFS su cui aggiungere il percorso di ricerca.  
  
`-path path` specifica il percorso assoluto della directory per il percorso di ricerca.
7. Verificare di aver aggiunto correttamente il percorso di ricerca utilizzando `vserver cifs home-directory search-path show` comando.
8. Se l'utente UNIX non esiste, creare l'utente UNIX utilizzando `vserver services unix-user create` comando.



Il nome utente UNIX a cui si esegue il mapping del nome utente Windows deve esistere prima di eseguire il mapping dell'utente.

9. Creare una mappatura dei nomi per l'utente Windows e l'utente UNIX utilizzando il seguente comando:  
`vserver name-mapping create -vserver vserver_name -direction win-unix`

`-priority integer -pattern windows_user_name -replacement unix_user_name`



Se esistono già mappature dei nomi che associano gli utenti Windows agli utenti UNIX, non è necessario eseguire la procedura di mappatura.

Il nome utente di Windows viene associato al nome utente UNIX corrispondente. Quando l'utente Windows si connette alla propria home directory share, si connette a una home directory creata dinamicamente con un nome di condivisione che corrisponde al proprio nome utente Windows senza essere consapevole che il nome della directory corrisponde al nome utente UNIX.

10. Per gli utenti con una home directory, creare una directory corrispondente nel qtree o nel volume designato per contenere home directory.

Ad esempio, se è stato creato un qtree con il percorso di `/vol/vol1/users` E il nome utente UNIX mappato dell'utente la cui directory si desidera creare è "unixuser1", si crea una directory con il seguente percorso: `/vol/vol1/users/unixuser1`.

Se è stato creato un volume denominato "home1" montato in `/home1`, creare una directory con il seguente percorso: `/home1/unixuser1`.

11. Verificare che un utente possa connettersi correttamente alla home share mappando un disco o connettendosi utilizzando il percorso UNC.

Ad esempio, se l'utente `mydomain/user1` esegue il mapping all'utente UNIX `unixuser1` e desidera connettersi alla directory creata nella fase 10 che si trova su SVM `vs1`, l'utente 1 si connette utilizzando il percorso UNC `\\vs1\user1`.

## Esempio

I comandi dell'esempio seguente creano una configurazione della home directory con le seguenti impostazioni:

- Il nome della condivisione è `%w`.
- Il percorso relativo della home directory è `%u`.
- Il percorso di ricerca utilizzato per contenere le home directory, `/home1`, È un volume configurato con lo stile di sicurezza UNIX.
- La configurazione viene creata su SVM `vs1`.

È possibile utilizzare questo tipo di configurazione della home directory quando gli utenti accedono alle proprie home directory da host Windows o Windows e da host UNIX e l'amministratore del file system utilizza utenti e gruppi basati su UNIX per controllare l'accesso al file system.



```
cluster::> vsriver cifs share create -vsriver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory
```

```
cluster::> vsriver cifs share show -vsriver vs1 -share-name %u
```

```

                Vserver: vs1
                Share: %w
CIFS Server NetBIOS Name: VS1
                Path: %u
    Share Properties: oplocks
                    browsable
                    changenotify
                    homedirectory
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster::> vsriver cifs home-directory search-path add -vsriver vs1 -path
/home1
```

```
cluster::> vsriver cifs home-directory search-path show -vsriver vs1
```

```
Vserver      Position Path
-----
vs1          1          /home1
```

```
cluster::> vsriver name-mapping create -vsriver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1
```

```
cluster::> vsriver name-mapping show -pattern user1
```

```
Vserver      Direction Position
-----
vs1          win-unix  5          Pattern: user1
                                Replacement: unixuser1
```

## Informazioni correlate

[Creazione di una configurazione della home directory utilizzando le variabili %w e %d.](#)

[Configurazioni aggiuntive della home directory](#)

[Visualizzazione delle informazioni sul percorso home directory di un utente SMB](#)

## Configurazioni aggiuntive della home directory

È possibile creare ulteriori configurazioni della home directory utilizzando %w, %d, e. %u variables, che consente di personalizzare la configurazione della home directory in base alle proprie esigenze.

È possibile creare una serie di configurazioni della home directory utilizzando una combinazione di variabili e stringhe statiche nei nomi di condivisione e nei percorsi di ricerca. La seguente tabella fornisce alcuni esempi che illustrano come creare diverse configurazioni della home directory:

Percorsi creati quando /vol1/user contiene home directory...	Comando di condivisione...
Per creare un percorso di condivisione \\vs1\~win_username che indica all'utente /vol1/user/win_username	<code>vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory</code>
Per creare un percorso di condivisione \\vs1\win_username che indica all'utente /vol1/user/domain/win_username	<code>vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory</code>
Per creare un percorso di condivisione \\vs1\win_username che indica all'utente /vol1/user/unix_username	<code>vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>
Per creare un percorso di condivisione \\vs1\unix_username che indica all'utente /vol1/user/unix_username	<code>vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory</code>

## Comandi per la gestione dei percorsi di ricerca

Esistono comandi ONTAP specifici per la gestione dei percorsi di ricerca per le configurazioni della home directory SMB. Ad esempio, sono disponibili comandi per aggiungere, rimuovere e visualizzare informazioni sui percorsi di ricerca. È inoltre disponibile un comando per modificare l'ordine dei percorsi di ricerca.

Se si desidera...	Utilizzare questo comando...
Aggiungere un percorso di ricerca	<code>vserver cifs home-directory search-path add</code>
Visualizzare i percorsi di ricerca	<code>vserver cifs home-directory search-path show</code>

Se si desidera...	Utilizzare questo comando...
Modificare l'ordine dei percorsi di ricerca	<code>vserver cifs home-directory search-path reorder</code>
Rimuovere un percorso di ricerca	<code>vserver cifs home-directory search-path remove</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

#### Visualizza informazioni sul percorso home directory di un utente SMB

È possibile visualizzare il percorso home directory di un utente SMB sulla macchina virtuale di storage (SVM), che può essere utilizzato se sono stati configurati più percorsi home directory CIFS e si desidera vedere quale percorso contiene la home directory dell'utente.

#### Fase

1. Visualizzare il percorso della home directory utilizzando `vserver cifs home-directory show-user` comando.

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

Vserver	User	Home Dir Path
vs1	user1	/home/user1

#### Informazioni correlate

[Gestione dell'accessibilità alle home directory degli utenti](#)

#### Gestire l'accessibilità alle home directory degli utenti

Per impostazione predefinita, l'accesso alla home directory di un utente è consentito solo a quell'utente. Per le condivisioni in cui il nome dinamico della condivisione è preceduto da una tilde (~), è possibile attivare o disattivare l'accesso alle home directory degli utenti da parte degli amministratori di Windows o di qualsiasi altro utente (accesso pubblico).

#### Prima di iniziare

Le condivisioni home directory sulla macchina virtuale di storage (SVM) devono essere configurate con nomi di condivisione dinamici preceduti da una tilde (~). I seguenti casi illustrano i requisiti di naming delle condivisioni:

Nome di condivisione della home directory	Esempio di comando per connettersi alla condivisione
~%d~%w	<code>net use * \\IPAddress\~domain~user/u:credentials</code>

Nome di condivisione della home directory	Esempio di comando per connettersi alla condivisione
~%W	net use * \\IPAddress\~user/u:credentials
~abc~%w	net use * \\IPAddress\abc~user/u:credentials

## Fase

1. Eseguire l'azione appropriata:

Se si desidera attivare o disattivare l'accesso alle home directory degli utenti per...	Immettere quanto segue...
Amministratori di Windows	vserver cifs home-directory modify -vserver vserver_name -is-home-dirs -access-for-admin-enabled {true false} `L'impostazione predefinita è `true.
Qualsiasi utente (accesso pubblico)	<ol style="list-style-type: none"> <li>a. Impostare il livello di privilegio su Advanced: set -privilege advanced</li> <li>b. Abilitare o disabilitare l'accesso: `vserver cifs home-directory modify -vserver vserver_name -is-home-dirs-access-for-public-enabled {true</li> </ol>

L'esempio seguente consente l'accesso pubblico alle home directory degli utenti:

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public-enabled true
set -privilege admin
```

## Informazioni correlate

[Visualizzazione delle informazioni sul percorso home directory di un utente SMB](#)

## Configurare l'accesso del client SMB ai collegamenti simbolici UNIX

In che modo ONTAP consente di fornire l'accesso del client SMB ai collegamenti simbolici UNIX

Un collegamento simbolico è un file creato in un ambiente UNIX che contiene un riferimento a un altro file o directory. Se un client accede a un collegamento simbolico, il client viene reindirizzato al file o alla directory di destinazione a cui si riferisce il collegamento simbolico. ONTAP supporta collegamenti simbolici relativi e assoluti, inclusi i widelink (collegamenti assoluti con destinazioni esterne al file system locale).

ONTAP offre ai client SMB la possibilità di seguire i collegamenti simbolici UNIX configurati sulla SVM. Questa funzione è opzionale ed è possibile configurarla in base alle condivisioni, utilizzando `-symlink-properties` opzione di `vserver cifs share create` con una delle seguenti impostazioni:

- Abilitato con accesso in lettura/scrittura
- Abilitato con accesso di sola lettura
- Disattivato nascondendo i collegamenti simbolici dai client SMB
- Disattivato senza accesso ai collegamenti simbolici dai client SMB

Se si abilitano i collegamenti simbolici su una condivisione, i collegamenti simbolici relativi funzionano senza ulteriori configurazioni.

Se si abilitano i collegamenti simbolici su una condivisione, i collegamenti simbolici assoluti non funzionano immediatamente. È necessario innanzitutto creare un mapping tra il percorso UNIX del collegamento simbolico e il percorso SMB di destinazione. Quando si creano mappature di collegamento simboliche assolute, è possibile specificare se si tratta di un collegamento locale o di un *widelink*; i *widelink* possono essere collegamenti a file system su altri dispositivi di storage o collegamenti a file system ospitati in SVM separate sullo stesso sistema ONTAP. Quando si crea un *widelink*, deve includere le informazioni che il client deve seguire; ovvero, si crea un punto di analisi per il client per rilevare il punto di giunzione della directory. Se si crea un collegamento simbolico assoluto a un file o a una directory all'esterno della condivisione locale ma si imposta la località su locale, ONTAP non consente l'accesso alla destinazione.



Se un client tenta di eliminare un collegamento simbolico locale (assoluto o relativo), viene cancellato solo il collegamento simbolico, non il file o la directory di destinazione. Tuttavia, se un client tenta di eliminare un *widelink*, potrebbe eliminare il file o la directory di destinazione effettiva a cui si riferisce il *widelink*. ONTAP non ha il controllo su questo dato che il client può aprire esplicitamente il file o la directory di destinazione all'esterno della SVM ed eliminarlo.

#### • Reparse point e servizi file system ONTAP

Un *punto di analisi* è un oggetto del file system NTFS che può essere facoltativamente memorizzato sui volumi insieme a un file. I reparse point offrono ai client SMB la possibilità di ricevere servizi di file system avanzati o estesi quando si lavora con volumi di stile NTFS. I punti di analisi sono costituiti da tag standard che identificano il tipo di punto di analisi e il contenuto del punto di analisi che può essere recuperato dai client SMB per un'ulteriore elaborazione da parte del client. Dei tipi di oggetti disponibili per la funzionalità estesa del file system, ONTAP implementa il supporto per i collegamenti simbolici NTFS e i punti di giunzione della directory utilizzando tag di punto di analisi. I client SMB che non sono in grado di comprendere il contenuto di un punto di analisi lo ignorano semplicemente e non forniscono il servizio di file system esteso che il punto di analisi potrebbe abilitare.

#### • Directory Junction point e supporto ONTAP per link simbolici

I punti di giunzione della directory sono posizioni all'interno di una struttura di directory del file system che possono fare riferimento a posizioni alternative in cui sono memorizzati i file, su un percorso diverso (collegamenti simbolici) o su un dispositivo di storage separato (*widelink*). I server SMB di ONTAP espongono i punti di giunzione della directory ai client Windows come punti di analisi, consentendo ai client in grado di ottenere contenuti dei punti di analisi da ONTAP quando viene attraversato un punto di giunzione della directory. In questo modo, possono navigare e connettersi a diversi percorsi o dispositivi di storage come se fossero parte dello stesso file system.

#### • Abilitazione del supporto widelink utilizzando le opzioni di reparse point

Il `-is-use-junctions-as-reparse-points-enabled` L'opzione è attivata per impostazione predefinita in ONTAP 9. Non tutti i client SMB supportano i *widelink*, pertanto l'opzione per abilitare le informazioni è configurabile in base alla versione per protocollo, consentendo agli amministratori di ospitare client SMB supportati e non supportati. In ONTAP 9.2 e versioni successive, è necessario attivare l'opzione `-widelink-as-reparse-point-versions` Per ogni protocollo client che accede alla


condivisione utilizzando i widelink, l'impostazione predefinita è SMB1. Nelle versioni precedenti, sono stati segnalati solo i widelink a cui si accedeva utilizzando SMB1 predefinito e i sistemi che utilizzavano SMB2 o SMB3 non erano in grado di accedere ai widelink.

Per ulteriori informazioni, consultare la documentazione di Microsoft NTFS.

["Documentazione Microsoft: Analisi dei punti"](#)

**Limiti durante la configurazione dei collegamenti simbolici UNIX per l'accesso SMB**

È necessario conoscere alcuni limiti durante la configurazione dei collegamenti simbolici UNIX per l'accesso SMB.

Limite	Descrizione
45	Lunghezza massima del nome del server CIFS che è possibile specificare quando si utilizza un FQDN per il nome del server CIFS. <div> In alternativa, è possibile specificare il nome del server CIFS come nome NetBIOS, che può contenere al massimo 15 caratteri.</div>
80	Lunghezza massima del nome di condivisione.
256	Lunghezza massima del percorso UNIX che è possibile specificare quando si crea un collegamento simbolico o si modifica il percorso UNIX di un collegamento simbolico esistente.il percorso UNIX deve iniziare con un "/" (slash) and end with a "/". Le barre iniziali e finali vengono conteggiate come parte del limite di 256 caratteri.
256	Lunghezza massima del percorso CIFS che è possibile specificare quando si crea un collegamento simbolico o si modifica il percorso CIFS di un collegamento simbolico esistente. Il percorso CIFS deve iniziare con un "/" (slash) and end with a "/". Le barre iniziali e finali vengono conteggiate come parte del limite di 256 caratteri.

**Informazioni correlate**

[Creazione di mappature di collegamento simboliche per le condivisioni SMB](#)

**Controlla gli annunci DFS automatici in ONTAP con un'opzione del server CIFS**

Un'opzione del server CIFS controlla il modo in cui le funzionalità DFS vengono pubblicizzate ai client SMB durante la connessione alle condivisioni. Poiché ONTAP utilizza i riferimenti DFS quando i client accedono a collegamenti simbolici su SMB, è

necessario essere consapevoli dell'impatto della disattivazione o dell'attivazione di questa opzione.

Un'opzione del server CIFS determina se i server CIFS annunciano automaticamente se sono compatibili con DFS per i client SMB. Per impostazione predefinita, questa opzione è attivata e il server CIFS comunica sempre che è compatibile con DFS per i client SMB (anche quando ci si connette a condivisioni in cui l'accesso ai collegamenti simbolici è disattivato). Se si desidera che il server CIFS annunci che è compatibile con DFS solo quando si connettono a condivisioni in cui è attivato l'accesso ai collegamenti simbolici, è possibile disattivare questa opzione.

Tenere presente cosa accade quando questa opzione è disattivata:

- Le configurazioni di condivisione per i collegamenti simbolici sono invariate.
- Se il parametro share è impostato in modo da consentire l'accesso simbolico al collegamento (accesso in lettura/scrittura o accesso in sola lettura), il server CIFS comunica le funzionalità DFS ai client che si connettono a tale condivisione.

Le connessioni client e l'accesso ai collegamenti simbolici continuano senza interruzioni.

- Se il parametro share è impostato in modo da non consentire l'accesso tramite collegamento simbolico (disattivando l'accesso o se il valore del parametro share è nullo), il server CIFS non segnala le funzionalità DFS ai client che si connettono a tale condivisione.

Poiché i client hanno memorizzato nella cache le informazioni che il server CIFS è compatibile con DFS e non pubblicizzano più, i client connessi alle condivisioni in cui l'accesso al collegamento simbolico è disattivato potrebbero non essere in grado di accedere a queste condivisioni dopo la disattivazione dell'opzione del server CIFS. Una volta disattivata l'opzione, potrebbe essere necessario riavviare i client connessi a queste condivisioni, eliminando così le informazioni memorizzate nella cache.

Queste modifiche non si applicano alle connessioni SMB 1.0.

#### **Configurare il supporto dei collegamenti simbolici UNIX sulle condivisioni SMB**

È possibile configurare il supporto del collegamento simbolico UNIX sulle condivisioni SMB specificando un'impostazione simbolica di proprietà-condivisione del collegamento quando si creano condivisioni SMB o in qualsiasi momento modificando le condivisioni SMB esistenti. Il supporto dei collegamenti simbolici UNIX è attivato per impostazione predefinita. È inoltre possibile disattivare il supporto dei collegamenti simbolici UNIX su una condivisione.

#### **A proposito di questa attività**

Quando si configura il supporto del collegamento simbolico UNIX per le condivisioni SMB, è possibile scegliere una delle seguenti impostazioni:

<b>Impostazione</b>	<b>Descrizione</b>
enable (OBSOLETO*)	Specifica che i collegamenti simbolici sono abilitati per l'accesso in lettura/scrittura.

Impostazione	Descrizione
<code>read_only</code> (OBSOLETO*)	Specifica che i collegamenti simbolici sono abilitati per l'accesso in sola lettura. Questa impostazione non si applica ai widelink. L'accesso a Widelink è sempre in lettura/scrittura.
<code>hide</code> (OBSOLETO*)	Specifica che ai client SMB viene impedito di visualizzare i collegamenti simbolici.
<code>no-strict-security</code>	Specifica che i client seguono collegamenti simbolici al di fuori dei limiti di condivisione.
<code>symlinks</code>	Specifica che i collegamenti simbolici sono attivati localmente per l'accesso in lettura/scrittura. Gli annunci DFS non vengono generati anche se l'opzione CIFS <code>is-advertise-dfs-enabled</code> è impostato su <code>true</code> . Questa è l'impostazione predefinita.
<code>symlinks-and-widelinks</code>	Specifica che sia i collegamenti simbolici locali che i collegamenti widelink per l'accesso in lettura/scrittura. Gli annunci DFS vengono generati sia per symlink locale che per widelink anche se l'opzione CIFS <code>is-advertise-dfs-enabled</code> è impostato su <code>false</code> .
<code>disable</code>	Specifica che i collegamenti simbolici e i collegamenti widelink sono disattivati. Gli annunci DFS non vengono generati anche se l'opzione CIFS <code>is-advertise-dfs-enabled</code> è impostato su <code>true</code> .
<code>""</code> (nullo, non impostato)	Disattiva i collegamenti simbolici sulla condivisione.
<code>-</code> (non impostato)	Disattiva i collegamenti simbolici sulla condivisione.



\*I parametri *enable*, *hide* e *Read-only* sono deprecati e possono essere rimossi in una release futura di ONTAP.

## Fasi

1. Configurare o disattivare il supporto dei collegamenti simbolici:

Se è...	Inserisci...
Una nuova condivisione SMB	<code>`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable</code>
<code>hide</code>	<code>read-only</code>



Se è...	Inserisci...
""	-
symlinks	symlinks-and-widelinks
disable},...]+`	Una condivisione SMB esistente
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},...]+`

2. Verificare che la configurazione della condivisione SMB sia corretta: `vserver cifs share show -vserver vserver_name -share-name share_name -instance`

### Esempio

Il seguente comando crea una condivisione SMB denominata "data1" con la configurazione del collegamento simbolico UNIX impostata su enable:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

Vserver: vs1
Share: data1
CIFS Server NetBIOS Name: VS1
Path: /data1
Share Properties: oplocks
browsable
changenotify
Symlink Properties: enable
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

## Informazioni correlate

### Creazione di mappature di collegamento simboliche per le condivisioni SMB

#### Creare mappature di collegamento simboliche per le condivisioni SMB

È possibile creare mappature di collegamenti simbolici UNIX per le condivisioni SMB. È possibile creare un collegamento simbolico relativo, che si riferisce al file o alla cartella relativa alla cartella principale, oppure creare un collegamento simbolico assoluto, che si riferisce al file o alla cartella utilizzando un percorso assoluto.

#### A proposito di questa attività

I Widelink non sono accessibili dai client Mac OS X se si utilizza SMB 2.x. Quando un utente tenta di connettersi a una condivisione utilizzando i collegamenti wireless da un client Mac OS X, il tentativo non riesce. Tuttavia, è possibile utilizzare i widelink con i client Mac OS X se si utilizza SMB 1.

#### Fasi

1. Per creare mappature di collegamento simboliche per le condivisioni SMB: `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

`-vserver virtual_server_name` Specifica il nome della SVM (Storage Virtual Machine).

`-unix-path path` Specifica il percorso UNIX. Il percorso UNIX deve iniziare con una barra (/) e deve terminare con una barra (/).

`-share-name share_name` Specifica il nome della condivisione SMB da mappare.

`-cifs-path path` Specifica il percorso CIFS. Il percorso CIFS deve iniziare con una barra (/) e deve terminare con una barra (/).

`-cifs-server server_name` Specifica il nome del server CIFS. Il nome del server CIFS può essere specificato come nome DNS (ad esempio, mynetwork.cifs.server.com), indirizzo IP o nome NetBIOS. Il nome NetBIOS può essere determinato utilizzando `vserver cifs show` comando. Se questo parametro opzionale non viene specificato, il valore predefinito è il nome NetBIOS del server CIFS locale.

`-locality local|free|widelink` specifica se creare un link locale, un link libero o un link simbolico esteso. Un collegamento simbolico locale viene mappato alla condivisione SMB locale. Un collegamento simbolico gratuito può essere mappato in qualsiasi punto del server SMB locale. Un link simbolico esteso si collega a qualsiasi condivisione SMB sulla rete. Se non si specifica questo parametro opzionale, il valore predefinito è `local`.

`-home-directory true false` specifica se la condivisione di destinazione è una home directory. Anche se questo parametro è facoltativo, è necessario impostarlo su `true` quando la condivisione di destinazione è configurata come home directory. L'impostazione predefinita è `false`.

#### Esempio

Il seguente comando crea un mapping di collegamento simbolico sulla SVM denominata vs1. Ha il percorso UNIX `/src/`, il nome di condivisione SMB "SOURCE", il percorso CIFS `/mycompany/source/`, E l'indirizzo IP del server CIFS 123.123.123.123, ed è un widelink.

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/  
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server  
123.123.123.123 -locality widelink
```

## Informazioni correlate

[Configurazione del supporto del collegamento simbolico UNIX sulle condivisioni SMB](#)

## Comandi per la gestione delle mappature di collegamenti simbolici

Sono disponibili comandi ONTAP specifici per la gestione delle mappature dei collegamenti simbolici.

Se si desidera...	Utilizzare questo comando...
Creare una mappatura simbolica del collegamento	<code>vserver cifs symlink create</code>
Visualizza informazioni sulle mappature dei collegamenti simbolici	<code>vserver cifs symlink show</code>
Modificare un mapping di collegamento simbolico	<code>vserver cifs symlink modify</code>
Eliminare un mapping di collegamento simbolico	<code>vserver cifs symlink delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Utilizza BranchCache per memorizzare nella cache i contenuti di condivisione SMB in una filiale

### Utilizza BranchCache per memorizzare nella cache i contenuti di condivisione SMB in una panoramica delle filiali

BranchCache è stato sviluppato da Microsoft per consentire il caching dei contenuti sui computer locali dei client che richiedono. L'implementazione ONTAP di BranchCache può ridurre l'utilizzo della WAN (Wide-Area Network) e fornire tempi di risposta dell'accesso migliorati quando gli utenti di una filiale accedono ai contenuti memorizzati su macchine virtuali storage (SVM) utilizzando le PMI.

Se si configura BranchCache, i client Windows BranchCache recuperano prima il contenuto dalla SVM e poi lo memorizzano nella cache su un computer all'interno della filiale. Se un altro client abilitato a BranchCache nella filiale richiede lo stesso contenuto, la SVM prima autentica e autorizza l'utente richiedente. La SVM determina quindi se il contenuto memorizzato nella cache è ancora aggiornato e, in tal caso, invia i metadati del client relativi al contenuto memorizzato nella cache. Il client utilizza quindi i metadati per recuperare il contenuto direttamente dalla cache basata su locale.

## Informazioni correlate

[Utilizzo di file offline per consentire il caching dei file per l'utilizzo offline](#)

### Supporto della versione di BranchCache

È necessario conoscere le versioni di BranchCache supportate da ONTAP.

ONTAP supporta BranchCache 1 e BranchCache 2:

- Quando configuri BranchCache sul server SMB per la macchina virtuale di storage (SVM), puoi abilitare BranchCache 1, BranchCache 2 o tutte le versioni.

Per impostazione predefinita, tutte le versioni sono attivate.

- Se si attiva solo BranchCache 2, i computer client Windows della sede remota devono supportare BranchCache 2.

Solo i client SMB 3.0 o versioni successive supportano BranchCache 2.

Per ulteriori informazioni sulle versioni di BranchCache, consulta la Microsoft TechNet Library.

### Informazioni correlate

"Microsoft TechNet Library: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

### Requisiti di supporto del protocollo di rete

È necessario conoscere i requisiti del protocollo di rete per l'implementazione di ONTAP BranchCache.

È possibile implementare la funzionalità BranchCache di ONTAP su reti IPv4 e IPv6 utilizzando SMB 2.1 o versioni successive.

Tutti i server CIFS e i computer delle filiali che partecipano all'implementazione di BranchCache devono avere il protocollo SMB 2.1 o successivo abilitato. SMB 2.1 dispone di estensioni di protocollo che consentono a un client di partecipare a un ambiente BranchCache. Questa è la versione minima del protocollo SMB che offre il supporto BranchCache. SMB 2.1 supporta la versione BranchCache versione 1.

Se si desidera utilizzare BranchCache versione 2, SMB 3.0 è la versione minima supportata. Tutti i server CIFS e i computer delle filiali che partecipano a un'implementazione di BranchCache 2 devono avere SMB 3.0 o versioni successive abilitate.

Se si dispone di uffici remoti in cui alcuni client supportano solo SMB 2.1 e alcuni client supportano SMB 3.0, è possibile implementare una configurazione BranchCache sul server CIFS che fornisce il supporto del caching su BranchCache 1 e BranchCache 2.



Anche se la funzionalità Microsoft BranchCache supporta l'utilizzo dei protocolli HTTP/HTTPS e SMB come protocolli di accesso ai file, ONTAP BranchCache supporta solo l'utilizzo di SMB.

### Requisiti di versione per gli host ONTAP e Windows

Gli host Windows di ONTAP e delle filiali devono soddisfare determinati requisiti di versione prima di poter configurare BranchCache.

Prima di configurare BranchCache, è necessario assicurarsi che la versione di ONTAP sul cluster e i client

delle filiali partecipanti supportino SMB 2.1 o versioni successive e la funzionalità BranchCache. Se si configura la modalità cache in hosting, è necessario anche assicurarsi di utilizzare un host supportato per il server della cache.

BranchCache 1 è supportato dalle seguenti versioni di ONTAP e dagli host Windows:

- Server di contenuti: SVM (Storage Virtual Machine) con ONTAP
- Server cache: Windows Server 2008 R2 o Windows Server 2012 o versione successiva
- Peer o client: Windows 7 Enterprise, Windows 7 Ultimate, Windows 8, Windows Server 2008 R2 o Windows Server 2012 o versione successiva

BranchCache 2 è supportato dalle seguenti versioni di ONTAP e dagli host Windows:

- Server di contenuti: SVM con ONTAP
- Server cache: Windows Server 2012 o versione successiva
- Peer o client: Windows 8 o Windows Server 2012 o versione successiva

### **Motivi per cui ONTAP invalida gli hash di BranchCache**

Comprendere i motivi per cui ONTAP invalida gli hash può essere utile durante la pianificazione della configurazione di BranchCache. Può aiutarti a decidere quale modalità operativa configurare e a scegliere quali condivisioni abilitare BranchCache.

ONTAP deve gestire gli hash BranchCache per garantire la validità degli hash. Se un hash non è valido, ONTAP invalida l'hash e calcola un nuovo hash alla successiva richiesta del contenuto, presupponendo che BranchCache sia ancora abilitato.

ONTAP invalida gli hash per i seguenti motivi:

- La chiave del server viene modificata.

Se la chiave del server viene modificata, ONTAP invalida tutti gli hash nell'archivio hash.

- Un hash viene svuotato dalla cache perché è stata raggiunta la dimensione massima dell'archivio hash BranchCache.

Si tratta di un parametro sintonizzabile che può essere modificato per soddisfare i requisiti di business.

- Un file viene modificato tramite accesso SMB o NFS.
- Un file per il quale sono stati calcolati gli hash viene ripristinato utilizzando `snap restore` comando.
- Un volume che contiene condivisioni SMB abilitate a BranchCache viene ripristinato utilizzando `snap restore` comando.

### **Linee guida per la scelta della posizione dell'archivio hash**

Quando configuri BranchCache, scegli dove memorizzare gli hash e le dimensioni dell'archivio hash. La comprensione delle linee guida per la scelta della posizione e delle dimensioni dell'archivio hash può aiutarti a pianificare la configurazione di BranchCache su una SVM abilitata per CIFS.

- È necessario individuare l'archivio hash su un volume in cui sono consentiti gli aggiornamenti atime.

Il tempo di accesso a un file hash viene utilizzato per conservare i file ad accesso frequente nell'archivio hash. Se gli aggiornamenti aTime sono disattivati, viene utilizzata l'ora di creazione. È preferibile utilizzare atime per tenere traccia dei file utilizzati di frequente.

- Non è possibile memorizzare gli hash su file system di sola lettura, ad esempio destinazioni SnapMirror e volumi SnapLock.
- Se viene raggiunta la dimensione massima dell'archivio hash, gli hash più vecchi vengono eliminati per fare spazio ai nuovi hash.

È possibile aumentare le dimensioni massime dell'archivio hash per ridurre la quantità di hash scaricati dalla cache.

- Se il volume su cui si memorizzano gli hash non è disponibile o è pieno, o se si verifica un problema di comunicazione all'interno del cluster in cui il servizio BranchCache non riesce a recuperare le informazioni sugli hash, i servizi BranchCache non sono disponibili.

Il volume potrebbe non essere disponibile perché non è in linea o perché l'amministratore dello storage ha specificato una nuova posizione per l'archivio hash.

Questo non causa problemi di accesso al file. Se l'accesso all'archivio hash viene impedito, ONTAP restituisce un errore definito da Microsoft al client, che fa in modo che il client richieda il file utilizzando la normale richiesta di lettura SMB.

## Informazioni correlate

[Configurare BranchCache sul server SMB](#)

[Modificare la configurazione di BranchCache](#)

## Consigli su BranchCache

Prima di configurare BranchCache, è necessario tenere a mente alcuni consigli quando si decide quali condivisioni SMB si desidera attivare il caching BranchCache.

Quando decidi quale modalità operativa utilizzare e su quali condivisioni SMB abilitare BranchCache, devi tenere a mente i seguenti consigli:

- I vantaggi di BranchCache si riducono quando i dati da memorizzare nella cache in remoto cambiano frequentemente.
- I servizi BranchCache sono vantaggiosi per le condivisioni contenenti contenuto di file che viene riutilizzato da più client della sede remota o da contenuto di file a cui un singolo utente remoto accede ripetutamente.
- Considerare l'attivazione del caching per contenuti di sola lettura, come i dati nelle copie Snapshot e nelle destinazioni SnapMirror.

## Configurare BranchCache

### Panoramica sulla configurazione di BranchCache

Configuri BranchCache sul tuo server SMB utilizzando i comandi ONTAP. Per implementare BranchCache, è necessario configurare anche i client e, facoltativamente, i server di cache ospitati nelle filiali in cui si desidera memorizzare il contenuto nella cache.

Se configuri BranchCache per abilitare il caching su base share-by-share, devi attivare BranchCache sulle condivisioni SMB per le quali desideri fornire servizi di caching BranchCache.

## Requisiti per la configurazione di BranchCache

Una volta soddisfatti alcuni prerequisiti, puoi impostare BranchCache.

Prima di configurare BranchCache sul server CIFS per SVM, è necessario soddisfare i seguenti requisiti:

- ONTAP deve essere installato su tutti i nodi del cluster.
- È necessario disporre della licenza CIFS ed è necessario configurare un server SMB. La licenza SMB è inclusa con "ONTAP [uno](#)". Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.
- È necessario configurare la connettività di rete IPv4 o IPv6.
- Per BranchCache 1, è necessario attivare SMB 2.1 o versione successiva.
- Per BranchCache 2, SMB 3.0 deve essere attivato e i client Windows remoti devono supportare BranchCache 2.

## Configurare BranchCache sul server SMB

Puoi configurare BranchCache per fornire i servizi BranchCache in base alle condivisioni. In alternativa, puoi configurare BranchCache per attivare automaticamente il caching su tutte le condivisioni SMB.

### A proposito di questa attività

È possibile configurare BranchCache sulle SVM.

- È possibile creare una configurazione BranchCache all-share se si desidera offrire servizi di caching per tutti i contenuti contenuti all'interno di tutte le condivisioni SMB sul server CIFS.
- È possibile creare una configurazione BranchCache per condivisione se si desidera offrire servizi di caching per il contenuto contenuto all'interno di condivisioni SMB selezionate sul server CIFS.

Durante la configurazione di BranchCache, è necessario specificare i seguenti parametri:

Parametri richiesti	Descrizione
<i>Nome SVM</i>	BranchCache viene configurato per SVM. Specificare su quale SVM CIFS-Enabled si desidera configurare il servizio BranchCache.

Parametri richiesti	Descrizione
<i>Percorso all'archivio hash</i>	<p>Gli hash BranchCache vengono memorizzati in file regolari sul volume SVM. È necessario specificare il percorso di una directory esistente in cui si desidera che ONTAP memorizzi i dati hash. Il percorso hash BranchCache deve essere leggibile-scrivibile. I percorsi di sola lettura, come le directory Snapshot, non sono consentiti. È possibile memorizzare i dati hash in un volume che contiene altri dati oppure creare un volume separato per memorizzare i dati hash.</p> <p>Se SVM è un'origine di disaster recovery SVM, il percorso hash non può trovarsi sul volume root. Questo perché il volume root non viene replicato nella destinazione del disaster recovery.</p> <p>Il percorso hash può contenere spazi vuoti e qualsiasi carattere di nome file valido.</p>

È possibile specificare i seguenti parametri:

Parametri opzionali	Descrizione
<i>Versioni supportate</i>	ONTAP supporta BranchCache 1 e 2. È possibile attivare la versione 1, la versione 2 o entrambe le versioni. L'impostazione predefinita prevede l'attivazione di entrambe le versioni.
<i>Dimensione massima dell'archivio hash</i>	È possibile specificare la dimensione da utilizzare per l'archivio dati hash. Se i dati hash superano questo valore, ONTAP elimina gli hash più vecchi per fare spazio agli hash più recenti. La dimensione predefinita per l'archivio hash è 1 GB. Le prestazioni di BranchCache sono più efficienti se gli hash non vengono scartati in modo eccessivamente aggressivo. Se si determina che gli hash vengono eliminati frequentemente perché l'archivio hash è pieno, è possibile aumentare le dimensioni dell'archivio hash modificando la configurazione di BranchCache.



Parametri opzionali	Descrizione
<i>Chiave server</i>	È possibile specificare una chiave server utilizzata dal servizio BranchCache per impedire ai client di rappresentare il server BranchCache. Se non si specifica una chiave server, ne viene generata una in modo casuale quando si crea la configurazione BranchCache. È possibile impostare la chiave del server su un valore specifico in modo che, se più server forniscono dati BranchCache per gli stessi file, i client possano utilizzare gli hash da qualsiasi server utilizzando la stessa chiave del server. Se la chiave del server contiene spazi, racchiudere la chiave del server tra virgolette.
<i>Modalità operativa</i>	<p>Per impostazione predefinita, BranchCache viene attivato in base alle condivisioni.</p> <ul style="list-style-type: none"> <li>• Per creare una configurazione BranchCache in cui abilitare BranchCache in base alle condivisioni, non è possibile specificare questo parametro facoltativo oppure è possibile specificarlo <code>per-share</code>.</li> <li>• Per attivare automaticamente BranchCache su tutte le condivisioni, è necessario impostare la modalità operativa su <code>all-shares</code>.</li> </ul>

## Fasi

### 1. Abilitazione di SMB 2.1 e 3.0 in base alle esigenze:

- Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
- Controllare le impostazioni SMB SVM configurate per determinare se tutte le versioni richieste di SMB sono abilitate: `vserver cifs options show -vserver vserver_name`
- Se necessario, abilitare SMB 2.1: `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

Il comando abilita sia SMB 2.0 che SMB 2.1.

- Se necessario, abilitare SMB 3.0: `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
- Tornare al livello di privilegio admin: `set -privilege admin`

### 2. Configura BranchCache: `vserver cifs branchcache create -vserver vserver_name -hash -store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all}] [-server-key text] -operating-mode {per-share|all-shares}`

Il percorso di storage hash specificato deve esistere e risiedere in un volume gestito da SVM. Il percorso deve trovarsi anche su un volume in lettura/scrittura. Il comando non riesce se il percorso è di sola lettura o non esiste.

Se si desidera utilizzare la stessa chiave server per ulteriori configurazioni SVM BranchCache, registrare il valore immesso per la chiave server. La chiave server non viene visualizzata quando si visualizzano informazioni sulla configurazione di BranchCache.

3. Verificare che la configurazione di BranchCache sia corretta: `vserver cifs branchcache show -vserver vserver_name`

### Esempi

I seguenti comandi verificano che SMB 2.1 e 3.0 siano attivati e configurano BranchCache per abilitare automaticamente il caching su tutte le condivisioni SMB su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
                Supported BranchCache Versions: enable_all
                        Path to Hash Store: /hash_data
                Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
                CIFS BranchCache Operating Modes: all_shares
```

I seguenti comandi verificano che SMB 2.1 e 3.0 siano attivati, configurano BranchCache per abilitare il caching per condivisione su SVM vs1 e verificano la configurazione di BranchCache:

```

cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vsserver cifs options show -vsserver vs1 -fields smb2-
enabled,smb3-enabled
vsserver smb2-enabled smb3-enabled
-----
vs1      true      true

cluster1::*> set -privilege admin

cluster1::> vsserver cifs branchcache create -vsserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vsserver cifs branchcache show -vsserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share

```

## Informazioni correlate

[Requisiti e linee guida: Supporto della versione di BranchCache](#)

[Dove trovare informazioni sulla configurazione di BranchCache presso la sede remota](#)

[Crea una condivisione SMB abilitata per BranchCache](#)

[Abilitare BranchCache su una condivisione SMB esistente](#)

[Modificare la configurazione di BranchCache](#)

[Panoramica sulla disattivazione di BranchCache sulle condivisioni SMB](#)

[Eliminare la configurazione BranchCache sulle SVM](#)

## Dove trovare informazioni sulla configurazione di BranchCache presso la sede remota

Dopo aver configurato BranchCache sul server SMB, è necessario installare e configurare BranchCache sui computer client e, facoltativamente, sui server di caching della sede remota. Microsoft fornisce istruzioni per la configurazione di BranchCache presso la sede remota.

Le istruzioni per la configurazione dei client delle filiali e, facoltativamente, dei server di caching per l'utilizzo di BranchCache sono disponibili sul sito Web Microsoft BranchCache.

["Documenti Microsoft BranchCache: Novità"](#)

## Configurare le condivisioni SMB abilitate per BranchCache

### Panoramica sulla configurazione delle condivisioni SMB abilitate a BranchCache

Dopo aver configurato BranchCache sul server SMB e nella filiale, è possibile attivare BranchCache sulle condivisioni SMB che contengono contenuti che si desidera consentire ai client delle filiali di memorizzare nella cache.

Il caching BranchCache può essere attivato su tutte le condivisioni SMB sul server SMB o su base share-by-share.

- Se abiliti BranchCache su base share-by-share, puoi abilitare BranchCache durante la creazione della condivisione o modificando le condivisioni esistenti.

Se abiliti il caching su una condivisione SMB esistente, ONTAP inizia a calcolare gli hash e a inviare metadati ai client che richiedono contenuti non appena abiliti BranchCache su quella condivisione.

- Tutti i client che dispongono di una connessione SMB esistente a una condivisione non ricevono il supporto BranchCache se BranchCache viene successivamente abilitato su tale condivisione.

ONTAP annuncia il supporto di BranchCache per una condivisione al momento della configurazione della sessione SMB. I client che hanno già stabilito sessioni quando BranchCache è abilitato devono disconnettersi e riconnettersi per utilizzare il contenuto memorizzato nella cache per questa condivisione.



Se BranchCache su una condivisione SMB viene successivamente disattivato, ONTAP interrompe l'invio dei metadati al client richiedente. Un client che necessita di dati lo recupera direttamente dal server di contenuti (server SMB).

## Crea una condivisione SMB abilitata per BranchCache

È possibile attivare BranchCache su una condivisione SMB quando si crea la condivisione impostando `branchcache` condividere la proprietà.

### A proposito di questa attività

- Se BranchCache è attivato nella condivisione SMB, la condivisione deve avere la configurazione dei file offline impostata sul caching manuale.

Questa è l'impostazione predefinita quando si crea una condivisione.

- È inoltre possibile specificare ulteriori parametri di condivisione opzionali quando si crea la condivisione abilitata per BranchCache.
- È possibile impostare `branchcache` Proprietà su una condivisione anche se BranchCache non è configurato e abilitato sulla macchina virtuale di storage (SVM).

Tuttavia, se si desidera che la condivisione offra contenuti memorizzati nella cache, è necessario configurare e attivare BranchCache sulla SVM.

- Poiché non esistono proprietà di condivisione predefinite applicate alla condivisione quando si utilizza `-share-properties` è necessario specificare tutte le altre proprietà di condivisione che si desidera applicare alla condivisione oltre a `branchcache` condividere la proprietà utilizzando un elenco delimitato da virgole.
- Per ulteriori informazioni, vedere la pagina man di `vserver cifs share create` comando.

## Fase

1. Creare una condivisione SMB abilitata per BranchCache:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties branchcache[,...]
```

2. Verificare che la proprietà di condivisione BranchCache sia impostata sulla condivisione SMB utilizzando `vserver cifs share show` comando.

## Esempio

Il seguente comando crea una condivisione SMB abilitata a BranchCache denominata “data” con un percorso di /data Su SVM vs1. Per impostazione predefinita, l'impostazione file offline è impostata su manual:

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path /data -share-properties branchcache,oplocks,browsable,changeNotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
      Vserver: vs1
      Share: data
CIFS Server NetBIOS Name: VS1
      Path: /data
      Share Properties: branchcache
                       oplocks
                       browsable
                       changeNotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: data
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

## Informazioni correlate

[Disattivazione di BranchCache in una singola condivisione SMB](#)

## Abilitare BranchCache su una condivisione SMB esistente

È possibile attivare BranchCache su una condivisione SMB esistente aggiungendo `branchcache` condividere la proprietà con l'elenco esistente di proprietà di condivisione.

## A proposito di questa attività

- Se BranchCache è attivato nella condivisione SMB, la condivisione deve avere la configurazione dei file offline impostata sul caching manuale.

Se l'impostazione dei file offline della condivisione esistente non è impostata sul caching manuale, è necessario configurarla modificando la condivisione.

- È possibile impostare `branchcache` Proprietà su una condivisione anche se BranchCache non è configurato e abilitato sulla macchina virtuale di storage (SVM).

Tuttavia, se si desidera che la condivisione offra contenuti memorizzati nella cache, è necessario configurare e attivare BranchCache sulla SVM.

- Quando si aggiunge `branchcache` la proprietà di condivisione nella condivisione, le impostazioni di condivisione esistenti e le proprietà di condivisione vengono conservate.

La proprietà di condivisione BranchCache viene aggiunta all'elenco esistente di proprietà di condivisione. Per ulteriori informazioni sull'utilizzo di `vserver cifs share properties add` vedere le pagine man.

## Fasi

1. Se necessario, configurare l'impostazione di condivisione file offline per il caching manuale:
  - a. Determinare l'impostazione di condivisione dei file offline utilizzando `vserver cifs share show` comando.
  - b. Se l'impostazione di condivisione file offline non è impostata su manuale, modificarla nel valore richiesto: `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. Abilitare BranchCache su una condivisione SMB esistente: `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. Verificare che la proprietà di condivisione BranchCache sia impostata sulla condivisione SMB: `vserver cifs share show -vserver vserver_name -share-name share_name`

## Esempio

Il seguente comando abilita BranchCache su una condivisione SMB esistente denominata "data2" con un percorso di `/data2` Su SVM vs1:

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     showsnapshot
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vservice cifs share properties add -vservice vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vservice cifs share show -vservice vs1 -share-name data2
```

```

        Vservice: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     showsnapshot
                     changenotify
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

## Informazioni correlate

## Gestire e monitorare la configurazione di BranchCache

### Modificare le configurazioni di BranchCache

È possibile modificare la configurazione del servizio BranchCache sulle SVM, tra cui la modifica del percorso della directory dell'archivio hash, la dimensione massima della directory dell'archivio hash, la modalità operativa e le versioni di BranchCache supportate. È inoltre possibile aumentare le dimensioni del volume che contiene l'archivio hash.

#### Fasi

1. Eseguire l'azione appropriata:

Se si desidera...	Immettere quanto segue...
Modificare le dimensioni della directory dell'archivio hash	<code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB</code>
MB	GB
TB	PB]}`
Aumentare le dimensioni del volume che contiene l'archivio hash	<code>`volume size -vserver vserver_name -volume volume_name -new-size new_size[k</code>
m	g
t]` Se il volume contenente l'archivio hash si riempie, potrebbe essere possibile aumentare le dimensioni del volume. È possibile specificare la nuova dimensione del volume come numero seguito da una designazione dell'unità.  Scopri di più <a href="#">"Gestione dei volumi FlexVol"</a>	Modificare il percorso della directory dell'archivio hash



Se si desidera...	Immettere quanto segue...
<code>`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true</code>	<p><code>false}`</code> Se SVM è un'origine di disaster recovery SVM, il percorso hash non può trovarsi sul volume root. Questo perché il volume root non viene replicato nella destinazione del disaster recovery.</p> <p>Il percorso hash di BranchCache può contenere spazi vuoti e qualsiasi carattere valido per il nome del file.</p> <p>Se si modifica il percorso hash, <code>-flush-hashes</code> È un parametro obbligatorio che specifica se si desidera che ONTAP svuota gli hash dalla posizione dell'archivio hash originale. È possibile impostare i seguenti valori per <code>-flush-hashes</code> parametro:</p> <p><b>Se si specifica <code>true</code>, ONTAP elimina gli hash nella posizione originale e crea nuovi hash nella nuova posizione man mano che le nuove richieste vengono effettuate dai client abilitati a BranchCache.</b></p> <p>Se si specifica <code>false</code>, gli hash non vengono spazzati via.</p> <p>+</p> <p>In questo caso, è possibile scegliere di riutilizzare gli hash esistenti in un secondo momento modificando il percorso dell'archivio hash nella posizione originale.</p>
Modificare la modalità operativa	<code>`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share</code>
<code>all-shares</code>	<p><code>disable}`</code></p> <p>Quando si modifica la modalità operativa, tenere presente quanto segue:</p> <p><b>ONTAP annuncia il supporto di BranchCache per una condivisione quando viene impostata la sessione SMB.</b></p> <p>I client che hanno già stabilito sessioni quando BranchCache è abilitato devono disconnettersi e riconnettersi per utilizzare il contenuto memorizzato nella cache per questa condivisione.</p>
Modificare il supporto della versione di BranchCache	<code>`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable</code>
<code>v2-enable</code>	<code>enable-all}`</code>

2. Verificare le modifiche alla configurazione utilizzando `vserver cifs branchcache show` comando.

## Visualizza informazioni sulle configurazioni di BranchCache

È possibile visualizzare informazioni sulle configurazioni di BranchCache sulle macchine virtuali di storage (SVM), che possono essere utilizzate per verificare una configurazione o per determinare le impostazioni correnti prima di modificare una configurazione.

### Fase

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare...	Immettere questo comando...
Informazioni riepilogative sulle configurazioni di BranchCache su tutte le SVM	<code>vserver cifs branchcache show</code>
Informazioni dettagliate sulla configurazione di una SVM specifica	<code>vserver cifs branchcache show -vserver vserver_name</code>

### Esempio

Nell'esempio seguente vengono visualizzate informazioni sulla configurazione di BranchCache su SVM vs1:

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                        Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

## Modificare la chiave del server BranchCache

È possibile modificare la chiave del server BranchCache modificando la configurazione BranchCache sulla macchina virtuale di storage (SVM) e specificando una chiave server diversa.

### A proposito di questa attività

È possibile impostare la chiave del server su un valore specifico in modo che, se più server forniscono dati BranchCache per gli stessi file, i client possano utilizzare gli hash da qualsiasi server utilizzando la stessa chiave del server.

Quando si modifica la chiave del server, è necessario svuotare anche la cache hash. Dopo aver eseguito il flushing degli hash, ONTAP crea nuovi hash man mano che i client abilitati a BranchCache inoltrano nuove richieste.

### Fasi

1. Modificare la chiave del server utilizzando il seguente comando: `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

Quando si configura una nuova chiave server, è necessario specificare anche `-flush-hashes` e impostare il valore su `true`.

2. Verificare che la configurazione di BranchCache sia corretta utilizzando `vserver cifs branchcache show` comando.

### Esempio

Nell'esempio seguente viene impostata una nuova chiave server che contiene spazi e svuota la cache hash su SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

### Informazioni correlate

[Motivi per cui ONTAP invalida gli hash di BranchCache](#)

### Pre-calcolare gli hash BranchCache su percorsi specifici

È possibile configurare il servizio BranchCache per pre-calcolare gli hash per un singolo file, per una directory o per tutti i file di una struttura di directory. Questo può essere utile se si desidera calcolare gli hash sui dati in una condivisione abilitata per BranchCache durante le ore non di punta.

#### A proposito di questa attività

Se si desidera raccogliere un campione di dati prima di visualizzare le statistiche hash, è necessario utilizzare `statistics start` e opzionale `statistics stop` comandi.

- È necessario specificare la SVM (Storage Virtual Machine) e il percorso su cui si desidera pre-calcolare gli hash.
- È inoltre necessario specificare se si desidera che gli hash vengano calcolati in modo ricorsivo.
- Se si desidera che gli hash vengano calcolati in modo ricorrente, il servizio BranchCache attraversa l'intero albero di directory nel percorso specificato e calcola gli hash per ciascun oggetto idoneo.

### Fasi

1. Pre-calcolare gli hash come desiderato:

Se si desidera pre-calcolare gli hash su...	Immettere il comando...
Un singolo file o directory	<code>vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false</code>
In modo ricorrente su tutti i file di una struttura di directory	<code>vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true</code>

2. Verificare che gli hash vengano calcolati utilizzando `statistics` comando:

- a. Visualizzare le statistiche per `hashd` Oggetto sull'istanza SVM desiderata: `statistics show -object hashd -instance vserver_name`
- b. Verificare che il numero di hash creati aumenti ripetendo il comando.

### Esempi

Nell'esempio seguente vengono creati gli hash sul percorso `/data` E su tutti i file e sottodirectory contenuti su SVM vs1:

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true
```

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	85
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

```
cluster1::> statistics show -object hashd -instance vs1
```

Object: hashd

Instance: vs1

Start-time: 9/6/2012 19:09:54

End-time: 9/6/2012 19:11:15

Cluster: cluster1

Counter	Value
branchcache_hash_created	92
branchcache_hash_files_replaced	0
branchcache_hash_rejected	0
branchcache_hash_store_bytes	0
branchcache_hash_store_size	0
instance_name	vs1
node_name	node1
node_uuid	11111111-1111-1111-1111-111111111111
process_name	-

## Informazioni correlate

["Configurazione del monitoraggio delle performance"](#)

## Scarica gli hash dall'archivio hash BranchCache di SVM

È possibile scaricare tutti gli hash memorizzati nella cache dall'archivio hash BranchCache sulla macchina virtuale di storage (SVM). Ciò può essere utile se hai modificato la configurazione BranchCache della filiale. Ad esempio, se di recente è stata riconfigurata la modalità di caching dalla modalità di caching distribuito alla modalità di caching in hosting, si consiglia di svuotare l'archivio hash.

### A proposito di questa attività

Dopo aver eseguito il flushing degli hash, ONTAP crea nuovi hash man mano che i client abilitati a BranchCache inoltrano nuove richieste.

### Fase

1. Eliminare gli hash dall'archivio hash di BranchCache: `vserver cifs branchcache hash-flush -vserver vserver_name`  
  
`vserver cifs branchcache hash-flush -vserver vs1`

## Visualizzare le statistiche di BranchCache

È possibile visualizzare le statistiche di BranchCache, tra l'altro, per identificare le prestazioni del caching, determinare se la configurazione fornisce contenuti memorizzati nella cache ai client e determinare se i file hash sono stati eliminati per fare spazio a dati hash più recenti.

### A proposito di questa attività

Il `hashd` Oggetto Statistic contiene contatori che forniscono informazioni statistiche sugli hash BranchCache. Il `cifs` Oggetto Statistic contiene contatori che forniscono informazioni statistiche sull'attività correlata a BranchCache. È possibile raccogliere e visualizzare informazioni su questi oggetti a livello di privilegi avanzati.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`

```
cluster1::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them  
only when directed to do so by support personnel.  
Do you want to continue? {y|n}: y
```

2. Visualizzare i contatori relativi a BranchCache utilizzando `statistics catalog counter show` comando.

Per ulteriori informazioni sui contatori delle statistiche, vedere la pagina man di questo comando.

```
cluster1::*> statistics catalog counter show -object hashd  
  
Object: hashd
```

Counter	Description
-----	-----
branchcache_hash_created	Number of times a request to generate BranchCache hash for a file succeeded.
branchcache_hash_files_replaced	Number of times a BranchCache hash file was deleted to make room for more recent hash data. This happens if the hash store size is exceeded.
branchcache_hash_rejected	Number of times a request to generate BranchCache hash data failed.
branchcache_hash_store_bytes	Total number of bytes used to store hash data.
branchcache_hash_store_size	Total space used to store BranchCache hash data for the Vserver.
instance_name	Instance Name
instance_uuid	Instance UUID
node_name	System node name
node_uuid	System node id

9 entries were displayed.

cluster1::\*> statistics catalog counter show -object cifs

Object: cifs

Counter	Description
-----	-----
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
avg_junction_depth	Average number of junctions crossed by SMB and SMB2 path-based commands
branchcache_hash_fetch_fail	Total number of times a request to fetch hash data failed. These are failures when

```

It
data
branchcache_hash_fetch_ok
hash
branchcache_hash_sent_bytes
branchcache_missing_hash_bytes
to be
that
.....Output truncated.....
attempting to read existing hash data.
does not include attempts to fetch hash
that has not yet been generated.
Total number of times a request to fetch
data succeeded.
Total number of bytes sent to clients
requesting hashes.
Total number of bytes of data that had
read by the client because the hash for
content was not available on the server.

```

3. Raccogliere le statistiche relative a BranchCache utilizzando `statistics start` e `statistics stop` comandi.

```

cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11

```

4. Visualizzare le statistiche BranchCache raccolte utilizzando `statistics show` comando.



```
cluster1::*> statistics show -object cifs -counter  
branchcache_hash_sent_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0
branchcache_hash_sent_bytes	0

```
cluster1::*> statistics show -object cifs -counter  
branchcache_missing_hash_bytes -sample-id 11
```

```
Object: cifs  
Instance: vs1  
Start-time: 12/26/2012 19:50:24  
End-time: 12/26/2012 19:51:01  
Cluster: cluster1
```

Counter	Value
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0
branchcache_missing_hash_bytes	0

5. Tornare al livello di privilegio admin: `set -privilege admin`

```
cluster1::*> set -privilege admin
```

## Informazioni correlate

[Visualizzazione delle statistiche](#)

["Configurazione del monitoraggio delle performance"](#)

## Supporto per gli oggetti Criteri di gruppo BranchCache

BranchCache di ONTAP fornisce il supporto per gli oggetti Criteri di gruppo

BranchCache, che consentono la gestione centralizzata di alcuni parametri di configurazione BranchCache. Per BranchCache vengono utilizzati due GPO, la pubblicazione Hash per l'oggetto Criteri di gruppo BranchCache e il supporto della versione Hash per l'oggetto Criteri di gruppo BranchCache.

- **Pubblicazione Hash per l'oggetto Criteri di gruppo BranchCache**

La pubblicazione Hash per l'oggetto Criteri di gruppo BranchCache corrisponde a. `-operating-mode` parametro. Quando si verificano gli aggiornamenti dei GPO, questo valore viene applicato agli oggetti SVM (Storage Virtual Machine) contenuti nell'unità organizzativa (OU) a cui si applicano i criteri di gruppo.

- **Supporto della versione Hash per l'oggetto Criteri di gruppo BranchCache**

Il supporto della versione Hash per l'oggetto Criteri di gruppo BranchCache corrisponde a. `-versions` parametro. Quando si verificano gli aggiornamenti dei GPO, questo valore viene applicato agli oggetti SVM contenuti nell'unità organizzativa a cui si applicano i criteri di gruppo.

## Informazioni correlate

[Applicazione di oggetti Criteri di gruppo ai server CIFS](#)

## Visualizza informazioni sugli oggetti Criteri di gruppo BranchCache

È possibile visualizzare informazioni sulla configurazione dell'oggetto Criteri di gruppo (GPO) del server CIFS per determinare se gli oggetti Criteri di gruppo BranchCache sono definiti per il dominio a cui appartiene il server CIFS e, in caso affermativo, quali sono le impostazioni consentite. È inoltre possibile determinare se le impostazioni dell'oggetto Criteri di gruppo BranchCache sono applicate al server CIFS.

### A proposito di questa attività

Anche se un'impostazione GPO è definita all'interno del dominio a cui appartiene il server CIFS, non viene necessariamente applicata all'unità organizzativa (OU) contenente la SVM (Storage Virtual Machine) abilitata per CIFS. Le impostazioni dell'oggetto Criteri di gruppo applicato sono il sottoinsieme di tutti gli oggetti Criteri di gruppo definiti che vengono applicati alla SVM abilitata per CIFS. Le impostazioni BranchCache applicate tramite gli oggetti GPO sovrascrivono le impostazioni applicate tramite l'interfaccia CLI.

### Fasi

1. Visualizzare l'impostazione dell'oggetto Criteri di gruppo BranchCache definita per il dominio Active Directory utilizzando `vserver cifs group-policy show-defined` comando.



In questo esempio non vengono visualizzati tutti i campi di output disponibili per il comando. L'output viene troncato.

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
    Level: Domain
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
    Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication for Mode BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

2. Visualizzare l'impostazione dell'oggetto Criteri di gruppo BranchCache applicata al server CIFS utilizzando `vserver cifs group-policy show-applied` comando.



In questo esempio non vengono visualizzati tutti i campi di output disponibili per il comando. L'output viene troncato.

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
```

```
Vserver: vs1
```

```
-----
```

```
    GPO Name: Default Domain Policy
```

```
        Level: Domain
```

```
        Status: enabled
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

```
    GPO Name: Resultant Set of Policy
```

```
        Level: RSOP
```

```
Advanced Audit Settings:
```

```
    Object Access:
```

```
        Central Access Policy Staging: failure
```

```
Registry Settings:
```

```
    Refresh Time Interval: 22
```

```
    Refresh Random Offset: 8
```

```
    Hash Publication Mode for BranchCache: per-share
```

```
    Hash Version Support for BranchCache: version1
```

```
[...]
```

## Informazioni correlate

[Attivazione o disattivazione del supporto GPO su un server CIFS](#)

## Disattiva BranchCache sulle condivisioni SMB

### Panoramica sulla disattivazione di BranchCache sulle condivisioni SMB

Se non si desidera fornire servizi di caching BranchCache su determinate condivisioni SMB, ma si desidera fornire servizi di caching su tali condivisioni in un secondo momento, è possibile disattivare BranchCache in base alla condivisione. Se BranchCache è configurato per offrire il caching su tutte le condivisioni, ma si desidera disattivare temporaneamente tutti i servizi di caching, è possibile modificare la configurazione di BranchCache per interrompere il caching automatico su tutte le condivisioni.

Se BranchCache su una condivisione SMB viene successivamente disattivato dopo la prima attivazione, ONTAP interrompe l'invio dei metadati al client richiedente. Un client che necessita di dati lo recupera

direttamente dal server di contenuti (server CIFS sulla macchina virtuale di storage (SVM)).

## Informazioni correlate

[Configurazione delle condivisioni SMB abilitate per BranchCache](#)

## Disattiva BranchCache su una singola condivisione SMB

Se non si desidera offrire servizi di caching su determinate condivisioni che in precedenza offrivano contenuti memorizzati nella cache, è possibile disattivare BranchCache su una condivisione SMB esistente.

### Fase

1. Immettere il seguente comando: `vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties branchcache`

La proprietà di condivisione BranchCache viene rimossa. Le altre proprietà di condivisione applicate rimangono attive.

### Esempio

Il seguente comando disattiva BranchCache in una condivisione SMB esistente denominata "data2":

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data2
```

```

        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
                     branchcache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

```
cluster1::> vsserver cifs share properties remove -vsserver vs1 -share-name
data2 -share-properties branchcache
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name data2
```

```

        Vserver: vs1
        Share: data2
CIFS Server NetBIOS Name: VS1
        Path: /data2
    Share Properties: oplocks
                     browsable
                     changenotify
                     attributecache
    Symlink Properties: -
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
            Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: -
        Offline Files: manual
Vscan File-Operations Profile: standard
```

## Arrestare il caching automatico su tutte le condivisioni SMB

Se la configurazione di BranchCache abilita automaticamente il caching su tutte le condivisioni SMB su ciascuna macchina virtuale di storage (SVM), puoi modificare la configurazione di BranchCache per interrompere automaticamente il caching del contenuto per tutte le condivisioni SMB.

### A proposito di questa attività

Per interrompere il caching automatico su tutte le condivisioni SMB, si cambia la modalità operativa BranchCache in caching per-share.

### Fasi

1. Configurare BranchCache per interrompere il caching automatico su tutte le condivisioni SMB: `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. Verificare che la configurazione di BranchCache sia corretta: `vserver cifs branchcache show -vserver vserver_name`

### Esempio

Il seguente comando modifica la configurazione di BranchCache su storage virtual machine (SVM, precedentemente noto come Vserver) vs1 per interrompere il caching automatico su tutte le condivisioni SMB:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
        Supported BranchCache Versions: enable_all
                                Path to Hash Store: /hash_data
        Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

## Disattivare o attivare BranchCache sulla SVM

### Cosa accade quando si disattiva o si riattiva BranchCache sul server CIFS

Se in precedenza è stato configurato BranchCache ma non si desidera che i client delle filiali utilizzino il contenuto memorizzato nella cache, è possibile disattivare il caching sul server CIFS. Devi essere consapevole di ciò che accade quando disattivi BranchCache.


Quando disattivi BranchCache, ONTAP non calcola più gli hash o invia i metadati al client richiedente. Tuttavia, non si verifica alcuna interruzione nell'accesso ai file. In seguito, quando i client abilitati a BranchCache richiedono informazioni sui metadati per il contenuto a cui desiderano accedere, ONTAP risponde con un errore definito da Microsoft, che fa in modo che il client invii una seconda richiesta, richiedendo il contenuto effettivo. In risposta alla richiesta di contenuto, il server CIFS invia il contenuto effettivo memorizzato sulla macchina virtuale di storage (SVM).

Una volta disattivato BranchCache sul server CIFS, le condivisioni SMB non pubblicizzano le funzionalità di BranchCache. Per accedere ai dati sulle nuove connessioni SMB, i client eseguono le normali richieste SMB in lettura.

Puoi riabilitare BranchCache sul server CIFS in qualsiasi momento.

- Poiché l'archivio hash non viene cancellato quando disattivi BranchCache, ONTAP può utilizzare gli hash memorizzati quando risponde alle richieste hash dopo la riabilitazione di BranchCache, a condizione che l'hash richiesto sia ancora valido.
- Tutti i client che hanno effettuato connessioni SMB alle condivisioni abilitate a BranchCache durante il periodo in cui BranchCache è stato disattivato non ottengono il supporto BranchCache se BranchCache viene successivamente riabilitato.

Questo perché ONTAP pubblicizza il supporto di BranchCache per una condivisione al momento della configurazione della sessione SMB. I client che hanno stabilito sessioni per le condivisioni abilitate a BranchCache mentre BranchCache è stato disattivato devono disconnettersi e riconnettersi per utilizzare il contenuto memorizzato nella cache per questa condivisione.



Se non si desidera salvare l'archivio hash dopo la disattivazione di BranchCache su un server CIFS, è possibile eliminarlo manualmente. Se riabiliti BranchCache, devi assicurarti che la directory dell'archivio hash esista. Una volta riabilitato BranchCache, le condivisioni abilitate a BranchCache pubblicizzano le funzionalità di BranchCache. ONTAP crea nuovi hash man mano che le nuove richieste vengono effettuate dai client abilitati a BranchCache.

**Disattiva o attiva BranchCache**

È possibile disattivare BranchCache sulla macchina virtuale di storage (SVM) modificando la modalità operativa BranchCache su `disabled`. Puoi abilitare BranchCache in qualsiasi momento modificando la modalità operativa per offrire servizi BranchCache per share o automaticamente per tutte le condivisioni.

**Fasi**

1. Eseguire il comando appropriato:

Se si desidera...	Quindi, immettere quanto segue...
Disattiva BranchCache	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode disable</code>
Attiva BranchCache per share	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share</code>
Abilitare BranchCache per tutte le condivisioni	<code>vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares</code>

2. Verificare che la modalità operativa BranchCache sia configurata con l'impostazione desiderata: `vserver cifs branchcache show -vserver vserver_name`



## Esempio

Nell'esempio seguente viene disattivata BranchCache su SVM vs1:

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                Vserver: vs1
Supported BranchCache Versions: enable_all
        Path to Hash Store: /hash_data
Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
CIFS BranchCache Operating Modes: disable
```

## Eliminare la configurazione BranchCache sulle SVM

### Cosa succede quando elimini la configurazione BranchCache

Se in precedenza è stato configurato BranchCache ma non si desidera che la macchina virtuale di storage (SVM) continui a fornire contenuto memorizzato nella cache, è possibile eliminare la configurazione BranchCache sul server CIFS. È necessario essere consapevoli di cosa accade quando si elimina la configurazione.

Quando si elimina la configurazione, ONTAP rimuove dal cluster le informazioni di configurazione relative a tale SVM e interrompe il servizio BranchCache. È possibile scegliere se ONTAP deve eliminare l'archivio hash sulla SVM.

L'eliminazione della configurazione BranchCache non interrompe l'accesso dei client abilitati a BranchCache. Successivamente, quando i client abilitati a BranchCache richiedono informazioni sui metadati sulle connessioni SMB esistenti per il contenuto già memorizzato nella cache, ONTAP risponde con un errore definito da Microsoft, che fa in modo che il client invii una seconda richiesta, richiedendo il contenuto effettivo. In risposta alla richiesta di contenuto, il server CIFS invia il contenuto effettivo memorizzato nella SVM.

Una volta eliminata la configurazione di BranchCache, le condivisioni SMB non pubblicizzano le funzionalità di BranchCache. Per accedere a contenuti che non sono stati precedentemente memorizzati nella cache utilizzando nuove connessioni SMB, i client eseguono normali richieste SMB in lettura.

### Eliminare la configurazione BranchCache

Il comando utilizzato per eliminare il servizio BranchCache sulla macchina virtuale di storage (SVM) varia a seconda che si desideri eliminare o mantenere gli hash esistenti.

#### Fase

1. Eseguire il comando appropriato:

Se si desidera...	Quindi, immettere quanto segue...
Eliminare la configurazione BranchCache ed eliminare gli hash esistenti	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes true</code>
Eliminare la configurazione BranchCache ma mantenere gli hash esistenti	<code>vserver cifs branchcache delete -vserver vserver_name -flush-hashes false</code>

### Esempio

Nell'esempio riportato di seguito viene eliminata la configurazione BranchCache su SVM vs1 e vengono eliminati tutti gli hash esistenti:

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes  
true
```

### Cosa succede a BranchCache quando si esegue il ripristino

È importante comprendere cosa accade quando si ripristina ONTAP a una release che non supporta BranchCache.

- Quando si torna a una versione di ONTAP che non supporta BranchCache, le condivisioni SMB non pubblicizzano le funzionalità di BranchCache ai client abilitati a BranchCache; pertanto, i client non richiedono informazioni hash.

Richiedono invece il contenuto effettivo utilizzando le normali richieste di lettura SMB. In risposta alla richiesta di contenuto, il server SMB invia il contenuto effettivo memorizzato sulla macchina virtuale di storage (SVM).

- Quando un nodo che ospita un archivio hash viene ripristinato a una release che non supporta BranchCache, l'amministratore dello storage deve ripristinare manualmente la configurazione BranchCache utilizzando un comando stampato durante il revert.

Questo comando elimina la configurazione e gli hash di BranchCache.

Una volta completato il ripristino, l'amministratore dello storage può eliminare manualmente la directory che conteneva l'archivio hash, se lo si desidera.

### Informazioni correlate

[Eliminazione della configurazione BranchCache sulle SVM](#)

### Migliorare le performance di copia remota di Microsoft

**Migliora la panoramica delle performance della copia remota di Microsoft**

Microsoft Offloaded Data Transfer (ODX), noto anche come *copy offload*, consente il trasferimento diretto dei dati all'interno o tra dispositivi di storage compatibili senza trasferire i dati attraverso il computer host.

ONTAP supporta ODX per i protocolli SMB e SAN. L'origine può essere un server CIFS o un LUN e la destinazione può essere un server CIFS o un LUN.

Nei trasferimenti di file non ODX, i dati vengono letti dall'origine e trasferiti attraverso la rete al computer client. Il computer client trasferisce i dati di nuovo sulla rete alla destinazione. In sintesi, il computer client legge i dati dall'origine e li scrive nella destinazione. Con i trasferimenti di file ODX, i dati vengono copiati direttamente dall'origine alla destinazione.

Poiché le copie ODX offloaded vengono eseguite direttamente tra lo storage di origine e di destinazione, le performance sono notevolmente migliorate. I benefici delle performance ottenuti includono tempi di copia più rapidi tra origine e destinazione, utilizzo ridotto delle risorse (CPU, memoria) sul client e utilizzo ridotto della larghezza di banda i/o di rete.

Per gli ambienti SMB, questa funzionalità è disponibile solo quando sia il client che il server di storage supportano SMB 3.0 e la funzionalità ODX. Per gli ambienti SAN, questa funzionalità è disponibile solo quando sia il client che il server di storage supportano la funzionalità ODX. I computer client che supportano ODX e che hanno ODX abilitato automaticamente e in modo trasparente utilizzano il trasferimento di file offload durante lo spostamento o la copia dei file. ODX viene utilizzato indipendentemente dal fatto che si trascinino i file tramite Esplora risorse o si utilizzino comandi di copia dei file dalla riga di comando o che un'applicazione client avvii richieste di copia dei file.

### Informazioni correlate

[Migliorare i tempi di risposta del client fornendo riferimenti automatici ai nodi SMB con Auto Location](#)

["Configurazione SMB per Microsoft Hyper-V e SQL Server"](#)

### Come funziona ODX

L'offload delle copie di ODX utilizza un meccanismo basato su token per la lettura e la scrittura dei dati all'interno o tra server CIFS abilitati per ODX. Invece di instradare i dati attraverso l'host, il server CIFS invia al client un piccolo token, che rappresenta i dati. Il client ODX presenta tale token al server di destinazione, che può quindi trasferire i dati rappresentati da tale token dall'origine alla destinazione.

Quando un client ODX rileva che il server CIFS è compatibile con ODX, apre il file di origine e richiede un token dal server CIFS. Dopo aver aperto il file di destinazione, il client utilizza il token per indicare al server di copiare i dati direttamente dall'origine alla destinazione.

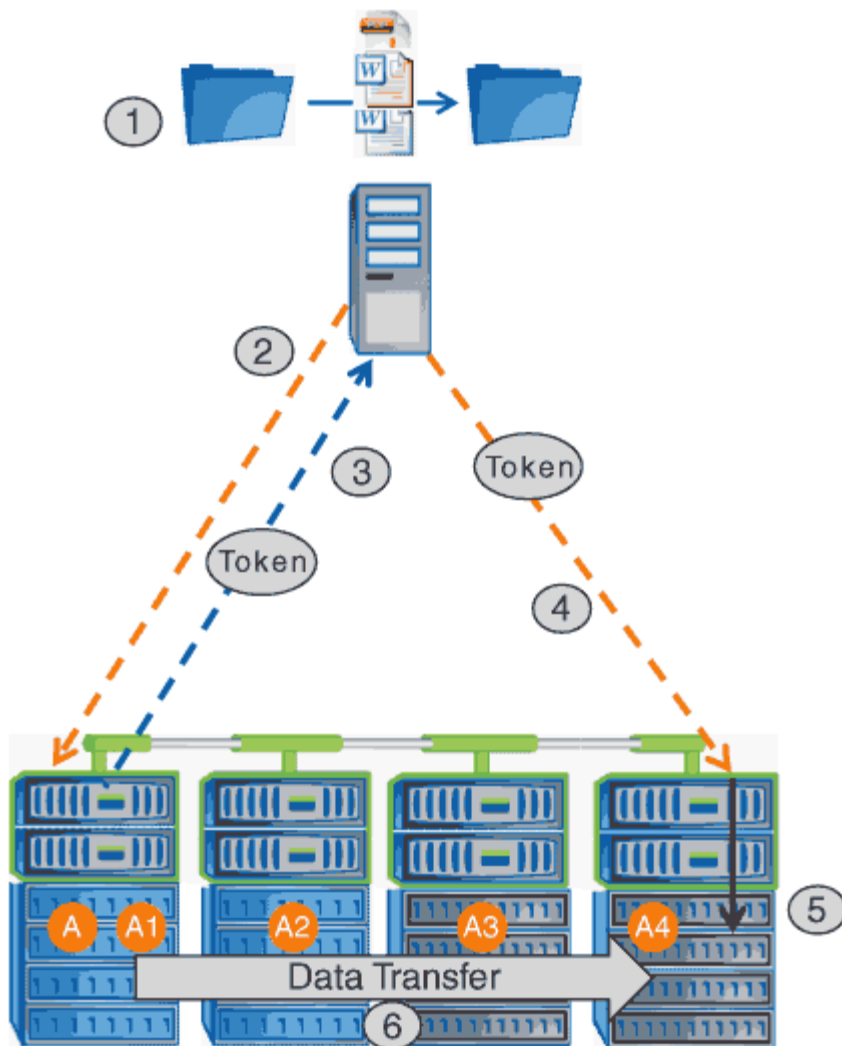


L'origine e la destinazione possono trovarsi sulla stessa SVM (Storage Virtual Machine) o su SVM diverse, a seconda dell'ambito dell'operazione di copia.

Il token funge da rappresentazione point-in-time dei dati. Ad esempio, quando si copiano i dati tra posizioni di storage, un token che rappresenta un segmento di dati viene restituito al client richiedente, che il client copia nella destinazione, eliminando così la necessità di copiare i dati sottostanti attraverso il client.

ONTAP supporta token che rappresentano 8 MB di dati. Le copie ODX superiori a 8 MB vengono eseguite utilizzando più token, ciascuno dei quali rappresenta 8 MB di dati.

La seguente figura illustra i passaggi relativi a un'operazione di copia ODX:



1. Un utente copia o sposta un file utilizzando Esplora risorse, un'interfaccia della riga di comando o come parte di una migrazione di macchine virtuali, oppure un'applicazione avvia copie o spostamenti di file.
2. Il client compatibile con ODX traduce automaticamente questa richiesta di trasferimento in una richiesta ODX.

La richiesta ODX inviata al server CIFS contiene una richiesta per un token.

3. Se ODX è attivato sul server CIFS e la connessione avviene tramite SMB 3.0, il server CIFS genera un token, che rappresenta una rappresentazione logica dei dati sull'origine.
4. Il client riceve un token che rappresenta i dati e li invia con la richiesta di scrittura al server CIFS di destinazione.

Si tratta degli unici dati copiati in rete dall'origine al client e quindi dal client alla destinazione.

5. Il token viene consegnato al sottosistema di storage.
6. La SVM esegue internamente la copia o lo spostamento.

Se il file che viene copiato o spostato è più grande di 8 MB, sono necessari più token per eseguire la copia. I passi da 2 a 6 vengono eseguiti in base alle necessità per completare la copia.



Se si verifica un errore con la copia ODX scaricata, l'operazione di copia o spostamento torna alle letture e scritture tradizionali per l'operazione di copia o spostamento. Allo stesso modo, se il server CIFS di destinazione non supporta ODX o ODX è disattivato, l'operazione di copia o spostamento ritorna alle operazioni di lettura e scrittura tradizionali per l'operazione di copia o spostamento.

### **Requisiti per l'utilizzo di ODX**

Prima di poter utilizzare ODX per gli offload delle copie con la vostra macchina virtuale di storage (SVM), dovete essere consapevoli di alcuni requisiti.

### **Requisiti di versione di ONTAP**

Le release di ONTAP supportano ODX per gli offload delle copie.

### **Requisiti di versione SMB**

- ONTAP supporta ODX con SMB 3.0 e versioni successive.
- SMB 3.0 deve essere abilitato sul server CIFS prima di poter abilitare ODX:
  - L'abilitazione di ODX abilita anche SMB 3.0, se non è già abilitato.
  - La disattivazione di SMB 3.0 disattiva anche ODX.

### **Requisiti di server e client Windows**

Prima di poter utilizzare ODX per gli offload delle copie, il client Windows deve supportare questa funzionalità.

Il "[Matrice di interoperabilità NetApp](#)" Contiene le informazioni più recenti sui client Windows supportati.

### **Requisiti di volume**

- I volumi di origine devono essere di almeno 1.25 GB.
- Se si utilizzano volumi compressi, il tipo di compressione deve essere adattivo e sono supportate solo le dimensioni del gruppo di compressione 8K.

Il tipo di compressione secondario non è supportato.

### **Linee guida per l'utilizzo di ODX**

Prima di poter utilizzare ODX per l'offload delle copie, è necessario conoscere le linee guida. Ad esempio, è necessario sapere quali tipi di volumi è possibile utilizzare ODX e comprendere le considerazioni relative a ODX all'interno del cluster e tra cluster.

### **Linee guida sui volumi**

- Non è possibile utilizzare ODX per l'offload delle copie con le seguenti configurazioni di volume:
  - Le dimensioni del volume di origine sono inferiori a 1.25 GB

Per utilizzare ODX, le dimensioni del volume devono essere pari o superiori a 1.25 GB.

- Volumi di sola lettura

ODX non viene utilizzato per file e cartelle residenti in mirror di condivisione del carico o in volumi di destinazione SnapMirror o SnapVault.

- Se il volume di origine non viene deduplicato
- Le copie ODX sono supportate solo per le copie all'interno del cluster.

Non è possibile utilizzare ODX per copiare file o cartelle in un volume in un altro cluster.

### Altre linee guida

- Negli ambienti SMB, per utilizzare ODX per l'offload delle copie, i file devono essere di 256 kb o superiore.

I file più piccoli vengono trasferiti utilizzando un'operazione di copia tradizionale.

- L'offload delle copie di ODX utilizza la deduplica come parte del processo di copia.

Se non si desidera che la deduplica avvenga sui volumi SVM durante la copia o lo spostamento dei dati, è necessario disattivare l'offload delle copie ODX su tale SVM.

- L'applicazione che esegue il trasferimento dei dati deve essere scritta per supportare ODX.

Le operazioni applicative che supportano ODX includono:

- Operazioni di gestione di Hyper-V, come la creazione e la conversione di dischi rigidi virtuali (VHD), la gestione di copie Snapshot e la copia di file tra macchine virtuali
- Operazioni di Esplora risorse
- Comandi di copia di Windows PowerShell
- Comandi di copia del prompt dei comandi di Windows

Robocopy al prompt dei comandi di Windows supporta ODX.



Le applicazioni devono essere in esecuzione su server o client Windows che supportano ODX.

+

Per ulteriori informazioni sulle applicazioni ODX supportate su server e client Windows, consultare la Microsoft TechNet Library.

### Informazioni correlate

"Microsoft TechNet Library: [technet.microsoft.com/en-us/library/](https://technet.microsoft.com/en-us/library/)"

### Casi di utilizzo per ODX

È necessario conoscere i casi di utilizzo per l'utilizzo di ODX su SVM in modo da poter determinare in quali circostanze ODX offre vantaggi in termini di performance.

I server e i client Windows che supportano ODX utilizzano l'offload delle copie come metodo predefinito per copiare i dati tra server remoti. Se il server o il client Windows non supporta ODX o l'offload delle copie ODX non riesce in qualsiasi momento, l'operazione di copia o spostamento ritorna alle tradizionali operazioni di lettura e scrittura per l'operazione di copia o spostamento.

I seguenti casi di utilizzo supportano l'utilizzo di copie e spostamenti ODX:

- Intra-volume

I file di origine e di destinazione o LUN si trovano all'interno dello stesso volume.

- Intervolume, stesso nodo, stessa SVM

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà della stessa SVM.

- Intervolume, nodi diversi, stessa SVM

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà della stessa SVM.

- Inter-SVM, stesso nodo

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà di diverse SVM.

- Inter-SVM, nodi diversi

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà di diverse SVM.

- Tra cluster

Le LUN di origine e di destinazione si trovano su volumi diversi che si trovano su nodi diversi tra cluster. Questo è supportato solo per SAN e non funziona per CIFS.

Esistono alcuni casi di utilizzo speciali aggiuntivi:

- Con l'implementazione di ONTAP ODX, è possibile utilizzare ODX per copiare i file tra le condivisioni SMB e le unità virtuali FC o iSCSI collegate.

È possibile utilizzare Esplora risorse, la CLI di Windows o PowerShell, Hyper-V o altre applicazioni che supportano ODX per copiare o spostare i file senza problemi utilizzando l'offload delle copie ODX tra le condivisioni SMB e le LUN connesse, a condizione che le condivisioni SMB e le LUN si trovino sullo stesso cluster.

- Hyper-V offre alcuni casi di utilizzo aggiuntivi per l'offload delle copie ODX:

- È possibile utilizzare il pass-through di offload delle copie ODX con Hyper-V per copiare i dati all'interno o tra file di dischi rigidi virtuali (VHD) o per copiare i dati tra le condivisioni SMB mappate e le LUN iSCSI connesse all'interno dello stesso cluster.

Ciò consente il passaggio delle copie dai sistemi operativi guest allo storage sottostante.

- Quando si creano VHD di dimensioni fisse, ODX viene utilizzato per inizializzare il disco con zero, utilizzando un token azzerato ben noto.
- L'offload delle copie ODX viene utilizzato per la migrazione dello storage delle macchine virtuali se lo storage di origine e di destinazione si trova sullo stesso cluster.



Per sfruttare i casi di utilizzo del pass-through di offload delle copie ODX con Hyper-V, il sistema operativo guest deve supportare ODX e i dischi del sistema operativo guest devono essere dischi SCSI supportati dallo storage (SMB o SAN) che supporti ODX. I dischi IDE sul sistema operativo guest non supportano il pass-through ODX.

#### Attivare o disattivare ODX

È possibile attivare o disattivare ODX su macchine virtuali storage (SVM). L'impostazione predefinita prevede l'attivazione del supporto per l'offload delle copie ODX se è attivato anche SMB 3.0.

#### Prima di iniziare

SMB 3.0 deve essere attivato.

#### A proposito di questa attività

Se si disattiva SMB 3.0, ONTAP disattiva anche SMB ODX. Se si riattiva SMB 3.0, è necessario riabilitare manualmente SMB ODX.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Eseguire una delle seguenti operazioni:

Se si desidera che l'offload delle copie ODX sia...	Immettere il comando...
Attivato	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -copy-offload-enabled false</code>

3. Tornare al livello di privilegio admin: `set -privilege admin`

#### Esempio

Il seguente esempio consente l'offload delle copie ODX su SVM vs1:



```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

## Informazioni correlate

[Opzioni server SMB disponibili](#)

## Migliora i tempi di risposta del client fornendo riferimenti automatici ai nodi SMB con Auto Location

**Migliora i tempi di risposta del client fornendo riferimenti automatici ai nodi SMB con panoramica della posizione automatica**

Auto Location utilizza i riferimenti automatici ai nodi SMB per aumentare le performance dei client SMB sulle macchine virtuali di storage (SVM). I riferimenti automatici ai nodi reindirizzano automaticamente il client richiedente a una LIF sul nodo SVM che ospita il volume in cui risiedono i dati, il che può portare a tempi di risposta del client migliorati.

Quando un client SMB si connette a una condivisione SMB ospitata sulla SVM, potrebbe connettersi utilizzando una LIF che si trova su un nodo che non possiede i dati richiesti. Il nodo a cui è connesso il client accede ai dati di proprietà di un altro nodo utilizzando la rete del cluster. Se la connessione SMB utilizza un LIF situato sul nodo contenente i dati richiesti, il client può ottenere tempi di risposta più rapidi:

- ONTAP fornisce questa funzionalità utilizzando i riferimenti DFS Microsoft per informare i client SMB che un file o una cartella richiesta nello spazio dei nomi è ospitato altrove.

Un nodo fa un riferimento quando determina che esiste una LIF SVM sul nodo contenente i dati.

- I riferimenti automatici dei nodi sono supportati per gli indirizzi IP LIF IPv4 e IPv6.
- I riferimenti vengono effettuati in base alla posizione della directory principale della condivisione attraverso la quale il client è connesso.
- Il riferimento si verifica durante la negoziazione SMB.

Il riferimento viene fatto prima che venga stabilita la connessione. Dopo che ONTAP fa riferimento al nodo di destinazione, la connessione viene stabilita e il client accede ai dati attraverso il percorso LIF indicato da quel punto in poi. In questo modo, i client possono accedere più rapidamente ai dati ed evitare ulteriori comunicazioni del cluster.



Se una condivisione si estende su più punti di giunzione e alcune delle giunzioni si riferiscono a volumi contenuti su altri nodi, i dati all'interno della condivisione vengono distribuiti su più nodi. Poiché ONTAP fornisce riferimenti locali alla directory principale della condivisione, ONTAP deve utilizzare la rete del cluster per recuperare i dati contenuti in questi volumi non locali. Con questo tipo di architettura dello spazio dei nomi, i riferimenti automatici ai nodi potrebbero non fornire benefici significativi in termini di performance.

Se il nodo che ospita i dati non dispone di una LIF disponibile, ONTAP stabilisce la connessione utilizzando la LIF scelta dal client. Dopo l'apertura di un file da parte di un client SMB, il file continua ad accedere attraverso la stessa connessione a cui si fa riferimento.

Se, per qualsiasi motivo, il server CIFS non è in grado di fare riferimento, il servizio SMB non viene disgiunto. La connessione SMB viene stabilita come se i riferimenti automatici al nodo non fossero abilitati.

### Informazioni correlate

[Miglioramento delle performance di copia remota di Microsoft](#)

### Requisiti e linee guida per l'utilizzo dei riferimenti automatici ai nodi

Prima di poter utilizzare i riferimenti automatici ai nodi SMB, noti anche come *autolocation*, è necessario conoscere alcuni requisiti, incluse le versioni di ONTAP che supportano la funzione. È inoltre necessario conoscere le versioni del protocollo SMB supportate e alcune altre linee guida speciali.

### Versione di ONTAP e requisiti di licenza

- Tutti i nodi del cluster devono eseguire una versione di ONTAP che supporti i riferimenti automatici dei nodi.
- Per utilizzare l'autolocation, i Widelink devono essere abilitati su una condivisione SMB.
- CIFS deve essere concesso in licenza e un server SMB deve esistere sulle SVM. La licenza SMB è inclusa con "ONTAP uno". Se non si dispone di ONTAP ONE e la licenza non è installata, contattare il rappresentante di vendita.

### Requisiti di versione del protocollo SMB

- Per le SVM, ONTAP supporta i riferimenti automatici dei nodi su tutte le versioni di SMB.

### Requisiti del client SMB

Tutti i client Microsoft supportati da ONTAP supportano i riferimenti automatici dei nodi SMB.

La matrice di interoperabilità contiene le informazioni più recenti sui client Windows supportati da ONTAP.

["Tool di matrice di interoperabilità NetApp"](#)

### Requisiti Data LIF

Se si desidera utilizzare una LIF di dati come potenziale riferimento per i client SMB, è necessario creare LIF di dati con NFS e CIFS abilitati.

I riferimenti automatici dei nodi possono non funzionare se il nodo di destinazione contiene LIF di dati che sono abilitati solo per il protocollo NFS o abilitati solo per il protocollo SMB.

Se questo requisito non viene soddisfatto, l'accesso ai dati non viene compromesso. Il client SMB esegue la mappatura della condivisione utilizzando la LIF originale utilizzata dal client per connettersi alla SVM.

### Requisiti di autenticazione NTLM quando si effettua una connessione SMB di riferimento

L'autenticazione NTLM deve essere consentita nel dominio contenente il server CIFS e nei domini contenenti client che desiderano utilizzare i riferimenti automatici ai nodi.

Quando si fa un riferimento, il server SMB fa riferimento a un indirizzo IP per il client Windows. Poiché l'autenticazione NTLM viene utilizzata quando si effettua una connessione utilizzando un indirizzo IP, l'autenticazione Kerberos non viene eseguita per le connessioni di riferimento.

Questo accade perché il client Windows non può creare il nome principale del servizio utilizzato da Kerberos (che è del formato `service/NetBIOS name` e. `service/FQDN`), il che significa che il client non può richiedere un ticket Kerberos al servizio.

### **Linee guida per l'utilizzo dei riferimenti automatici ai nodi con la funzione home directory**

Quando le condivisioni sono configurate con la proprietà di condivisione della home directory attivata, possono essere configurati uno o più percorsi di ricerca della home directory per una configurazione della home directory. I percorsi di ricerca possono puntare ai volumi contenuti in ciascun nodo contenente volumi SVM. I client ricevono un riferimento e, se è disponibile un LIF di dati locale attivo, si connettono attraverso un LIF di riferimento locale alla home directory dell'utente domestico.

Esistono linee guida quando i client SMB 1.0 accedono alle home directory dinamiche con i riferimenti automatici dei nodi abilitati. Questo perché i client SMB 1.0 richiedono il riferimento automatico al nodo prima dell'autenticazione, ovvero prima che il server SMB abbia il nome dell'utente. Tuttavia, l'accesso alla home directory SMB funziona correttamente per i client SMB 1.0 se le seguenti affermazioni sono vere:

- Le home directory SMB sono configurate in modo da utilizzare nomi semplici, come “%w” (nome utente Windows) o “%u” (nome utente UNIX mappato) e non nomi di stile dominio, come “%d%w” (nome-dominio nome-utente).
- Quando si creano condivisioni della home directory, i nomi delle condivisioni della home directory CIFS vengono configurati con variabili (“%w” o “%u”) e non con nomi statici, ad esempio “HOME”.

Per i client SMB 2.x e SMB 3.0, non esistono linee guida speciali per l'accesso alle home directory mediante riferimenti automatici ai nodi.

### **Linee guida per la disattivazione dei riferimenti automatici dei nodi sui server CIFS con connessioni referenziate esistenti**

Se si disattivano i riferimenti automatici ai nodi dopo l'attivazione dell'opzione, i client attualmente connessi a una LIF referenziata mantengono la connessione referenziata. Poiché ONTAP utilizza i riferimenti DFS come meccanismo per i riferimenti automatici ai nodi SMB, i client possono anche riconnettersi al file LIF indicato dopo aver disattivato l'opzione fino al timeout del riferimento DFS memorizzato nella cache del client per la connessione a cui si fa riferimento. Ciò vale anche nel caso di un ripristino di una versione di ONTAP che non supporta i riferimenti automatici ai nodi. I client continuano a utilizzare i riferimenti fino a quando il riferimento DFS non passa in timeout dalla cache del client.

L'autolocation utilizza i riferimenti automatici ai nodi SMB per aumentare le performance dei client SMB facendo riferimento ai client alla LIF sul nodo proprietario del volume di dati di una SVM. Quando un client SMB si connette a una condivisione SMB ospitata su una SVM, potrebbe connettersi utilizzando una LIF su un nodo che non possiede i dati richiesti e utilizza una rete di interconnessione cluster per recuperare i dati. Se la connessione SMB utilizza un LIF situato sul nodo contenente i dati richiesti, il client può ottenere tempi di risposta più rapidi.

ONTAP fornisce questa funzionalità utilizzando i riferimenti del file system distribuito Microsoft (DFS) per informare i client SMB che un file o una cartella richiesti nello spazio dei nomi è ospitato altrove. Un nodo fa un riferimento quando determina la presenza di una LIF SVM sul nodo contenente i dati. I riferimenti vengono effettuati in base alla posizione della directory principale della condivisione attraverso la quale il client è connesso.

Il riferimento si verifica durante la negoziazione SMB. Il riferimento viene fatto prima che venga stabilita la connessione. Dopo che ONTAP fa riferimento al nodo di destinazione, la connessione viene stabilita e il client accede ai dati attraverso il percorso LIF indicato da quel punto in poi. In questo modo, i client possono accedere più rapidamente ai dati ed evitare ulteriori comunicazioni del cluster.

## **Linee guida per l'utilizzo dei riferimenti automatici dei nodi con client Mac OS**

I client Mac OS X non supportano i riferimenti automatici ai nodi SMB, anche se Mac OS supporta il file system distribuito (DFS) di Microsoft. I client Windows effettuano una richiesta di riferimento DFS prima di connettersi a una condivisione SMB. ONTAP fornisce un riferimento a una LIF di dati trovata sullo stesso nodo che ospita i dati richiesti, il che porta a tempi di risposta del client migliorati. Anche se Mac OS supporta DFS, i client Mac OS non si comportano esattamente come i client Windows in quest'area.

### **Informazioni correlate**

[In che modo ONTAP abilita le home directory dinamiche](#)

["Gestione della rete"](#)

["Tool di matrice di interoperabilità NetApp"](#)

### **Supporto per i riferimenti automatici ai nodi SMB**

Prima di attivare i riferimenti automatici ai nodi SMB, è necessario tenere presente che alcune funzionalità di ONTAP non supportano i riferimenti.

- I seguenti tipi di volumi non supportano i riferimenti automatici ai nodi SMB:
  - Membri di sola lettura di un mirror di condivisione del carico
  - Volume di destinazione di un mirror per la protezione dei dati
- I riferimenti ai nodi non si spostano insieme a uno spostamento LIF.

Se un client utilizza una connessione di riferimento su una connessione SMB 2.x o SMB 3.0 e una LIF dati si sposta senza interruzioni, il client continua a utilizzare la stessa connessione di riferimento, anche se la LIF non è più locale rispetto ai dati.

- I riferimenti ai nodi non si spostano insieme a uno spostamento del volume.

Se un client utilizza una connessione di riferimento su qualsiasi connessione SMB e si verifica uno spostamento del volume, il client continua a utilizzare la stessa connessione di riferimento, anche se il volume non si trova più sullo stesso nodo del LIF dei dati.

### **Attiva o disattiva i riferimenti automatici ai nodi SMB**

È possibile abilitare i riferimenti automatici ai nodi SMB per aumentare le performance di accesso al client SMB. È possibile disattivare i riferimenti automatici dei nodi se non si desidera che ONTAP faccia riferimento ai client SMB.

### **Prima di iniziare**

Un server CIFS deve essere configurato e in esecuzione sulla macchina virtuale di storage (SVM).

### **A proposito di questa attività**

Per impostazione predefinita, la funzionalità SMB automatic node referrals (riferimenti automatici al nodo SMB) è disattivata. È possibile attivare o disattivare questa funzionalità su ogni SVM in base alle esigenze.

Questa opzione è disponibile al livello di privilegio avanzato.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Attivare o disattivare i riferimenti automatici ai nodi SMB secondo necessità:

Se si desidera che i riferimenti automatici ai nodi SMB siano...	Immettere il seguente comando...
Attivato	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -is-referral-enabled false</code>

L'impostazione dell'opzione ha effetto per le nuove sessioni SMB. I client con connessione esistente possono utilizzare il riferimento al nodo solo quando scade il timeout della cache esistente.

3. Passare al livello di privilegio admin: `set -privilege admin`

## Informazioni correlate

[Opzioni server SMB disponibili](#)

### Utilizza le statistiche per monitorare l'attività di riferimento automatico del nodo

Per determinare il numero di connessioni SMB a cui si fa riferimento, è possibile monitorare l'attività di riferimento automatico del nodo utilizzando `statistics` comando. Monitorando i riferimenti è possibile determinare in che misura i riferimenti automatici individuano le connessioni sui nodi che ospitano le condivisioni e se è necessario ridistribuire i file LIF dei dati per fornire un migliore accesso locale alle condivisioni sul server CIFS.

### A proposito di questa attività

Il `cifs` Object fornisce diversi contatori a livello di privilegio avanzato che sono utili per il monitoraggio dei riferimenti automatici ai nodi SMB:

- `node_referral_issued`

Numero di client che hanno ricevuto un riferimento al nodo della directory principale di condivisione dopo che il client si è connesso utilizzando una LIF ospitata da un nodo diverso dal nodo della directory principale di condivisione.

- `node_referral_local`

Numero di client connessi utilizzando una LIF ospitata dallo stesso nodo che ospita la directory principale di condivisione. L'accesso locale offre generalmente performance ottimali.

- `node_referral_not_possible`

Numero di client che non hanno ricevuto un riferimento al nodo che ospita la directory principale di condivisione dopo la connessione utilizzando una LIF ospitata da un nodo diverso dal nodo della directory principale di condivisione. Questo perché non è stato trovato un LIF di dati attivo per il nodo della directory principale di condivisione.

- `node_referral_remote`

Numero di client connessi utilizzando una LIF ospitata da un nodo diverso dal nodo che ospita la directory principale di condivisione. L'accesso remoto potrebbe causare un peggioramento delle performance.

È possibile monitorare le statistiche di riferimento dei nodi automatici sulla macchina virtuale di storage (SVM) raccogliendo e visualizzando i dati per un periodo di tempo specifico (un esempio). Se non si interrompe la raccolta dei dati, è possibile visualizzare i dati del campione. L'interruzione della raccolta dei dati fornisce un campione fisso. La mancata interruzione della raccolta dei dati consente di ottenere dati aggiornati da utilizzare per il confronto con le query precedenti. Il confronto può aiutarti a identificare le tendenze delle performance.



Per valutare e utilizzare le informazioni raccolte da `statistics` è necessario conoscere la distribuzione dei client nei propri ambienti.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`
2. Visualizzare le statistiche di riferimento dei nodi automatici utilizzando `statistics` comando.

Questo esempio visualizza le statistiche di riferimento dei nodi automatici raccogliendo e visualizzando i dati per un periodo di tempo campionato:

- a. Avviare la raccolta: `statistics start -object cifs -instance vs1 -sample-id sample1`

```
Statistics collection is being started for Sample-id: sample1
```

- b. Attendere il tempo di raccolta desiderato.
- c. Interrompere la raccolta: `statistics stop -sample-id sample1`

```
Statistics collection is being stopped for Sample-id: sample1
```

- d. Visualizzare le statistiche di riferimento dei nodi automatici: `statistics show -sample-id sample1 -counter node`

```
Object: cifs
Instance: vs1
Start-time: 2/4/2013 19:27:02
End-time: 2/4/2013 19:30:11
Cluster: cluster1
```

Counter	Value
node_name	node1
node_referral_issued	0
node_referral_local	1
node_referral_not_possible	2
node_referral_remote	2
...	
node_name	node2
node_referral_issued	2
node_referral_local	1
node_referral_not_possible	0
node_referral_remote	2
...	

L'output visualizza i contatori di tutti i nodi che partecipano a SVM vs1. Per maggiore chiarezza, nell'esempio vengono forniti solo i campi di output relativi alle statistiche di riferimento dei nodi automatici.

3. Tornare al livello di privilegio admin: `set -privilege admin`

### Informazioni correlate

[Visualizzazione delle statistiche](#)

["Configurazione del monitoraggio delle performance"](#)

### Monitorare le informazioni di riferimento del nodo automatico SMB lato client utilizzando un client Windows

Per determinare quali riferimenti vengono fatti dal punto di vista del client, è possibile utilizzare Windows `dfsutil.exe` utility.

Il kit Remote Server Administration Tools (RSAT) disponibile con Windows 7 e i client successivi contiene `dfsutil.exe` utility. Utilizzando questa utility, è possibile visualizzare informazioni sul contenuto della cache di riferimento e le informazioni relative a ciascun riferimento attualmente utilizzato dal client. È inoltre possibile utilizzare l'utility per cancellare la cache di riferimento del client. Per ulteriori informazioni, consultare la Microsoft TechNet Library.

### Informazioni correlate

["Microsoft TechNet Library: technet.microsoft.com/en-us/library/"](http://technet.microsoft.com/en-us/library/)

## Sicurezza delle cartelle sulle condivisioni con enumerazione basata sull'accesso

Fornire la sicurezza delle cartelle sulle condivisioni con una panoramica dell'enumerazione basata sull'accesso

Quando l'enumerazione basata sull'accesso (ABE) è attivata su una condivisione SMB, gli utenti che non dispongono dell'autorizzazione per accedere a una cartella o a un file contenuto nella condivisione (tramite restrizioni di autorizzazione individuali o di gruppo) non vedono la risorsa condivisa visualizzata nel proprio ambiente, anche se la condivisione stessa rimane visibile.

Le proprietà di condivisione convenzionali consentono di specificare quali utenti (individualmente o in gruppi) dispongono dell'autorizzazione per visualizzare o modificare file o cartelle contenuti nella condivisione. Tuttavia, non consentono di controllare se le cartelle o i file all'interno della condivisione sono visibili agli utenti che non dispongono dell'autorizzazione per accedervi. Ciò potrebbe causare problemi se i nomi di queste cartelle o file all'interno della condivisione descrivono informazioni riservate, come i nomi dei clienti o dei prodotti in fase di sviluppo.

L'enumerazione basata sull'accesso (ABE) estende le proprietà di condivisione per includere l'enumerazione di file e cartelle all'interno della condivisione. ABE consente quindi di filtrare la visualizzazione di file e cartelle all'interno della condivisione in base ai diritti di accesso dell'utente. In altre termini, la condivisione stessa sarebbe visibile a tutti gli utenti, ma i file e le cartelle all'interno della condivisione potrebbero essere visualizzati o nascosti agli utenti designati. Oltre a proteggere le informazioni sensibili sul luogo di lavoro, ABE consente di semplificare la visualizzazione di grandi strutture di directory a beneficio degli utenti che non hanno bisogno di accedere all'intera gamma di contenuti. Ad esempio, la condivisione stessa sarebbe visibile a tutti gli utenti, ma i file e le cartelle all'interno della condivisione potrebbero essere visualizzati o nascosti.

Scopri di più ["Impatto delle performance quando si utilizza l'enumerazione SMB/CIFS Access Based Enumeration"](#).

### Abilitare o disabilitare l'enumerazione basata sull'accesso sulle condivisioni SMB

È possibile attivare o disattivare l'enumerazione basata sull'accesso (ABE) sulle condivisioni SMB per consentire o impedire agli utenti di visualizzare le risorse condivise a cui non dispongono dell'autorizzazione di accesso.

#### A proposito di questa attività

Per impostazione predefinita, ABE è disattivato.

#### Fasi

1. Eseguire una delle seguenti operazioni:



Se si desidera...	Immettere il comando...
Abilitare ABE su una nuova condivisione	<code>vserver cifs share create -vserver vserver_name -share-name share_name -path path -share-properties access-based-enumeration</code> Quando si crea una condivisione SMB, è possibile specificare ulteriori impostazioni di condivisione opzionali e proprietà di condivisione aggiuntive. Per ulteriori informazioni, vedere la pagina man di <code>vserver cifs share create</code> comando.
Abilitare ABE su una condivisione esistente	<code>vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> Le proprietà di condivisione esistenti vengono conservate. La proprietà di condivisione ABE viene aggiunta all'elenco esistente di proprietà di condivisione.
Disattiva ABE su una condivisione esistente	<code>vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration</code> Le altre proprietà di condivisione vengono conservate. Solo la proprietà di condivisione ABE viene rimossa dall'elenco delle proprietà di condivisione.

2. Verificare che la configurazione della condivisione sia corretta utilizzando `vserver cifs share show` comando.

### Esempi

Nell'esempio seguente viene creata una condivisione SMB ABE denominata "sales" con un percorso di /sales Su SVM vs1. La condivisione viene creata con `access-based-enumeration` come proprietà condivisa:

```

cluster1::> vsserver cifs share create -vsriver vs1 -share-name sales -path
/sales -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vsserver cifs share show -vsriver vs1 -share-name sales

          Vserver: vs1
          Share: sales
CIFS Server NetBIOS Name: VS1
          Path: /sales
      Share Properties: access-based-enumeration
                        oplocks
                        browsable
                        changenotify
      Symlink Properties: enable
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
          Share Comment: -
          Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
          Volume Name: -
          Offline Files: manual
Vscan File-Operations Profile: standard

```

Nell'esempio riportato di seguito viene aggiunto il access-based-enumeration Condividere la proprietà su una condivisione SMB denominata "data2":

```

cluster1::> vsserver cifs share properties add -vsriver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vsserver cifs share show -vsriver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
-----
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration

```

## Informazioni correlate

[Aggiunta o rimozione delle proprietà di condivisione su una condivisione SMB esistente](#)

**Abilitare o disabilitare l'enumerazione basata sull'accesso da un client Windows**

È possibile attivare o disattivare l'enumerazione basata sull'accesso (ABE) sulle condivisioni SMB da un client Windows, che consente di configurare questa impostazione di condivisione senza la necessità di connettersi al server CIFS.



Il `abecmd` L'utility non è disponibile nelle nuove versioni dei client Windows Server e Windows. È stato rilasciato come parte di Windows Server 2008. Il supporto per Windows Server 2008 è terminato il 14 gennaio 2020.

## Fasi

1. Da un client Windows che supporta ABE, immettere il seguente comando: `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

Per ulteriori informazioni su `abecmd` Consultare la documentazione del client Windows.

## Dipendenze di nomi di file e directory NFS e SMB

### Panoramica delle dipendenze di nomi di file e directory NFS e SMB

Le convenzioni di denominazione di file e directory dipendono dai sistemi operativi dei client di rete e dai protocolli di condivisione file, oltre alle impostazioni della lingua del cluster e dei client ONTAP.

Il sistema operativo e i protocolli di condivisione file determinano quanto segue:

- Caratteri che possono essere utilizzati da un nome file
- Distinzione tra maiuscole e minuscole per un nome file

ONTAP supporta caratteri multi-byte nei nomi di file, directory e qtree, a seconda della versione di ONTAP.

### Caratteri che possono essere utilizzati da un nome di file o di directory

Se si accede a un file o a una directory da client con sistemi operativi diversi, utilizzare caratteri validi in entrambi i sistemi operativi.

Ad esempio, se si utilizza UNIX per creare un file o una directory, non utilizzare i due punti (:) nel nome perché i due punti non sono consentiti nei nomi di file o directory MS-DOS. Poiché le restrizioni sui caratteri validi variano da un sistema operativo all'altro, consultare la documentazione del sistema operativo client per ulteriori informazioni sui caratteri non consentiti.

### Distinzione tra maiuscole e minuscole dei nomi di file e directory in un ambiente multiprotocollo

I nomi di file e directory sono sensibili al maiuscolo/minuscolo per i client NFS e non al maiuscolo/minuscolo ma conservano il maiuscolo/minuscolo per i client SMB. È necessario comprendere le implicazioni di un ambiente multiprotocollo e le azioni da intraprendere quando si specifica il percorso durante la creazione di condivisioni SMB e quando si accede ai dati all'interno delle condivisioni.

Se un client SMB crea una directory denominata `testdir`, Sia i client SMB che NFS visualizzano il nome del file come `testdir`. Tuttavia, se un utente SMB tenta in seguito di creare un nome di directory `TESTDIR`, il nome non è consentito perché, per il client SMB, tale nome esiste attualmente. Se un utente NFS successivamente crea una directory denominata `TESTDIR` il client , NFS e SMB visualizzano il nome della directory in modo diverso, come segue:

- Sui client NFS, ad esempio, vengono visualizzati entrambi i nomi di directory così come sono stati creati

`testdir` e `TESTDIR`, perché i nomi delle directory sono sensibili al maiuscolo/minuscolo.

- I client SMB utilizzano i nomi 8.3 per distinguere le due directory. Una directory ha il nome del file di base. Alle directory aggiuntive viene assegnato un nome file 8.3.
  - Sui client SMB, viene visualizzato `testdir` e `TESTDI~1`.
  - ONTAP crea il `TESTDI~1` nome della directory per differenziare le due directory.

In questo caso, è necessario utilizzare il nome 8.3 quando si specifica un percorso di condivisione durante la creazione o la modifica di una condivisione su una macchina virtuale di storage (SVM).

Analogamente per i file, se viene creato un client SMB `test.txt`, Sia i client SMB che NFS visualizzano il nome del file come `test.txt`. Tuttavia, se un utente SMB tenta di creare in un secondo momento `Test.txt`, Il nome non è consentito perché, per il client SMB, tale nome esiste attualmente. Se un utente NFS successivamente crea un file denominato `Test.txt` I client , NFS e SMB visualizzano il nome del file in modo diverso, come segue:

- Sui client NFS, vengono visualizzati entrambi i nomi dei file così come sono stati creati, `test.txt` e `Test.txt`, perché i nomi dei file sono sensibili al maiuscolo/minuscolo.
- I client SMB utilizzano i nomi 8.3 per distinguere i due file. Un file ha il nome del file di base. Ai file aggiuntivi viene assegnato un nome file 8.3.
  - Sui client SMB, viene visualizzato `test.txt` e `TEST~1.TXT`.
  - ONTAP crea il `TEST~1.TXT` nome del file per differenziare i due file.



Se è stata attivata o modificata la mappatura dei caratteri utilizzando i comandi di mappatura dei caratteri CIFS di Vserver, una ricerca di Windows normalmente non sensibile al maiuscolo/minuscolo diventa sensibile al maiuscolo/minuscolo.

## Come ONTAP crea i nomi di file e directory

ONTAP crea e mantiene due nomi per i file o le directory in qualsiasi directory che ha accesso da un client SMB: Il nome lungo originale e un nome in formato 8.3.

Per i nomi di file o directory che superano il nome di otto caratteri o il limite di estensione di tre caratteri (per i file), ONTAP genera un nome in formato 8.3 come segue:

- Il nome del file o della directory originale viene troncato a sei caratteri, se il nome supera i sei caratteri.
- Aggiunge una tilde (~) e un numero, da uno a cinque, ai nomi di file o directory che non sono più univoci dopo essere stati troncati.

Se esaurisce i numeri perché ci sono più di cinque nomi simili, crea un nome unico che non ha alcuna relazione con il nome originale.

- Nel caso dei file, l'estensione del nome del file viene troncata a tre caratteri.

Ad esempio, se un client NFS crea un file denominato `specifications.html`, Il nome del file di formato 8.3 creato da ONTAP è `specif~1.htm`. Se questo nome esiste già, ONTAP utilizza un numero diverso alla fine del nome del file. Ad esempio, se un client NFS crea un altro file denominato `specifications_new.html`, il formato 8.3 di `specifications_new.html` è `specif~2.htm`.

## Come ONTAP gestisce i nomi di file, directory e qtree multi-byte

A partire da ONTAP 9.5, il supporto per i nomi codificati UTF-8 a 4 byte consente la creazione e la visualizzazione di nomi di file, directory e albero che includono caratteri aggiuntivi Unicode al di fuori del piano multilingua di base (BMP). Nelle versioni precedenti, questi caratteri supplementari non erano visualizzati correttamente negli ambienti multiprotocollo.

Per abilitare il supporto per i nomi codificati UTF-8 a 4 byte, è disponibile un nuovo codice lingua *utf8mb4* per *vserver* e. volume famiglie di comandi.

È necessario creare un nuovo volume in uno dei seguenti modi:

- Impostazione del volume `-language` opzione esplicitamente: `volume create -language utf8mb4 {...}`
- Ereditare il volume `-language` Opzione da una SVM creata con o modificata per l'opzione: `vserver [create|modify] -language utf8mb4 {...}``volume create {...}`
- In ONTAP 9,6 e versioni precedenti, non è possibile modificare i volumi esistenti per il supporto di *utf8mb4*; è necessario creare un nuovo volume pronto per *utf8mb4* e quindi migrare i dati utilizzando strumenti di copia basati su client.

È possibile aggiornare le SVM per il supporto di *utf8mb4*, ma i volumi esistenti conservano i codici lingua originali.

Se si utilizza ONTAP 9.7P1 o versione successiva, è possibile modificare i volumi esistenti per *utf8mb4* con una richiesta di supporto. Per ulteriori informazioni, vedere ["È possibile modificare la lingua del volume dopo la creazione in ONTAP?"](#).

- A partire da ONTAP 9,8, è possibile utilizzare `[-language <Language code>]` Parametro per modificare la lingua del volume da \*.UTF-8 a *utf8mb4*. Per modificare la lingua di un volume, contattare ["Supporto NetApp"](#).



I nomi LUN con caratteri UTF-8 a 4 byte non sono attualmente supportati.

- I dati dei caratteri Unicode sono generalmente rappresentati nelle applicazioni di file system Windows che utilizzano il formato di trasformazione Unicode a 16 bit (UTF-16) e nei file system NFS che utilizzano il formato di trasformazione Unicode a 8 bit (UTF-8).

Nelle release precedenti a ONTAP 9.5, i nomi, inclusi i caratteri supplementari UTF-16 creati dai client Windows, venivano visualizzati correttamente su altri client Windows ma non sono stati tradotti correttamente in UTF-8 per i client NFS. Analogamente, i nomi con caratteri supplementari UTF-8 creati dai client NFS non sono stati tradotti correttamente in UTF-16 per i client Windows.

- Quando si creano nomi di file su sistemi con ONTAP 9.4 o versioni precedenti che contengono caratteri supplementari validi o non validi, ONTAP rifiuta il nome del file e restituisce un errore di nome del file non valido.

Per evitare questo problema, utilizzare solo caratteri BMP nei nomi dei file ed evitare di utilizzare caratteri supplementari oppure eseguire l'aggiornamento a ONTAP 9.5 o versioni successive.

A partire da ONTAP 9, i caratteri Unicode sono consentiti nei nomi qtree.

- È possibile utilizzare il `volume qtree` Command Family o System Manager per impostare o modificare i nomi di qtree.
- I nomi qtree possono includere caratteri multi-byte in formato Unicode, ad esempio caratteri giapponesi e cinesi.
- Nelle versioni precedenti a ONTAP 9.5, erano supportati solo i caratteri BMP (ovvero quelli che potevano essere rappresentati in 3 byte).



Nelle release precedenti a ONTAP 9.5, il percorso di giunzione del volume padre del qtree può contenere nomi di qtree e directory con caratteri Unicode. Il `volume show` Il comando visualizza correttamente questi nomi quando il volume d'origine dispone di un'impostazione della lingua UTF-8. Tuttavia, se la lingua del volume padre non è una delle impostazioni della lingua UTF-8, alcune parti del percorso di giunzione vengono visualizzate utilizzando un nome alternativo NFS numerico.

- Nella versione 9.5 e successive, i caratteri a 4 byte sono supportati nei nomi qtree, a condizione che il qtree si trovi in un volume abilitato per `utf8mb4`.

## Configurare la mappatura dei caratteri per la conversione dei nomi file SMB sui volumi

I client NFS possono creare nomi di file che contengono caratteri non validi per i client SMB e alcune applicazioni Windows. È possibile configurare la mappatura dei caratteri per la conversione dei nomi file sui volumi per consentire ai client SMB di accedere ai file con nomi NFS che altrimenti non sarebbero validi.

### A proposito di questa attività

Quando i client SMB accedono ai file creati dai client NFS, ONTAP esamina il nome del file. Se il nome non è un nome file SMB valido (ad esempio, se ha un carattere ":" incorporato), ONTAP restituisce il nome file 8.3 che viene mantenuto per ciascun file. Tuttavia, questo causa problemi per le applicazioni che codificano informazioni importanti in nomi di file lunghi.

Pertanto, se si condivide un file tra client su sistemi operativi diversi, è necessario utilizzare caratteri nei nomi dei file validi in entrambi i sistemi operativi.

Tuttavia, se si dispone di client NFS che creano nomi file contenenti caratteri non validi per i client SMB, è possibile definire una mappa che converte i caratteri NFS non validi in caratteri Unicode accettati sia da SMB che da alcune applicazioni Windows. Ad esempio, questa funzionalità supporta le applicazioni CATIA MCAD e Mathematica e altre applicazioni che richiedono questo requisito.

È possibile configurare la mappatura dei caratteri volume per volume.

Quando si configura la mappatura dei caratteri su un volume, è necessario tenere presente quanto segue:

- La mappatura dei caratteri non viene applicata tra i punti di giunzione.

È necessario configurare esplicitamente la mappatura dei caratteri per ciascun volume di giunzione.

- È necessario assicurarsi che i caratteri Unicode utilizzati per rappresentare caratteri non validi o non validi siano caratteri che normalmente non vengono visualizzati nei nomi dei file; in caso contrario, si verificano mappature indesiderate.

Ad esempio, se si tenta di mappare i due punti (:) a un trattino (-) ma il trattino (-) è stato utilizzato correttamente nel nome del file, un client Windows che tenta di accedere a un file denominato "a-b"

avrebbe la sua richiesta mappata al nome NFS "a:b" (non il risultato desiderato).

- Dopo aver applicato la mappatura dei caratteri, se la mappatura contiene ancora un carattere Windows non valido, ONTAP torna ai nomi file di Windows 8.3.
- Nelle notifiche FPolicy, nei registri di controllo NAS e nei messaggi di traccia di sicurezza, vengono visualizzati i nomi dei file mappati.
- Quando viene creata una relazione SnapMirror di tipo DP, la mappatura dei caratteri del volume di origine non viene replicata sul volume DP di destinazione.
- Distinzione tra maiuscole e minuscole: Poiché i nomi Windows mappati diventano nomi NFS, la ricerca dei nomi segue la semantica NFS. Ciò include il fatto che le ricerche NFS sono sensibili al maiuscolo/minuscolo. Ciò significa che le applicazioni che accedono alle condivisioni mappate non devono fare affidamento sul comportamento di Windows senza distinzione tra maiuscole e minuscole. Tuttavia, il nome 8.3 è disponibile, senza distinzione tra maiuscole e minuscole.
- Mappature parziali o non valide: Dopo aver mappato un nome da restituire ai client che eseguono l'enumerazione della directory ("dir"), il nome Unicode risultante viene controllato per la validità di Windows. Se il nome contiene ancora caratteri non validi o se non è valido per Windows (ad esempio, termina con "." o vuoto) viene restituito il nome 8.3 invece del nome non valido.

## Fase

1. Configurare la mappatura dei caratteri: +

```
vserver cifs character-mapping create -vserver vserver_name -volume volume_name  
-mapping mapping_text, ... +
```

Il mapping è costituito da un elenco di coppie di caratteri origine-destinazione separate da ":". I caratteri sono caratteri Unicode immessi utilizzando cifre esadecimali. Ad esempio: 3C:E03C. +

Il primo valore di ciascuno `mapping_text` La coppia separata dai due punti è il valore esadecimale del carattere NFS che si desidera convertire, mentre il secondo valore è il valore Unicode utilizzato da SMB. Le coppie di mappatura devono essere univoche (deve esistere una mappatura uno a uno).

- Mappatura di origine +

La tabella seguente mostra il set di caratteri Unicode consentito per il mapping di origine:

+

Carattere Unicode	Carattere stampato	Descrizione
0x01-0x19	Non applicabile	Caratteri di controllo non stampabili
0x5C		Barra rovesciata
0x3A	:	Due punti
0x2A	*	Asterisco
0x3F	?	Punto interrogativo
0x22	"	Virgoletta

Carattere Unicode	Carattere stampato	Descrizione
0x3C	<	Inferiore a.
0x3E	>	Maggiore di
0x7C		
Linea verticale	0xB1	±

- Mappatura di destinazione

È possibile specificare i caratteri di destinazione nella “Private Use Area” di Unicode nel seguente intervallo: U+E0000...U+F8FF.

### Esempio

Il seguente comando crea un mapping di caratteri per un volume denominato “data” su storage virtual machine (SVM) vs1:

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show
```

Vserver	Volume Name	Character Mapping
vs1	data	3c:e17c, 3e:f17d, 2a:f745

### Informazioni correlate

[Creazione e gestione di volumi di dati negli spazi dei nomi NAS](#)

### Comandi per la gestione delle mappature dei caratteri per la conversione dei nomi file SMB

È possibile gestire la mappatura dei caratteri creando, modificando, visualizzando o eliminando le mappature dei caratteri dei file utilizzate per la conversione dei nomi dei file SMB sui volumi FlexVol.

Se si desidera...	Utilizzare questo comando...
Creare nuove mappature dei caratteri del file	<code>vserver cifs character-mapping create</code>
Visualizza le informazioni sulle mappature dei caratteri del file	<code>vserver cifs character-mapping show</code>
Modificare le mappature dei caratteri del file esistente	<code>vserver cifs character-mapping modify</code>



Se si desidera...	Utilizzare questo comando...
Eliminare le mappature dei caratteri del file	<code>vserver cifs character-mapping delete</code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

#### Informazioni correlate

[Configurazione della mappatura dei caratteri per la conversione dei nomi file SMB sui volumi](#)

## Fornire l'accesso del client S3 ai dati NAS

### Panoramica sul multiprotocollo S3

A partire da ONTAP 9.12.1, è possibile consentire ai client che eseguono il protocollo S3 di accedere agli stessi dati forniti ai client che utilizzano i protocolli NFS e SMB senza riformattare. Questa funzionalità consente ai dati NAS di continuare a essere serviti ai client NAS, presentando al contempo i dati a oggetti ai client S3 che eseguono applicazioni S3 (come data mining e intelligenza artificiale).

La funzionalità multiprotocollo S3 consente di gestire due casi di utilizzo:

#### 1. Accesso ai dati NAS esistenti mediante client S3

Se i dati esistenti sono stati creati utilizzando client NAS tradizionali (NFS o SMB) e si trovano su volumi NAS (volumi FlexVol o FlexGroup), è ora possibile utilizzare strumenti analitici sui client S3 per accedere a questi dati.

#### 2. Storage back-end per client moderni in grado di eseguire i/o utilizzando protocolli NAS e S3

È ora possibile fornire un accesso integrato ad applicazioni come Spark e Kafka in grado di leggere e scrivere gli stessi dati utilizzando i protocolli NAS e S3.

### Funzionamento del multiprotocollo S3

Il multiprotocollo ONTAP consente di presentare lo stesso set di dati come una gerarchia di file o come oggetti in un bucket. A tale scopo, ONTAP crea "bucket S3 NAS" che consentono ai client S3 di creare, leggere, eliminare ed enumerare i file nello storage NAS utilizzando le richieste a oggetti S3. Questa mappatura è conforme alla configurazione di sicurezza NAS, osservando le autorizzazioni di accesso a file e directory e scrivendo nel registro di controllo della sicurezza secondo necessità.

Questa mappatura viene eseguita presentando una gerarchia di directory NAS specificata come bucket S3. Ogni file nella gerarchia di directory è rappresentato come un oggetto S3 il cui nome è relativo dalla directory mappata verso il basso, con i limiti di directory rappresentati dal carattere barra ('/').

Gli utenti S3 definiti da ONTAP normali possono accedere a questo storage, in base alle policy bucket definite per il bucket che esegue la mappatura alla directory NAS. Affinché ciò sia possibile, è necessario definire le mappature tra gli utenti S3 e gli utenti SMB/NFS. Le credenziali dell'utente SMB/NFS verranno utilizzate per il controllo delle autorizzazioni NAS e incluse nei record di audit risultanti da tali accessi.

Quando viene creato da client SMB o NFS, un file viene immediatamente inserito in una directory e quindi visibile ai client, prima che i dati vengano scritti in essa. I client S3 si aspettano semantica diversa, in cui il

nuovo oggetto non è visibile nello spazio dei nomi fino a quando non sono stati scritti tutti i dati. Questa mappatura di S3 allo storage NAS crea file utilizzando la semantica S3, mantenendo i file invisibili esternamente fino al completamento del comando di creazione S3.

## **Protezione dei dati per i bucket S3 NAS**

I "bucket" S3 NAS sono semplicemente mappature di dati NAS per i client S3, non sono bucket S3 standard. Pertanto, non è necessario proteggere i bucket S3 NAS utilizzando la funzionalità SnapMirror di NetApp S3. È invece possibile proteggere volumi contenenti bucket S3 NAS utilizzando la replica del volume asincrona SnapMirror. Il disaster recovery di SnapMirror Synchronous e SVM non è supportato.

A partire da ONTAP 9.14.1, i bucket S3 NAS sono supportati in aggregati con mirroring e senza mirror per le configurazioni MetroCluster IP e FC.

Scopri di più ["SnapMirror asincrono"](#).

## **Audit per i bucket S3 NAS**

Poiché i bucket S3 NAS non sono bucket S3 convenzionali, l'audit S3 non può essere configurato per controllare l'accesso su di essi. Scopri di più ["Verifica S3"](#).

Tuttavia, i file e le directory NAS mappati nei bucket S3 NAS possono essere controllati per gli eventi di accesso utilizzando le procedure di audit ONTAP convenzionali. Le operazioni S3 possono quindi attivare eventi di audit NAS, con le seguenti eccezioni:

- Se l'accesso al client S3 viene negato dalla configurazione del criterio S3 (policy di gruppo o bucket), l'audit NAS per l'evento non viene avviato. Questo perché le autorizzazioni S3 vengono controllate prima di poter eseguire i controlli di audit SVM.
- Se il file di destinazione di una richiesta S3 GET è di dimensione 0, il contenuto 0 viene restituito alla richiesta GET e l'accesso in lettura non viene registrato.
- Se il file di destinazione di una richiesta S3 GET si trova in una cartella per la quale l'utente non dispone dell'autorizzazione di attraversamento, il tentativo di accesso non riesce e l'evento non viene registrato.

Scopri di più ["Controllo degli eventi NAS su SVM"](#).

## **Interoperabilità S3 e NAS**

I bucket NAS ONTAP S3 supportano le funzionalità NAS e S3 standard, ad eccezione di quelle elencate di seguito.

### **Funzionalità NAS attualmente non supportata dai bucket S3 NAS**

#### **Tier di capacità FabricPool**

I bucket S3 NAS non possono essere configurati come Tier di capacità per FabricPool.

### **La funzionalità S3 non è attualmente supportata dai bucket S3 NAS**

#### **Metadati utente AWS**

- Le coppie di valori chiave ricevute come parte dei metadati utente S3 non vengono memorizzate su disco insieme ai dati oggetto nella release corrente.
- Le intestazioni delle richieste con il prefisso "x-amz-meta" vengono ignorate.

## Tag AWS

- All'avvio delle richieste PUT object e Multipart, le intestazioni con il prefisso "x-amz-tagging" vengono ignorate.
- Le richieste di aggiornamento dei tag su un file esistente (ad esempio, richieste put, GET ed Delete con la stringa di query ?tagging) vengono rifiutate con un errore.

## Versione

Non è possibile specificare la versione nella configurazione di mappatura bucket.

- Le richieste che includono specifiche di versione non null (versionID=stringa di query xyz) ricevono risposte di errore.
- Le richieste che influiscono sullo stato di versione di un bucket vengono rifiutate con errori.

## Operazioni multiparte

Le seguenti operazioni non sono supportate:

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

## Requisiti dei dati NAS per l'accesso al client S3

È importante comprendere che ci sono alcune incompatibilità intrinseche quando si mappano file e directory NAS per l'accesso S3. Potrebbe essere necessario regolare le gerarchie dei file NAS prima di servirle utilizzando i bucket S3 NAS.

Un bucket S3 NAS fornisce l'accesso S3 a una directory NAS mappando tale directory utilizzando la sintassi del bucket S3 e i file nell'albero delle directory vengono visualizzati come oggetti. I nomi degli oggetti sono i percorsi delimitati dalla barra dei file relativi alla directory specificata nella configurazione del bucket S3.

Questa mappatura impone alcuni requisiti quando i file e le directory vengono serviti utilizzando i bucket NAS S3:

- I nomi S3 sono limitati a 1024 byte, pertanto i file con percorsi più lunghi non sono accessibili utilizzando S3.
- I nomi di file e directory sono limitati a 255 caratteri, pertanto il nome di un oggetto non può contenere più di 255 caratteri consecutivi non slash ('/')
- Un nome percorso SMB delimitato da caratteri backslash ("\") viene visualizzato in s3 come nome di oggetto contenente caratteri '/' (barra rovesciata).
- Alcune coppie di nomi di oggetti S3 legali non possono coesistere nell'albero di directory NAS mappato. Ad esempio, i nomi degli oggetti S3 legali "part1/part2" e "part1/part2/part3" corrispondono a file che non possono esistere contemporaneamente nell'albero delle directory NAS, in quanto "part1/part2" è un file nel nome e una directory nell'altro.
  - Se "part1/part2" è un file esistente, la creazione S3 di "part1/part2/part3" non riesce.
  - Se "part1/part2/part3" è un file esistente, la creazione o l'eliminazione S3 di "part1/part2" non avrà esito positivo.
  - La creazione di un oggetto S3 che corrisponde al nome di un oggetto esistente sostituisce l'oggetto

pre-esistente (nei bucket senza versione), che contiene in NAS ma richiede una corrispondenza esatta. Gli esempi precedenti non causeranno la rimozione dell'oggetto esistente perché, mentre i nomi si scontrano, non corrispondono.

Sebbene un archivio di oggetti sia progettato per supportare un numero molto elevato di nomi arbitrari, una struttura di directory NAS può riscontrare problemi di performance se un numero molto elevato di nomi viene inserito in una directory. In particolare, i nomi che non contengono caratteri slash (/) verranno tutti inseriti nella directory principale della mappatura NAS. Le applicazioni che utilizzano in modo esteso nomi non compatibili con NAS potrebbero essere ospitate meglio su un bucket di archivio di oggetti effettivo piuttosto che su una mappatura NAS.

## Abilitare l'accesso del protocollo S3 ai dati NAS

L'abilitazione dell'accesso al protocollo S3 consiste nel garantire che una SVM abilitata NAS soddisfi gli stessi requisiti di un server abilitato S3, tra cui l'aggiunta di un server di archiviazione a oggetti e la verifica dei requisiti di rete e autenticazione.

Per le nuove installazioni ONTAP, si consiglia di abilitare l'accesso al protocollo S3 a una SVM dopo averla configurato per fornire i dati NAS ai client. Per ulteriori informazioni sulla configurazione del protocollo NAS, consultare:

- ["Configurazione NFS"](#)
- ["Configurazione SMB"](#)

### Prima di iniziare

Prima di attivare il protocollo S3, è necessario configurare quanto segue:

- Il protocollo S3 e i protocolli NAS desiderati (NFS, SMB o entrambi) sono concessi in licenza.
- Viene configurata una SVM per i protocolli NAS desiderati.
- Esistono server NFS e/o SMB.
- Il DNS e gli altri servizi richiesti sono configurati.
- I dati NAS vengono esportati o condivisi nei sistemi client.

### A proposito di questa attività


Per abilitare il traffico HTTPS dai client S3 alla SVM abilitata per S3, è necessario un certificato CA (Certificate Authority). È possibile utilizzare certificati CA provenienti da tre origini:

- Un nuovo certificato autofirmato ONTAP sulla SVM.
- Un certificato autofirmato ONTAP esistente su SVM.
- Un certificato di terze parti.

Per il bucket S3/NAS è possibile utilizzare le stesse LIF di dati utilizzate per la fornitura dei dati NAS. Se sono richiesti indirizzi IP specifici, vedere ["Creazione di LIF di dati"](#). Per attivare il traffico dati S3 su LIF è necessaria una policy dei dati del servizio S3; è possibile modificare la policy di servizio esistente di SVM in modo da includere S3.

Quando si crea il server a oggetti S3, si dovrebbe essere pronti a inserire il nome del server S3 come FQDN (Fully Qualified Domain Name), che i client utilizzeranno per l'accesso S3. L'FQDN del server S3 non deve iniziare con un nome bucket.

## System Manager

1. Abilitare S3 su una VM di storage con protocolli NAS configurati.
  - a. Fare clic su **Storage > Storage VM**, selezionare una VM storage pronta per NAS, fare clic su Settings (Impostazioni), quindi fare clic su  Sotto S3.
  - b. Selezionare il tipo di certificato. Se si seleziona un certificato generato dal sistema o uno dei propri, questo sarà necessario per l'accesso del client.
  - c. Inserire le interfacce di rete.
2. Se è stato selezionato il certificato generato dal sistema, le informazioni del certificato vengono visualizzate quando viene confermata la creazione della nuova VM di storage. Fare clic su **Download** e salvarlo per accedere al client.
  - La chiave segreta non viene visualizzata di nuovo.
  - Se sono necessarie nuovamente le informazioni del certificato: Fare clic su **Storage > Storage VMS**, selezionare la VM di storage e fare clic su **Settings** (Impostazioni).

## CLI

1. Verificare che il protocollo S3 sia consentito su SVM:  
`vserver show -fields allowed-protocols`
2. Registrare il certificato della chiave pubblica per questa SVM. + se è necessario un nuovo certificato autofirmato ONTAP, vedere ["Creare e installare un certificato CA sulla SVM"](#).
3. Aggiornare la policy dei dati del servizio
  - a. Visualizzare la policy dei dati di servizio per SVM  
`network interface service-policy show -vserver svm_name`
  - b. Aggiungere il data-core e data-s3-server services se non sono presenti.  
`network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. Verificare che i dati LIF presenti su SVM soddisfino i requisiti:  
`network interface show -vserver svm_name`
5. Creare il server S3:  
`vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

È possibile specificare opzioni aggiuntive durante la creazione del server S3 o in qualsiasi momento successivo.

- HTTPS è attivato per impostazione predefinita sulla porta 443. È possibile modificare il numero di porta con l'opzione `-Secure-listener-port`. + quando HTTPS è attivato, i certificati CA sono necessari per la corretta integrazione con SSL/TLS.
- HTTP è disattivato per impostazione predefinita; se attivato, il server è in attesa sulla porta 80. Puoi abilitarlo con l'opzione `-is-http-enabled` o modificare il numero di porta con l'opzione `-listener-port`. + quando HTTP è attivato, tutte le richieste e le risposte vengono inviate in rete in testo non crittografato.

1. Verificare che S3 sia configurato come desiderato:  
`vserver object-store-server show`

**Esempio** + il seguente comando verifica i valori di configurazione di tutti i server di storage a oggetti:

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1
```

```
Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svml_ca
Comment: Server comment
```

## Creare un bucket S3 NAS

Un bucket S3 NAS è una mappatura tra un nome di bucket S3 e un percorso NAS. I bucket NAS S3 consentono di fornire l'accesso S3 a qualsiasi parte di uno spazio dei nomi SVM con volumi e struttura di directory esistenti.

### Prima di iniziare

- Un server a oggetti S3 è configurato in una SVM contenente dati NAS.
- I dati NAS sono conformi a ["Requisiti per l'accesso al client S3"](#).

### A proposito di questa attività

È possibile configurare i bucket S3 NAS per specificare qualsiasi set di file e directory all'interno della directory root di SVM.

È inoltre possibile impostare policy bucket che consentono o non consentono l'accesso ai dati NAS in base a qualsiasi combinazione di questi parametri:

- File e directory
- Autorizzazioni utente e gruppo
- Operazioni S3

Ad esempio, potrebbero essere necessarie policy di bucket separate che concedano l'accesso ai dati di sola lettura a un gruppo di utenti di grandi dimensioni e un'altra che consenta a un gruppo limitato di eseguire operazioni su un sottoinsieme di tali dati.

Poiché i "bucket" S3 NAS sono mappature e non bucket S3, le seguenti proprietà dei bucket S3 standard non si applicano ai bucket S3 NAS.

- **Aggr-list/aggr-list-moltiplicer/storage-service-level/volume/size/exclude-aggr-list/qos-policy-group** + Nessun volume o qtree viene creato durante la configurazione dei bucket S3 NAS.
- **Il ruolo è -protetto/è -Protected-on-ontap/è -Protected-on-cloud** + i bucket NAS S3 non sono protetti o mirrorati utilizzando S3 SnapMirror, ma utilizzeranno invece la protezione SnapMirror regolare disponibile alla granularità del volume.

- **Versioning-state** + i volumi NAS dispongono solitamente della tecnologia Snapshot per salvare versioni diverse. Tuttavia, la versione non è attualmente disponibile nei bucket S3 NAS.
- I comandi del volume consentono di accedere alle statistiche utilizzate in modo logico/object-count\* + equivalenti per i volumi NAS.

### System Manager

Aggiungere un nuovo bucket S3 NAS su una VM di storage abilitata per NAS.

1. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
2. Inserire un nome per il bucket S3 NAS e selezionare la VM di storage, non inserire una dimensione, quindi fare clic su **altre opzioni**.
3. Immettere un nome di percorso valido o fare clic su Browse (Sfoglia) per effettuare una selezione da un elenco di nomi di percorso validi. + quando si immette un nome di percorso valido, le opzioni non rilevanti per la configurazione S3 NAS vengono nascoste.
4. Se gli utenti S3 sono già stati mappati agli utenti NAS e sono stati creati dei gruppi, è possibile configurarne le autorizzazioni, quindi fare clic su **Save** (Salva). + prima di configurare le autorizzazioni in questa fase, è necessario aver già mappato gli utenti S3 agli utenti NAS.

Altrimenti, fare clic su **Save** (Salva) per completare la configurazione del bucket S3 NAS.

### CLI

Creare un bucket S3 NAS in una SVM contenente i filesystem NAS.

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name -type nas -nas-path junction_path [-comment text]
```

Esempio:

```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type
nas -path /vol1
```

## Abilitare gli utenti del client S3

Per consentire agli utenti del client S3 di accedere ai dati NAS, è necessario mappare i nomi utente S3 agli utenti NAS corrispondenti, quindi concedere loro l'autorizzazione ad accedere ai dati NAS utilizzando i criteri di servizio bucket.

### Prima di iniziare

I nomi utente per l'accesso al client (utenti LINUX/UNIX, Windows e S3) devono già esistere.

### A proposito di questa attività

La mappatura di un nome utente S3 a un utente LINUX/UNIX o Windows corrispondente consente di onorare i controlli di autorizzazione sui file NAS quando tali file sono accessibili dai client S3. Le mappature da S3 a NAS vengono specificate fornendo un nome utente S3 *Pattern*, che può essere espresso come un singolo nome o un'espressione regolare POSIX, e un nome utente LINUX/UNIX o Windows *Replacement*.

Se non è presente alcuna mappatura dei nomi, viene utilizzata la mappatura dei nomi predefinita, in cui il nome utente S3 stesso verrà utilizzato come nome utente UNIX e nome utente Windows. È possibile modificare le mappature predefinite dei nomi utente UNIX e Windows con `vserver object-store-server modify` comando.

È supportata solo la configurazione di mappatura dei nomi locali; LDAP non è supportato.

Una volta mappati gli utenti S3 agli utenti NAS, è possibile concedere autorizzazioni agli utenti specificando le risorse (directory e file) a cui hanno accesso e le azioni che possono eseguire o meno.



## System Manager

1. Creare mappature dei nomi locali per client UNIX o Windows (o entrambi).
  - a. Fare clic su **Storage > Bucket**, quindi selezionare la VM di storage abilitata per S3/NAS.
  - b. Selezionare **Impostazioni**, quindi fare clic su ➔ In **Name Mapping** (sotto **host Users and Groups**).
  - c. Nei riquadri **S3 to Windows** o **S3 to UNIX** (o entrambi), fare clic su **Add** (Aggiungi), quindi immettere i nomi utente desiderati **Pattern** (S3) e **Replacement** (NAS).
2. Creare una policy bucket per fornire l'accesso al client.
  - a. Fare clic su **Storage > Bucket**, quindi su ⓘ Accanto al bucket S3 desiderato, quindi fare clic su **Edit** (Modifica).
  - b. Fare clic su **Add** (Aggiungi) e fornire i valori desiderati.
    - **Principal** - specificare i nomi utente S3 o utilizzare il valore predefinito (tutti gli utenti).
    - **Effetto** - selezionare **Consenti** o **Nega**.
    - **Azioni** - inserire azioni per questi utenti e risorse. Le operazioni di risorsa attualmente supportate dal server di archiviazione a oggetti per i bucket NAS S3 sono: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `GetObjectTagging`, `PutObjectTagging`, `DeleteObjectTagging`, `GetBucketLocation`, `GetBucketVersioning`, `PutBucketVersioning` e `ListBucketVersions`. I caratteri jolly sono accettati per questo parametro.
    - **Risorse** - inserire i percorsi di cartella o file in cui le azioni sono consentite o rifiutate, oppure utilizzare le impostazioni predefinite (directory principale del bucket).

## CLI

1. Creare mappature dei nomi locali per client UNIX o Windows (o entrambi).

```
vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix}
-position integer -pattern s3_user_name -replacement nas_user_name
```

  - `-position` - numero di priorità per la valutazione della mappatura; inserire 1 o 2.
  - `-pattern` - Un nome utente S3 o un'espressione regolare
  - `-replacement` - un nome utente windows o unix

## Esempi

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. Creare una policy bucket per fornire l'accesso al client.

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {deny|allow} -action list_of_actions -principal
list_of_users_or_groups -resource [-sid alphanumeric_text]
```

  - `-effect {deny|allow}` - specifica se l'accesso è consentito o negato quando un utente richiede un'azione.
  - `-action <Action>, ...` - specifica le operazioni di risorsa consentite o negate. Le operazioni di risorsa attualmente supportate dal server di archiviazione a oggetti per i bucket NAS S3 sono: `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`, `GetObjectAcl`, `GetObjectTagging`,

PutObjectTagging, DeleteObjectTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning e ListBucketVersions. I caratteri jolly sono accettati per questo parametro.

- `-principal <Objectstore Principal>, ...` - convalida l'utente che richiede l'accesso in base agli utenti o ai gruppi del server dell'archivio di oggetti specificati in questo parametro.
  - Per specificare un gruppo di server di archiviazione oggetti, aggiungere un gruppo di prefissi/ al nome del gruppo.
  - `-principal` - (il trattino) consente l'accesso a tutti gli utenti.
- `-resource <text>, ...` - specifica il bucket, la cartella o l'oggetto per il quale sono impostate le autorizzazioni allow/deny. I caratteri jolly sono accettati per questo parametro.
- `[-sid <SID>]` - specifica un commento di testo facoltativo per l'istruzione del criterio bucket del server archivio oggetti.

#### Esempi

```
cluster1::> vservers object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* -sid "FullAccessForUser1"

cluster1::> vservers object-store-server bucket policy statement create
-vservers vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

## Configurazione SMB per Microsoft Hyper-V e SQL Server

### Panoramica della configurazione SMB per Microsoft Hyper-V e SQL Server

Le funzionalità di ONTAP consentono di eseguire operazioni senza interruzioni per due applicazioni Microsoft tramite il protocollo SMB: Microsoft Hyper-V e Microsoft SQL Server.

Utilizzare queste procedure se si desidera implementare operazioni SMB senza interruzioni nei seguenti casi:

- È stato configurato l'accesso al file del protocollo SMB di base.
- Si desidera abilitare le condivisioni di file SMB 3.0 o versioni successive che risiedono in SVM per memorizzare i seguenti oggetti:
  - File di macchine virtuali Hyper-V.
  - Database di sistema di SQL Server

#### Informazioni correlate

Per ulteriori informazioni sulla tecnologia ONTAP e sull'interazione con i servizi esterni, consultare i seguenti report tecnici: ["Report tecnico NetApp 4172: Best practice Microsoft Hyper-V su SMB 3.0 con ONTAP"](#) ["Report tecnico NetApp 4369: Best practice per Microsoft SQL Server e SnapManager 7.2 per SQL Server con Clustered Data ONTAP"](#)

## Configurare ONTAP per le soluzioni Microsoft Hyper-V e SQL Server su SMB

È possibile utilizzare le condivisioni di file SMB 3.0 e versioni successive disponibili in modo continuo per memorizzare i file delle macchine virtuali Hyper-V o i database di sistema SQL Server e i database degli utenti su volumi residenti in SVM, fornendo al contempo operazioni senza interruzioni (NDOS) per eventi pianificati e non pianificati.

### Microsoft Hyper-V su SMB

Per creare una soluzione Hyper-V su SMB, devi prima configurare ONTAP per fornire servizi di storage per i server Microsoft Hyper-V. Inoltre, è necessario configurare anche i cluster Microsoft (se si utilizza una configurazione in cluster), i server Hyper-V, le connessioni SMB 3.0 continuamente disponibili alle condivisioni ospitate dal server CIFS e, facoltativamente, i servizi di backup per proteggere i file delle macchine virtuali memorizzati nei volumi SVM.



I server Hyper-V devono essere configurati su Windows 2012 Server o versioni successive. Sono supportate le configurazioni dei server Hyper-V in cluster e standalone.

- Per informazioni sulla creazione di cluster Microsoft e server Hyper-V, visitare il sito Web Microsoft.
- SnapManager per Hyper-V è un'applicazione basata su host che semplifica i servizi di backup rapidi basati su copia Snapshot, progettati per l'integrazione con le configurazioni Hyper-V su SMB.

Per informazioni sull'utilizzo di SnapManager con configurazioni Hyper-V su SMB, consultare la [\\_Guida all'installazione e all'amministrazione di SnapManager per Hyper-V](#).

### Microsoft SQL Server su SMB

Per creare una soluzione SQL Server su SMB, è necessario prima configurare ONTAP per fornire servizi di storage per l'applicazione Microsoft SQL Server. Inoltre, è necessario configurare anche i cluster Microsoft (se si utilizza una configurazione in cluster). Installare e configurare SQL Server sui server Windows e creare connessioni SMB 3.0 continuamente disponibili alle condivisioni ospitate dal server CIFS. Facoltativamente, è possibile configurare i servizi di backup per proteggere i file di database memorizzati nei volumi SVM.



SQL Server deve essere installato e configurato su Windows 2012 Server o versione successiva. Sono supportate sia le configurazioni standalone che quelle in cluster.

- Per informazioni sulla creazione di cluster Microsoft e sull'installazione e configurazione di SQL Server, visitare il sito Web Microsoft.
- Il plug-in SnapCenter per Microsoft SQL Server è un'applicazione basata su host che semplifica i servizi di backup rapidi basati su copia Snapshot, progettati per l'integrazione con le configurazioni SQL Server su SMB.

Per informazioni sull'utilizzo del plug-in SnapCenter per Microsoft SQL Server, vedere ["Plug-in SnapCenter per Microsoft SQL Server"](#) documento.

## Operazioni senza interruzioni per Hyper-V e SQL Server su SMB

### Che cosa significa operazioni senza interruzioni per Hyper-V e SQL Server su SMB

Le operazioni senza interruzioni per Hyper-V e SQL Server su SMB si riferiscono alla

combinazione di funzionalità che consentono ai server di applicazioni e alle macchine virtuali o ai database contenuti di rimanere online e di garantire una disponibilità continua durante molte attività amministrative. Ciò include downtime pianificati e non pianificati dell'infrastruttura storage.

Le operazioni senza interruzioni supportate per i server di applicazioni su SMB includono:

- Acquisizione e giveback pianificati
- Takeover non pianificato
- Eseguire l'upgrade
- Delocalizzazione pianificata degli aggregati (ARL)
- Migrazione LIF e failover
- Spostamento pianificato del volume

### **Protocolli che consentono operazioni senza interruzioni su SMB**

Insieme al rilascio di SMB 3.0, Microsoft ha rilasciato nuovi protocolli per fornire le funzionalità necessarie per supportare operazioni senza interruzioni per Hyper-V e SQL Server su SMB.

ONTAP utilizza questi protocolli quando fornisce operazioni senza interruzioni per server di applicazioni su PMI:

- SMB 3.0
- Testimone

### **Concetti chiave sulle operazioni senza interruzioni per Hyper-V e SQL Server su SMB**

Prima di configurare la soluzione Hyper-V o SQL Server su SMB, è necessario comprendere alcuni concetti relativi alle operazioni senza interruzioni (NDOS).

#### **• Quota a disponibilità continua**

Una condivisione SMB 3.0 con la proprietà di condivisione continuamente disponibile impostata. I client che si connettono attraverso condivisioni continuamente disponibili possono sopravvivere a eventi di interruzione come takeover, giveback e trasferimento aggregato.

#### **• Nodo \***

Un singolo controller che è membro di un cluster. Per distinguere i due nodi di una coppia SFO, un nodo viene talvolta chiamato *nodo locale* e l'altro nodo viene talvolta chiamato *nodo partner* o *nodo remoto*. Il principale proprietario dello storage è il nodo locale. Il proprietario secondario, che assume il controllo dello storage in caso di guasto del proprietario primario, è il nodo partner. Ciascun nodo è il principale proprietario dello storage e il proprietario secondario dello storage del partner.

#### **• Trasferimento aggregato senza interruzioni**

Possibilità di spostare un aggregato tra nodi partner all'interno di una coppia SFO in un cluster senza interrompere le applicazioni client.

- **Failover senza interruzioni**

Vedi *Takeover*.

- **Migrazione LIF senza interruzioni**

La possibilità di eseguire una migrazione LIF senza interrompere le applicazioni client connesse al cluster attraverso tale LIF. Per le connessioni SMB, ciò è possibile solo per i client che si connettono utilizzando SMB 2.0 o versioni successive.

- **Operazioni senza interruzioni**

La capacità di eseguire importanti operazioni di gestione e aggiornamento di ONTAP e di resistere agli errori dei nodi senza interrompere le applicazioni client. Questo termine si riferisce alla raccolta di funzionalità di Takeover senza interruzioni, upgrade senza interruzioni e migrazione senza interruzioni nel loro complesso.

- **Upgrade senza interruzioni**

Possibilità di aggiornare l'hardware o il software del nodo senza interruzioni dell'applicazione.

- **Spostamento del volume senza interruzioni**

Possibilità di spostare liberamente un volume nel cluster senza interrompere le applicazioni che utilizzano il volume. Per le connessioni SMB, tutte le versioni di SMB supportano spostamenti di volume senza interruzioni.

- **Handle persistenti**

Proprietà di SMB 3.0 che consente alle connessioni continuamente disponibili di riconnettersi in modo trasparente al server CIFS in caso di disconnessione. In modo analogo ai gestori a lunga durata, i gestori persistenti vengono mantenuti dal server CIFS per un periodo di tempo successivo alla perdita della comunicazione con il client di connessione. Tuttavia, le maniglie persistenti hanno una maggiore resilienza rispetto alle maniglie resistenti. Oltre a dare al client la possibilità di recuperare l'handle in una finestra di 60 secondi dopo la riconnessione, il server CIFS nega l'accesso a tutti gli altri client che richiedono l'accesso al file durante la finestra di 60 secondi.

Le informazioni sugli handle persistenti vengono mirrorate sullo storage persistente del partner SFO, che consente ai client con handle persistenti disconnessi di recuperare gli handle durevoli dopo un evento in cui il partner SFO assume la proprietà dello storage del nodo. Oltre a fornire operazioni senza interruzioni in caso di spostamenti LIF (che supportano la gestione durevole), le maniglie persistenti forniscono operazioni senza interruzioni per il takeover, il giveback e il trasferimento di aggregati.

- **Giveback SFO**

Restituzione degli aggregati nelle sedi domestiche durante il ripristino da un evento di Takeover.

- **Coppia SFO**

Coppia di nodi i cui controller sono configurati per fornire dati l'uno per l'altro se uno dei due nodi smette di funzionare. A seconda del modello di sistema, entrambi i controller possono trovarsi in un unico chassis o in uno chassis separato. Nota come coppia ha in un cluster a due nodi.

- **Takeover**

Il processo mediante il quale il partner assume il controllo dello storage in caso di guasto del proprietario

principale dello storage. Nel contesto di SFO, il failover e il takeover sono sinonimi.

## **In che modo la funzionalità SMB 3.0 supporta operazioni senza interruzioni sulle condivisioni SMB**

SMB 3.0 offre funzionalità cruciali che consentono il supporto per operazioni senza interruzioni per Hyper-V e SQL Server su condivisioni SMB. Ciò include `continuously-available` Condividere la proprietà e un tipo di handle di file noto come *handle persistente* che consentono ai client SMB di recuperare lo stato di apertura del file e ristabilire in modo trasparente le connessioni SMB.

Gli handle persistenti possono essere concessi ai client SMB 3.0 che si connettono a una condivisione con il set di proprietà di condivisione continuamente disponibile. Se la sessione SMB viene disconnessa, il server CIFS conserva le informazioni sullo stato di handle persistente. Il server CIFS blocca le altre richieste client durante il periodo di 60 secondi in cui il client può riconnettersi, consentendo così al client con l'handle persistente di recuperare l'handle dopo una disconnessione dalla rete. I client con handle persistenti possono riconnettersi utilizzando una delle LIF di dati sulla macchina virtuale di storage (SVM), riconnettendosi attraverso lo stesso LIF o attraverso un LIF diverso.

Il trasferimento, il takeover e il giveback degli aggregati avvengono tra coppie SFO. Per gestire senza problemi la disconnessione e la riconnessione delle sessioni con file con handle persistenti, il nodo partner conserva una copia di tutte le informazioni persistenti sul blocco degli handle. Sia che l'evento sia pianificato o non pianificato, il partner SFO può gestire senza interruzioni le riconnesse persistenti dell'handle. Con questa nuova funzionalità, le connessioni SMB 3.0 al server CIFS possono eseguire il failover trasparente e senza interruzioni su un altro LIF di dati assegnato a SVM in eventi che tradizionalmente hanno subito interruzioni.

Sebbene l'utilizzo di handle persistenti consenta al server CIFS di eseguire il failover in modo trasparente sulle connessioni SMB 3.0, se un errore causa il failover dell'applicazione Hyper-V su un altro nodo nel cluster di Windows Server, il client non ha alcun modo per recuperare gli handle di file di questi handle disconnessi. In questo scenario, gli handle di file in stato disconnesso possono potenzialmente bloccare l'accesso all'applicazione Hyper-V se viene riavviata su un nodo diverso. "failover Clustering" fa parte di SMB 3.0 che risolve questo scenario fornendo un meccanismo per invalidare handle obsoleti e in conflitto. Grazie a questo meccanismo, un cluster Hyper-V può essere ripristinato rapidamente in caso di guasto dei nodi del cluster Hyper-V.

## **Cosa fa il protocollo Witness per migliorare il failover trasparente**

Il protocollo Witness offre funzionalità di failover client avanzate per le condivisioni SMB 3.0 a disponibilità continua (condivisioni CA). La funzione Witness facilita un failover più rapido perché evita il periodo di failover di LIF. Notifica agli application server quando un nodo non è disponibile senza dover attendere il timeout della connessione SMB 3.0.

Il failover è perfetto, con le applicazioni in esecuzione sul client che non sono a conoscenza del failover. Se il server di controllo del mirroring non è disponibile, le operazioni di failover continuano a essere eseguite correttamente, ma il failover senza server di controllo del mirroring è meno efficiente.

Il failover avanzato di Witness è possibile quando vengono soddisfatti i seguenti requisiti:

- Può essere utilizzato solo con server CIFS con funzionalità SMB 3.0 e SMB 3.0 abilitati.
- Le condivisioni devono utilizzare SMB 3.0 con la proprietà di condivisione a disponibilità continua impostata.
- Il partner SFO del nodo a cui sono connessi i server applicazioni deve avere almeno una LIF di dati

operativi assegnata alla macchina virtuale di storage (SVM) che ospita i dati per i server applicazioni.



Il protocollo Witness opera tra coppie SFO. Poiché i LIF possono migrare a qualsiasi nodo all'interno del cluster, qualsiasi nodo potrebbe dover essere il testimone per il partner SFO. Il protocollo Witness non è in grado di fornire un failover rapido delle connessioni SMB su un dato nodo se la SVM che ospita i dati per gli application server non dispone di una LIF di dati attiva sul nodo partner. Pertanto, ogni nodo del cluster deve disporre di almeno una LIF di dati per ogni SVM che ospita una di queste configurazioni.

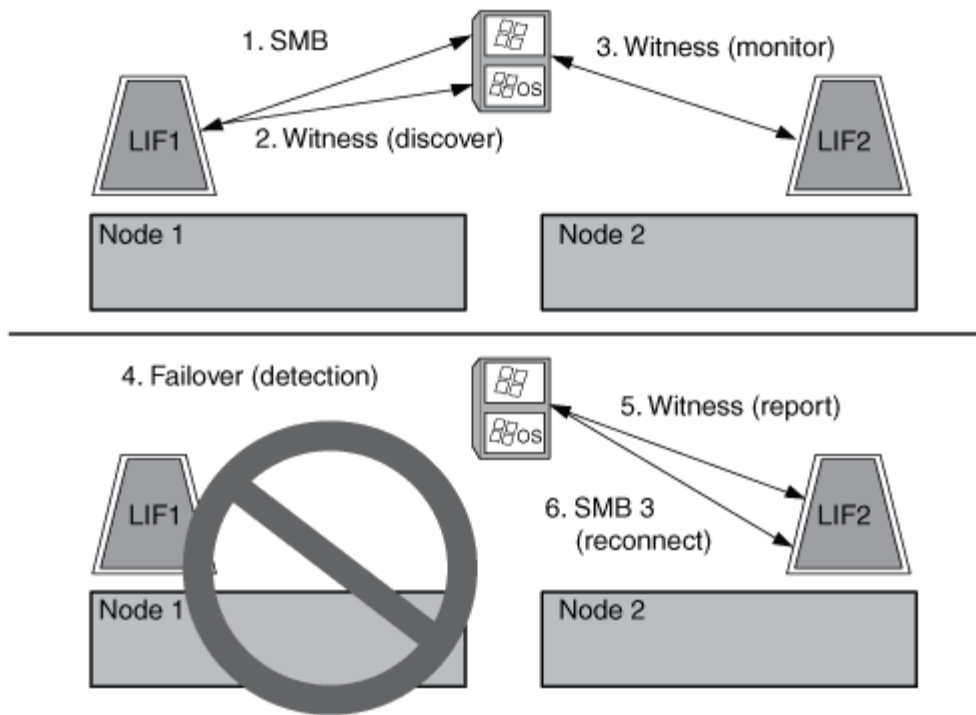
- I server applicazioni devono connettersi al server CIFS utilizzando il nome del server CIFS memorizzato in DNS invece di utilizzare singoli indirizzi IP LIF.

### **Funzionamento del protocollo Witness**

ONTAP implementa il protocollo Witness utilizzando il partner SFO di un nodo come Witness. In caso di guasto, il partner rileva rapidamente il guasto e notifica il client SMB.

Il protocollo Witness offre un failover avanzato utilizzando il seguente processo:

1. Quando l'application server stabilisce una connessione SMB continuamente disponibile al Node1, il server CIFS informa l'application server che il server di controllo è disponibile.
2. Il server applicazioni richiede gli indirizzi IP del server di controllo del mirroring dal Node1 e riceve un elenco di indirizzi IP LIF dei dati Node2 (il partner SFO) assegnati alla macchina virtuale di storage (SVM).
3. Il server applicazioni sceglie uno degli indirizzi IP, crea una connessione testimone a Node2 e registra per ricevere una notifica se la connessione continuamente disponibile su Node1 deve spostarsi.
4. Se si verifica un evento di failover su Node1, Witness facilita gli eventi di failover, ma non è coinvolto nel giveback.
5. Il server di controllo del mirroring rileva l'evento di failover e notifica al server applicazioni tramite la connessione di controllo del mirroring che la connessione SMB deve spostarsi su Node2.
6. L'application server sposta la sessione SMB su Node2 e ripristina la connessione senza interrompere l'accesso al client.



## Backup basati su condivisione con Remote VSS

### Backup basati su condivisione con panoramica di Remote VSS

È possibile utilizzare Remote VSS per eseguire backup basati su condivisioni di file di macchine virtuali Hyper-V memorizzati su un server CIFS.

Microsoft Remote VSS (Volume Shadow Copy Services) è un'estensione dell'infrastruttura Microsoft VSS esistente. Con Remote VSS, Microsoft ha esteso l'infrastruttura VSS per supportare la copia shadow delle condivisioni SMB. Inoltre, le applicazioni server come Hyper-V possono memorizzare i file VHD nelle condivisioni di file SMB. Con queste estensioni, è possibile creare copie shadow coerenti con le applicazioni per le macchine virtuali che memorizzano i file di dati e di configurazione su condivisioni.

### Concetti VSS remoti

È necessario conoscere alcuni concetti necessari per comprendere in che modo i servizi di backup con configurazioni Hyper-V su SMB utilizzano il servizio Remote VSS (Volume Shadow Copy Service).

- **VSS (Volume Shadow Copy Service)**

Tecnologia Microsoft utilizzata per eseguire copie di backup o snapshot di dati su un volume specifico in un determinato momento. Il sistema VSS coordina tra server di dati, applicazioni di backup e software di gestione dello storage per supportare la creazione e la gestione di backup coerenti.

- **VSS remoto (Remote Volume Shadow Copy Service)**

Tecnologia Microsoft utilizzata per eseguire copie di backup basate su condivisione dei dati in uno stato coerente con i dati in un momento specifico in cui si accede ai dati tramite le condivisioni SMB 3.0. Noto anche come *Volume Shadow Copy Service*.



- **Copia shadow**

Un insieme duplicato di dati contenuti nella condivisione in un istante di tempo ben definito. Le copie shadow vengono utilizzate per creare backup point-in-time coerenti dei dati, consentendo al sistema o alle applicazioni di continuare ad aggiornare i dati sui volumi originali.

- **Set di copie shadow**

Una raccolta di una o più copie shadow, con ciascuna copia shadow corrispondente a una condivisione. Le copie shadow all'interno di un set di copie shadow rappresentano tutte le condivisioni di cui è necessario eseguire il backup nella stessa operazione. Il client VSS nell'applicazione abilitata per VSS identifica le copie shadow da includere nel set.

- **Recupero automatico del set di copie shadow**

Parte del processo di backup per le applicazioni di backup remote abilitate per VSS in cui la directory di replica contenente le copie shadow viene resa coerente point-in-time. All'inizio del backup, il client VSS sull'applicazione attiva l'applicazione per prendere punti di controllo software sui dati pianificati per il backup (i file della macchina virtuale nel caso di Hyper-V). Il client VSS consente quindi alle applicazioni di continuare. Una volta creato il set di copie shadow, Remote VSS rende il set di copie shadow scrivibile ed espone la copia scrivibile alle applicazioni. L'applicazione prepara il set di copie shadow per il backup eseguendo un ripristino automatico utilizzando il checkpoint del software preso in precedenza. Il ripristino automatico porta le copie shadow in uno stato coerente srotolando le modifiche apportate ai file e alle directory dalla creazione del checkpoint. Il ripristino automatico è un passaggio opzionale per i backup abilitati per VSS.

- **ID copia shadow**

GUID che identifica in modo univoco una copia shadow.

- **ID set copia shadow**

GUID che identifica in modo univoco una raccolta di ID di copia shadow sullo stesso server.

- **SnapManager per Hyper-V**

Il software che automatizza e semplifica le operazioni di backup e ripristino per Microsoft Windows Server 2012 Hyper-V. SnapManager per Hyper-V utilizza VSS remoto con recovery automatico per eseguire il backup dei file Hyper-V sulle condivisioni SMB.

## **Informazioni correlate**

[Concetti chiave sulle operazioni senza interruzioni per Hyper-V e SQL Server su SMB](#)

[Backup basati su condivisione con Remote VSS](#)

## **Esempio di struttura di directory utilizzata da Remote VSS**

Il VSS remoto attraversa la struttura di directory che memorizza i file delle macchine virtuali Hyper-V durante la creazione di copie shadow. È importante capire quale sia la struttura di directory appropriata, in modo da poter creare correttamente i backup dei file delle macchine virtuali.

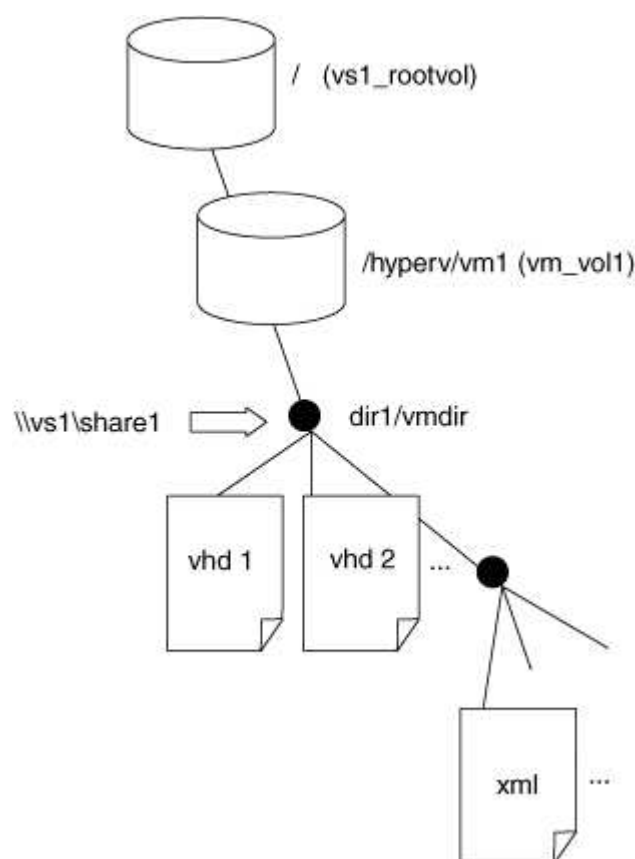
Una struttura di directory supportata per la creazione di copie shadow è conforme ai seguenti requisiti:

- Solo le directory e i file regolari sono presenti all'interno della struttura di directory utilizzata per memorizzare i file delle macchine virtuali.

La struttura di directory non contiene giunzioni, collegamenti o file non regolari.

- Tutti i file di una macchina virtuale risiedono all'interno di una singola condivisione.
- La struttura di directory utilizzata per memorizzare i file delle macchine virtuali non supera la profondità configurata della directory di copia shadow.
- La directory principale della condivisione contiene solo i file o le directory delle macchine virtuali.

Nella seguente illustrazione, il volume denominato `vm_vol1` viene creato con un punto di giunzione in `/hyperv/vm1` Su storage virtual machine (SVM) `vs1`. Le sottodirectory che contengono i file della macchina virtuale vengono create sotto il punto di giunzione. Ai file della macchina virtuale del server Hyper-V si accede tramite `share1` che ha il percorso `/hyperv/vm1/dir1/vmdir`. Il servizio di copia shadow crea copie shadow di tutti i file della macchina virtuale contenuti nella struttura di directory sotto `share1` (fino alla profondità configurata della directory di copia shadow).



### In che modo SnapManager per Hyper-V gestisce backup remoti basati su VSS per Hyper-V su SMB

È possibile utilizzare SnapManager per Hyper-V per gestire i servizi di backup basati su VSS remoto. L'utilizzo del servizio di backup gestito di SnapManager per Hyper-V offre vantaggi per creare set di backup efficienti in termini di spazio.

Le ottimizzazioni di SnapManager per i backup gestiti da Hyper-V includono quanto segue:

- L'integrazione di SnapDrive con ONTAP offre l'ottimizzazione delle performance quando si scopre la posizione di condivisione delle PMI.

ONTAP fornisce a SnapDrive il nome del volume in cui risiede la condivisione.

- SnapManager per Hyper-V specifica l'elenco dei file delle macchine virtuali nelle condivisioni SMB che il servizio di copia shadow deve copiare.

Fornendo un elenco mirato di file di macchine virtuali, il servizio di copia shadow non deve creare copie shadow di tutti i file nella condivisione.

- La macchina virtuale per lo storage (SVM) conserva le copie Snapshot per SnapManager per Hyper-V da utilizzare per i ripristini.

Non esiste alcuna fase di backup. Il backup è la copia Snapshot efficiente in termini di spazio.

SnapManager per Hyper-V offre funzionalità di backup e ripristino per HyperV su SMB utilizzando il seguente processo:

#### 1. Preparazione per l'operazione di copia shadow

Il client VSS di SnapManager per l'applicazione Hyper-V imposta il set di copie shadow. Il client VSS raccoglie informazioni sulle condivisioni da includere nel set di copie shadow e fornisce queste informazioni a ONTAP. Un set potrebbe contenere una o più copie shadow e una copia shadow corrisponde a una condivisione.

#### 2. Creazione del set di copie shadow (se viene utilizzato il ripristino automatico)

Per ogni condivisione inclusa nel set di copie shadow, ONTAP crea una copia shadow e la rende scrivibile.

#### 3. Esposizione del set di copie shadow

Dopo che ONTAP ha creato le copie shadow, queste vengono esposte a SnapManager per Hyper-V in modo che i writer VSS dell'applicazione possano eseguire il ripristino automatico.

#### 4. Ripristino automatico del set di copie shadow

Durante la creazione del set di copie shadow, vi è un periodo di tempo in cui si verificano modifiche attive ai file inclusi nel set di backup. I writer VSS dell'applicazione devono aggiornare le copie shadow per assicurarsi che si trovino in uno stato completamente coerente prima del backup.



Il modo in cui viene eseguito il ripristino automatico è specifico dell'applicazione. Il VSS remoto non è coinvolto in questa fase.

#### 5. Completamento e pulizia del set di copie shadow

Il client VSS notifica a ONTAP una volta completato il ripristino automatico. Il set di copie shadow viene reso di sola lettura e quindi pronto per il backup. Quando si utilizza SnapManager per Hyper-V per il backup, i file in una copia Snapshot diventano il backup; pertanto, per la fase di backup, viene creata una copia Snapshot per ogni volume contenente condivisioni nel set di backup. Una volta completato il backup, il set di copie shadow viene rimosso dal server CIFS.

## Come viene utilizzato l'offload delle copie ODX con Hyper-V e SQL Server su condivisioni SMB

Offloaded Data Transfer (ODX), noto anche come *copy offload*, consente il trasferimento

diretto dei dati all'interno o tra dispositivi di storage compatibili senza trasferire i dati attraverso il computer host. L'offload delle copie ODX di ONTAP offre vantaggi in termini di performance quando si eseguono operazioni di copia sul server applicativo rispetto all'installazione SMB.

Nei trasferimenti di file non ODX, i dati vengono letti dal server CIFS di origine e trasferiti attraverso la rete al computer client. Il computer client trasferisce di nuovo i dati sulla rete al server CIFS di destinazione. In sintesi, il computer client legge i dati dall'origine e li scrive nella destinazione. Con i trasferimenti di file ODX, i dati vengono copiati direttamente dall'origine alla destinazione.

Poiché le copie ODX offloaded vengono eseguite direttamente tra lo storage di origine e di destinazione, le performance sono notevolmente migliorate. I benefici delle performance ottenuti includono tempi di copia più rapidi tra origine e destinazione, utilizzo ridotto delle risorse (CPU, memoria) sul client e utilizzo ridotto della larghezza di banda i/o di rete.

ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0 continuously available connections.

I seguenti casi di utilizzo supportano l'utilizzo di copie e spostamenti ODX:

- Intra-volume

I file di origine e di destinazione o LUN si trovano all'interno dello stesso volume.

- Tra volumi, stesso nodo, stessa SVM (Storage Virtual Machine)

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà della stessa SVM.

- Intervolume, nodi diversi, stessa SVM

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà della stessa SVM.

- Inter-SVM, stesso nodo

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà di diverse SVM.

- Inter-SVM, nodi diversi

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà di diverse SVM.

I casi di utilizzo specifici per l'offload delle copie ODX con le soluzioni Hyper-V includono:

- È possibile utilizzare il pass-through di offload delle copie ODX con Hyper-V per copiare i dati all'interno o tra file di dischi rigidi virtuali (VHD) o per copiare i dati tra le condivisioni SMB mappate e le LUN iSCSI connesse all'interno dello stesso cluster.

Ciò consente il passaggio delle copie dai sistemi operativi guest allo storage sottostante.

- Quando si creano VHD di dimensioni fisse, ODX viene utilizzato per inizializzare il disco con zero, utilizzando un token azzerato ben noto.
- L'offload delle copie ODX viene utilizzato per la migrazione dello storage delle macchine virtuali se lo storage di origine e di destinazione si trova sullo stesso cluster.



Per sfruttare i casi di utilizzo del pass-through di offload delle copie ODX con Hyper-V, il sistema operativo guest deve supportare ODX e i dischi del sistema operativo guest devono essere dischi SCSI supportati dallo storage (SMB o SAN) che supporti ODX. I dischi IDE sul sistema operativo guest non supportano il pass-through ODX.

I casi di utilizzo specifici per l'offload delle copie ODX con le soluzioni SQL Server includono:

- È possibile utilizzare l'offload delle copie di ODX per esportare e importare i database SQL Server tra le condivisioni SMB mappate o tra le condivisioni SMB e le LUN iSCSI connesse all'interno dello stesso cluster.
- L'offload delle copie ODX viene utilizzato per le esportazioni e le importazioni dei database se lo storage di origine e di destinazione si trova nello stesso cluster.

## Requisiti di configurazione e considerazioni

### ONTAP e requisiti di licenza

Quando si creano soluzioni SQL Server o Hyper-V su PMI, è necessario conoscere alcuni requisiti di licenza e ONTAP per operazioni senza interruzioni su SVM.

#### Requisiti di versione di ONTAP

- Hyper-V su SMB

ONTAP supporta operazioni senza interruzioni sulle condivisioni SMB per Hyper-V in esecuzione su Windows 2012 o versioni successive.

- SQL Server su SMB

ONTAP supporta operazioni senza interruzioni su condivisioni SMB per SQL Server 2012 o versioni successive in esecuzione su Windows 2012 o versioni successive.

Per informazioni aggiornate sulle versioni supportate di ONTAP, Windows Server e SQL Server per operazioni senza interruzioni sulle condivisioni SMB, consulta la matrice di interoperabilità.

["Tool di matrice di interoperabilità NetApp"](#)

#### Requisiti di licenza

Sono necessarie le seguenti licenze:

- CIFS
- FlexClone (solo per Hyper-V su SMB)

Questa licenza è necessaria se si utilizza VSS remoto per i backup. Il servizio di copia shadow utilizza FlexClone per creare copie point-in-time dei file che vengono poi utilizzate durante la creazione di un backup.

Una licenza FlexClone è opzionale se si utilizza un metodo di backup che non utilizza Remote VSS.

La licenza FlexClone è inclusa in "ONTAP uno". Se non si dispone di ONTAP ONE, è necessario ["verificare che le licenze richieste siano installate"](#), e, se necessario, ["installarli"](#).

## Requisiti LIF di rete e dati

Quando si creano configurazioni SQL Server o Hyper-V su SMB per operazioni senza interruzioni, è necessario conoscere alcuni requisiti LIF di rete e dati).

### Requisiti del protocollo di rete

- Sono supportate le reti IPv4 e IPv6.
- È richiesto SMB 3.0 o versione successiva.

SMB 3.0 offre le funzionalità necessarie per creare le connessioni SMB continuamente disponibili necessarie per offrire operazioni senza interruzioni.

- I server DNS devono contenere voci che associano il nome del server CIFS agli indirizzi IP assegnati ai file LIF dei dati sulla macchina virtuale di storage (SVM).

I server applicativi Hyper-V o SQL Server in genere effettuano più connessioni su più file di dati LIF quando accedono a macchine virtuali o file di database. Per una corretta funzionalità, i server applicazioni devono stabilire connessioni SMB multiple utilizzando il nome del server CIFS invece di effettuare connessioni multiple a più indirizzi IP univoci.

Il server Witness richiede inoltre l'utilizzo del nome DNS del server CIFS invece di singoli indirizzi IP LIF.

A partire da ONTAP 9.4, è possibile migliorare il throughput e la tolleranza agli errori per Hyper-V e SQL Server sulle configurazioni SMB attivando SMB multicanale. A tale scopo, è necessario implementare più NIC 1G, 10G o superiori nel cluster e nei client.

### Requisiti Data LIF

- La SVM che ospita l'application server sulla soluzione SMB deve avere almeno un LIF di dati operativi su ogni nodo del cluster.

Le LIF dei dati SVM possono eseguire il failover su altre porte dati all'interno del cluster, inclusi i nodi che attualmente non ospitano dati a cui accedono i server applicazioni. Inoltre, poiché il nodo di controllo è sempre il partner SFO di un nodo a cui è connesso l'application server, ogni nodo del cluster è un potenziale nodo di controllo.

- I file LIF dei dati non devono essere configurati per il ripristino automatico.

Dopo un takeover o un evento di giveback, è necessario ripristinare manualmente le LIF dei dati alle porte home.

- Tutti gli indirizzi IP LIF dei dati devono avere una voce nel DNS e tutte le voci devono essere risolte nel nome del server CIFS.

I server applicazioni devono connettersi alle condivisioni SMB utilizzando il nome del server CIFS. Non è necessario configurare i server applicazioni per effettuare connessioni utilizzando gli indirizzi IP LIF.

- Se il nome del server CIFS è diverso dal nome SVM, le voci DNS devono essere risolte nel nome del server CIFS.

## Requisiti di volume e server SMB per Hyper-V su SMB

Quando si creano configurazioni Hyper-V su SMB per operazioni senza interruzioni, è necessario conoscere alcuni requisiti di volume e server SMB.

### Requisiti dei server SMB

- SMB 3.0 deve essere attivato.

Questa opzione è attivata per impostazione predefinita.

- L'opzione predefinita del server CIFS dell'utente UNIX deve essere configurata con un account utente UNIX valido.

I server applicazioni utilizzano l'account del computer quando creano una connessione SMB. Poiché tutti gli accessi SMB richiedono che l'utente Windows si meda correttamente a un account utente UNIX o all'account utente UNIX predefinito, ONTAP deve essere in grado di mappare l'account del computer dell'application server all'account utente UNIX predefinito.

- I riferimenti automatici dei nodi devono essere disattivati (questa funzionalità è disattivata per impostazione predefinita).

Se si desidera utilizzare riferimenti automatici ai nodi per l'accesso a dati diversi dai file macchina Hyper-V, è necessario creare una SVM separata per tali dati.

- L'autenticazione Kerberos e NTLM deve essere consentita nel dominio a cui appartiene il server SMB.

ONTAP non annuncia il servizio Kerberos per il VSS remoto; pertanto, il dominio deve essere impostato su Consenti NTLM.

- La funzionalità di copia shadow deve essere attivata.

Questa funzionalità è attivata per impostazione predefinita.

- L'account di dominio Windows utilizzato dal servizio di copia shadow per la creazione delle copie shadow deve essere membro del gruppo BUILTIN/Administrators locale del server SMB o del gruppo BUILTIN/Backup Operators.

### Requisiti di volume

- I volumi utilizzati per memorizzare i file delle macchine virtuali devono essere creati come volumi di sicurezza NTFS.

Per fornire NDOS ai server applicazioni che utilizzano connessioni SMB a disponibilità continua, il volume contenente la condivisione deve essere un volume NTFS. Inoltre, deve sempre essere un volume NTFS. Non è possibile modificare un volume misto di sicurezza o un volume UNIX di sicurezza in un volume NTFS di sicurezza e utilizzarlo direttamente per le condivisioni NDOS su SMB. Se si modifica un volume misto di sicurezza in un volume di sicurezza NTFS e si intende utilizzarlo per le condivisioni NDOS su SMB, è necessario inserire manualmente un ACL nella parte superiore del volume e propagare tale ACL a tutti i file e cartelle contenuti. In caso contrario, le migrazioni delle macchine virtuali o le esportazioni e le importazioni dei file di database in cui i file vengono spostati in un altro volume possono non riuscire se i volumi di origine o di destinazione sono stati inizialmente creati come volumi misti o UNIX di sicurezza e

successivamente modificati in stile di sicurezza NTFS.

- Per eseguire correttamente le operazioni di copia shadow, è necessario disporre di spazio disponibile sufficiente sul volume.

Lo spazio disponibile deve essere almeno pari allo spazio combinato utilizzato da tutti i file, le directory e le sottodirectory contenuti nelle condivisioni incluse nel set di backup delle copie shadow. Questo requisito si applica solo alle copie shadow con ripristino automatico.

### Informazioni correlate

"Microsoft TechNet Library: [technet.microsoft.com/en-us/library/](http://technet.microsoft.com/en-us/library/)"

### Requisiti di volume e server SMB per SQL Server su SMB

Quando si creano configurazioni SQL Server su SMB per operazioni senza interruzioni, è necessario essere a conoscenza di determinati requisiti di volume e server SMB.

#### Requisiti dei server SMB

- SMB 3.0 deve essere attivato.

Questa opzione è attivata per impostazione predefinita.

- L'opzione predefinita del server CIFS dell'utente UNIX deve essere configurata con un account utente UNIX valido.

I server applicazioni utilizzano l'account del computer quando creano una connessione SMB. Poiché tutti gli accessi SMB richiedono che l'utente Windows si logga correttamente a un account utente UNIX o all'account utente UNIX predefinito, ONTAP deve essere in grado di mappare l'account del computer dell'application server all'account utente UNIX predefinito.

Inoltre, SQL Server utilizza un utente di dominio come account del servizio SQL Server. L'account di servizio deve anche essere associato all'utente UNIX predefinito.

- I riferimenti automatici dei nodi devono essere disattivati (questa funzionalità è disattivata per impostazione predefinita).

Se si desidera utilizzare riferimenti automatici ai nodi per l'accesso a dati diversi dai file di database di SQL Server, è necessario creare una SVM separata per tali dati.

- All'account utente Windows utilizzato per l'installazione di SQL Server su ONTAP deve essere assegnato il privilegio SeSecurityPrivilege.

Questo privilegio viene assegnato al gruppo BUILTIN/Administrators locale del server SMB.

#### Requisiti di volume

- I volumi utilizzati per memorizzare i file delle macchine virtuali devono essere creati come volumi di sicurezza NTFS.

Per fornire NDOS ai server applicazioni che utilizzano connessioni SMB a disponibilità continua, il volume contenente la condivisione deve essere un volume NTFS. Inoltre, deve sempre essere un volume NTFS. Non è possibile modificare un volume misto di sicurezza o un volume UNIX di sicurezza in un volume NTFS di sicurezza e utilizzarlo direttamente per le condivisioni NDOS su SMB. Se si modifica un volume



misto di sicurezza in un volume di sicurezza NTFS e si intende utilizzarlo per le condivisioni NDOS su SMB, è necessario inserire manualmente un ACL nella parte superiore del volume e propagare tale ACL a tutti i file e cartelle contenuti. In caso contrario, le migrazioni delle macchine virtuali o le esportazioni e le importazioni dei file di database in cui i file vengono spostati in un altro volume possono non riuscire se i volumi di origine o di destinazione sono stati inizialmente creati come volumi misti o UNIX di sicurezza e successivamente modificati in stile di sicurezza NTFS.

- Sebbene il volume contenente i file di database possa contenere giunzioni, SQL Server non si incrocia durante la creazione della struttura di directory del database.
- Per eseguire correttamente le operazioni di backup del plug-in SnapCenter per SQL Server, è necessario disporre di spazio disponibile sufficiente sul volume.

Il volume su cui risiedono i file di database di SQL Server deve essere sufficientemente grande da contenere la struttura di directory del database e tutti i file contenuti che risiedono nella condivisione.

### Informazioni correlate

["Microsoft TechNet Library: technet.microsoft.com/en-us/library/"](https://technet.microsoft.com/en-us/library/)

### Requisiti e considerazioni di condivisione continuamente disponibili per Hyper-V su SMB

Quando si configurano condivisioni a disponibilità continua per configurazioni Hyper-V su SMB che supportano operazioni senza interruzioni, è necessario essere consapevoli di determinati requisiti e considerazioni.

#### Condividere i requisiti

- Le condivisioni utilizzate dai server applicazioni devono essere configurate con il set di proprietà Continuously Available (disponibilità continua).

Gli application server che si connettono alle condivisioni continuamente disponibili ricevono handle persistenti che consentono loro di riconnettersi senza interruzioni alle condivisioni SMB e recuperare i blocchi di file dopo eventi di interruzione, come takeover, giveback e trasferimento di aggregati.

- Se si desidera utilizzare i servizi di backup abilitati per Remote VSS, non è possibile inserire i file Hyper-V in condivisioni che contengono giunzioni.

In caso di ripristino automatico, la creazione della copia shadow non riesce se viene rilevata una giunzione durante l'attraversamento della condivisione. In caso di non ripristino automatico, la creazione della copia shadow non fallisce, ma la giunzione non punta a nulla.

- Se si desidera utilizzare i servizi di backup abilitati per Remote VSS con il ripristino automatico, non è possibile inserire i file Hyper-V in condivisioni contenenti quanto segue:

- Symlink, hardlink o widelink
- File non regolari

La creazione della copia shadow non riesce se nella copia shadow sono presenti collegamenti o file non regolari. Questo requisito si applica solo alle copie shadow con ripristino automatico.

- Per eseguire correttamente le operazioni di copia shadow, è necessario disporre di spazio disponibile sufficiente sul volume (solo per Hyper-V su SMB).

Lo spazio disponibile deve essere almeno pari allo spazio combinato utilizzato da tutti i file, le directory e le sottodirectory contenuti nelle condivisioni incluse nel set di backup delle copie shadow. Questo

requisito si applica solo alle copie shadow con ripristino automatico.

- Le seguenti proprietà di condivisione non devono essere impostate sulle condivisioni a disponibilità continua utilizzate dai server applicazioni:
  - Home directory
  - Caching degli attributi
  - BranchCache

#### Considerazioni

- Le quote sono supportate nelle condivisioni a disponibilità continua.
- Le seguenti funzionalità non sono supportate per le configurazioni Hyper-V su SMB:
  - Controllo
  - FPolicy
- La scansione antivirus non viene eseguita sulle condivisioni SMB con `continuously-availability` parametro impostato su `Yes`.

#### Requisiti e considerazioni di condivisione continuamente disponibili per SQL Server su SMB

Quando si configurano condivisioni a disponibilità continua per configurazioni SQL Server su SMB che supportano operazioni senza interruzioni, è necessario essere a conoscenza di determinati requisiti e considerazioni.

#### Condividere i requisiti

- I volumi utilizzati per memorizzare i file delle macchine virtuali devono essere creati come volumi di sicurezza NTFS.

Per fornire operazioni senza interruzioni per i server applicazioni che utilizzano connessioni SMB a disponibilità continua, il volume contenente la condivisione deve essere un volume NTFS. Inoltre, deve sempre essere un volume NTFS. Non è possibile modificare un volume misto di sicurezza o un volume UNIX di sicurezza in un volume NTFS di sicurezza e utilizzarlo direttamente per operazioni senza interruzioni sulle condivisioni SMB. Se si modifica un volume misto di sicurezza in un volume di sicurezza NTFS e si intende utilizzarlo per operazioni senza interruzioni sulle condivisioni SMB, è necessario posizionare manualmente un ACL nella parte superiore del volume e propagare tale ACL a tutti i file e cartelle contenuti. In caso contrario, le migrazioni delle macchine virtuali o le esportazioni e le importazioni dei file di database in cui i file vengono spostati in un altro volume possono non riuscire se i volumi di origine o di destinazione sono stati inizialmente creati come volumi misti o UNIX di sicurezza e successivamente modificati in stile di sicurezza NTFS.

- Le condivisioni utilizzate dai server applicazioni devono essere configurate con il set di proprietà `Continuously Available` (disponibilità continua).

Gli application server che si connettono alle condivisioni continuamente disponibili ricevono handle persistenti che consentono loro di riconnettersi senza interruzioni alle condivisioni SMB e recuperare i blocchi di file dopo eventi di interruzione, come takeover, giveback e trasferimento di aggregati.

- Sebbene il volume contenente i file di database possa contenere giunzioni, SQL Server non si incrocia durante la creazione della struttura di directory del database.
- Per eseguire correttamente le operazioni del plug-in SnapCenter per SQL Server, è necessario disporre di

spazio disponibile sufficiente sul volume.

Il volume su cui risiedono i file di database di SQL Server deve essere sufficientemente grande da contenere la struttura di directory del database e tutti i file contenuti che risiedono nella condivisione.

- Le seguenti proprietà di condivisione non devono essere impostate sulle condivisioni a disponibilità continua utilizzate dai server applicazioni:
  - Home directory
  - Caching degli attributi
  - BranchCache

#### **Condividere le considerazioni**

- Le quote sono supportate nelle condivisioni a disponibilità continua.
- Le seguenti funzionalità non sono supportate per le configurazioni SQL Server su SMB:
  - Controllo
  - FPolicy
- La scansione antivirus non viene eseguita sulle condivisioni SMB con `continuously-availability` condividere il set di proprietà.

#### **Considerazioni sul VSS remoto per le configurazioni Hyper-V su SMB**

Quando si utilizzano soluzioni di backup abilitate per VSS remoto per configurazioni Hyper-V su SMB, è necessario tenere presenti alcune considerazioni.

#### **Considerazioni generali su Remote VSS**

- È possibile configurare un massimo di 64 condivisioni per server applicazioni Microsoft.

L'operazione di copia shadow non riesce se sono presenti più di 64 condivisioni in un set di copie shadow. Si tratta di un requisito Microsoft.

- È consentito un solo set di copie shadow attive per server CIFS.

Un'operazione di copia shadow non riesce se è in corso un'operazione di copia shadow sullo stesso server CIFS. Si tratta di un requisito Microsoft.

- Non sono consentite giunzioni all'interno della struttura di directory in cui Remote VSS crea una copia shadow.
  - In caso di ripristino automatico, la creazione della copia shadow non riesce se si incontra una giunzione durante l'attraversamento della condivisione.
  - Nel caso di recovery non automatico, la creazione della copia shadow non fallisce, ma la giunzione non punta a nulla.

#### **Considerazioni sul VSS remoto valide solo per le copie shadow con ripristino automatico**

Alcuni limiti si applicano solo alle copie shadow con ripristino automatico.

- Per la creazione delle copie shadow è consentita una profondità massima di directory di cinque sottodirectory.

Questa è la profondità della directory in cui il servizio di copia shadow crea un set di backup delle copie shadow. La creazione della copia shadow non riesce se le directory contenenti il file della macchina virtuale sono nidificate più in profondità di cinque livelli. Questa opzione consente di limitare l'attraversamento della directory durante la clonazione della condivisione. È possibile modificare la profondità massima della directory utilizzando un'opzione del server CIFS.

- La quantità di spazio disponibile sul volume deve essere adeguata.

Lo spazio disponibile deve essere almeno pari allo spazio combinato utilizzato da tutti i file, le directory e le sottodirectory contenuti nelle condivisioni incluse nel set di backup delle copie shadow.

- Non sono consentiti collegamenti o file non regolari all'interno della struttura di directory in cui Remote VSS crea una copia shadow.

La creazione della copia shadow non riesce se nella condivisione sono presenti collegamenti o file non regolari alla copia shadow. Il processo di clonazione non li supporta.

- Non sono consentiti ACL NFSv4 nelle directory.

Sebbene la creazione delle copie shadow conservi gli ACL NFSv4 nei file, gli ACL NFSv4 nelle directory vengono persi.

- È consentito creare un set di copie shadow per un massimo di 60 secondi.

Le specifiche Microsoft consentono di creare il set di copie shadow per un massimo di 60 secondi. Se il client VSS non riesce a creare il set di copie shadow entro questo intervallo di tempo, l'operazione di copia shadow non riesce; pertanto, questo limita il numero di file in un set di copie shadow. Il numero effettivo di file o macchine virtuali che possono essere inclusi in un set di backup varia; tale numero dipende da molti fattori e deve essere determinato per ogni ambiente del cliente.

## **Requisiti di offload delle copie ODX per SQL Server e Hyper-V su SMB**

L'offload delle copie ODX deve essere attivato se si desidera migrare i file delle macchine virtuali o esportare e importare i file di database direttamente dall'origine alla posizione di storage di destinazione senza inviare dati attraverso i server applicazioni. È necessario comprendere alcuni requisiti sull'utilizzo dell'offload delle copie ODX con SQL Server e Hyper-V su soluzioni SMB.

L'utilizzo dell'offload delle copie di ODX offre un significativo vantaggio in termini di performance. Questa opzione del server CIFS è attivata per impostazione predefinita.

- SMB 3.0 deve essere abilitato per utilizzare l'offload delle copie ODX.
- I volumi di origine devono essere di almeno 1.25 GB.
- La deduplica deve essere attivata sui volumi utilizzati con l'offload delle copie.
- Se si utilizzano volumi compressi, il tipo di compressione deve essere adattivo e sono supportate solo le dimensioni del gruppo di compressione 8K.

Il tipo di compressione secondario non è supportato

- Per utilizzare l'offload delle copie di ODX per migrare i guest Hyper-V all'interno e tra i dischi, i server Hyper-V devono essere configurati per l'utilizzo di dischi SCSI.

L'impostazione predefinita prevede la configurazione dei dischi IDE, ma l'offload delle copie ODX non funziona quando i guest vengono migrati se i dischi vengono creati utilizzando dischi IDE.

## Raccomandazioni per le configurazioni SQL Server e Hyper-V su SMB

Per essere sicuri che le configurazioni di SQL Server e Hyper-V su SMB siano solide e operative, è necessario conoscere le Best practice consigliate per la configurazione delle soluzioni.

### Raccomandazioni generali

- Separare i file del server applicazioni dai dati generali dell'utente.

Se possibile, dedicare un'intera macchina virtuale di storage (SVM) e il relativo storage ai dati dell'application server.

- Per ottenere performance ottimali, non abilitare la firma SMB sulle SVM utilizzate per memorizzare i dati dell'application server.
- Per ottenere le migliori performance e una maggiore tolleranza agli errori, abilitare SMB multicanale per fornire più connessioni tra ONTAP e client in una singola sessione SMB.
- Non creare condivisioni continuamente disponibili su condivisioni diverse da quelle utilizzate nella configurazione Hyper-V o SQL Server su SMB.
- Disattiva la notifica delle modifiche sulle condivisioni utilizzate per la disponibilità continua.
- Non eseguire uno spostamento del volume contemporaneamente al trasferimento dell'aggregato (ARL) perché ARL ha fasi che interrompono alcune operazioni.
- Per le soluzioni Hyper-V su SMB, utilizzare dischi iSCSI in-guest durante la creazione di macchine virtuali in cluster. Condiviso .VHDX I file non sono supportati per Hyper-V su SMB nelle condivisioni SMB ONTAP.

## Pianificare la configurazione di Hyper-V o SQL Server su SMB

### Completare il foglio di lavoro per la configurazione del volume

Il foglio di lavoro offre un modo semplice per registrare i valori necessari per la creazione di volumi per le configurazioni SQL Server e Hyper-V su SMB.

Per ciascun volume, è necessario specificare le seguenti informazioni:

- Nome SVM (Storage Virtual Machine)

Il nome SVM è lo stesso per tutti i volumi.

- Nome del volume
- Nome dell'aggregato

È possibile creare volumi su aggregati situati su qualsiasi nodo del cluster.

- Dimensione
- Percorso di giunzione

Quando si creano volumi utilizzati per memorizzare i dati dell'application server, tenere presente quanto segue:

- Se il volume root non dispone di uno stile di protezione NTFS, è necessario specificare lo stile di protezione come NTFS quando si crea il volume.

Per impostazione predefinita, i volumi ereditano lo stile di sicurezza del volume root SVM.

- I volumi devono essere configurati con la garanzia di spazio del volume predefinita.
- Facoltativamente, è possibile configurare l'impostazione di gestione automatica dello spazio.
- Impostare l'opzione che determina la riserva di spazio di copia Snapshot su 0.
- Il criterio Snapshot applicato al volume deve essere disattivato.

Se il criterio Snapshot SVM è disattivato, non è necessario specificare un criterio Snapshot per i volumi. I volumi ereditano la policy Snapshot per SVM. Se il criterio Snapshot per SVM non è disattivato ed è configurato per creare copie Snapshot, è necessario specificare un criterio Snapshot a livello di volume e tale criterio deve essere disattivato. I backup abilitati al servizio di copia shadow e i backup di SQL Server gestiscono la creazione e l'eliminazione delle copie Snapshot.

- Non è possibile configurare i mirror di condivisione del carico per i volumi.

I percorsi di giunzione su cui si intende creare le condivisioni utilizzate dai server applicazioni devono essere scelti in modo che non vi siano volumi congiunti al di sotto del punto di ingresso della condivisione.

Ad esempio, se si desidera memorizzare i file delle macchine virtuali su quattro volumi denominati “vol1”, “vol2”, “vol3” e “vol4”, è possibile creare lo spazio dei nomi mostrato nell'esempio. È quindi possibile creare condivisioni per i server applicazioni nei seguenti percorsi: /data1/vol1, /data1/vol2, /data2/vol3, e, /data2/vol4.

Vserver	Volume	Junction		Junction	
		Active	Junction Path	Path	Source
vs1	data1	true	/data1	RW_volume	
vs1	vol1	true	/data1/vol1	RW_volume	
vs1	vol2	true	/data1/vol2	RW_volume	
vs1	data2	true	/data2	RW_volume	
vs1	vol3	true	/data2/vol3	RW_volume	
vs1	vol4	true	/data2/vol4	RW_volume	

Tipi di informazioni	Valori
<i>Volume 1: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	
<i>Volume 2: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	
<i>Volume 3: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	

Tipi di informazioni	Valori
<i>Volume 4: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	
<i>Volume 5: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	
<i>Volume 6: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	
<i>Volumi aggiuntivi: Nome del volume, aggregato, dimensione, percorso di giunzione</i>	

### Completare il foglio di lavoro per la configurazione della condivisione SMB

Utilizzare questo foglio di lavoro per registrare i valori necessari per la creazione di condivisioni SMB continuamente disponibili per le configurazioni SQL Server e Hyper-V su SMB.

#### Informazioni sulle proprietà delle condivisioni SMB e sulle impostazioni di configurazione

Per ciascuna condivisione, è necessario specificare le seguenti informazioni:

- Nome SVM (Storage Virtual Machine)

Il nome SVM è lo stesso per tutte le condivisioni

- Nome di condivisione
- Percorso
- Condividere le proprietà

È necessario configurare le seguenti due proprietà di condivisione:

- `oplocks`
- `continuously-available`

Le seguenti proprietà di condivisione non devono essere impostate:

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - I collegamenti simbolici devono essere disattivati (il valore per `-symlink-properties` il parametro deve essere nullo [""]).

#### Informazioni sui percorsi di condivisione

Se si utilizza il VSS remoto per eseguire il backup dei file Hyper-V, è importante scegliere i percorsi di condivisione da utilizzare per le connessioni SMB dai server Hyper-V alle posizioni di storage in cui sono

memorizzati i file delle macchine virtuali. Sebbene sia possibile creare condivisioni in qualsiasi punto dello spazio dei nomi, i percorsi per le condivisioni utilizzati dai server Hyper-V non devono contenere volumi congiunti. Le operazioni di copia shadow non possono essere eseguite su percorsi di condivisione che contengono punti di giunzione.

SQL Server non è in grado di incrociare le giunzioni durante la creazione della struttura di directory del database. Non creare percorsi di condivisione per SQL Server che contengono punti di giunzione.

Ad esempio, dato lo spazio dei nomi mostrato, se si desidera memorizzare i file di macchine virtuali o i file di database sui volumi “vol1”, “vol2”, “vol3” e “vol4”, è necessario creare condivisioni per i server applicazioni nei seguenti percorsi: /data1/vol1, /data1/vol2, /data2/vol3, e. /data2/vol4.

Vserver	Volume	Junction		Junction Path Source
		Active	Junction Path	
vs1	data1	true	/data1	RW_volume
vs1	vol1	true	/data1/vol1	RW_volume
vs1	vol2	true	/data1/vol2	RW_volume
vs1	data2	true	/data2	RW_volume
vs1	vol3	true	/data2/vol3	RW_volume
vs1	vol4	true	/data2/vol4	RW_volume



Sebbene sia possibile creare condivisioni su /data1 e. /data2 percorsi per la gestione amministrativa, non è necessario configurare i server applicazioni per utilizzare tali condivisioni per memorizzare i dati.

Foglio di lavoro per la pianificazione

Tipi di informazioni	Valori
Volume 1: Nome e percorso della condivisione SMB	
Volume 2: Nome e percorso della condivisione SMB	
Volume 3: Nome e percorso della condivisione SMB	
Volume 4: Nome e percorso della condivisione SMB	
Volume 5: Nome e percorso della condivisione SMB	
Volume 6: Nome e percorso della condivisione SMB	
Volume 7: Nome e percorso della condivisione SMB	
Volumi aggiuntivi: Nomi e percorsi di condivisione SMB	



# Creazione di configurazioni ONTAP per operazioni senza interruzioni con Hyper-V e SQL Server su SMB

## Crea configurazioni ONTAP per operazioni senza interruzioni con la panoramica di Hyper-V e SQL Server su SMB

Per preparare le installazioni di ONTAP e Hyper-V, è necessario eseguire diverse operazioni di configurazione di SQL Server che forniscono operazioni senza interruzioni su SMB.

Prima di creare la configurazione ONTAP per operazioni senza interruzioni con Hyper-V e SQL Server su SMB, è necessario completare le seguenti attività:

- I servizi Time devono essere impostati sul cluster.
- È necessario configurare la rete per SVM.
- È necessario creare la SVM.
- Le interfacce Data LIF devono essere configurate su SVM.
- Il DNS deve essere configurato sulla SVM.
- I servizi Names desiderati devono essere impostati per la SVM.
- È necessario creare il server SMB.

### Informazioni correlate

[Pianificare la configurazione di Hyper-V o SQL Server su SMB](#)

[Requisiti di configurazione e considerazioni](#)

### Verificare che sia consentita l'autenticazione Kerberos e NTLMv2 (Hyper-V su condivisioni SMB)

Le operazioni senza interruzioni per Hyper-V su SMB richiedono che il server CIFS su una SVM dati e il server Hyper-V consentano l'autenticazione Kerberos e NTLMv2. È necessario verificare le impostazioni sul server CIFS e sui server Hyper-V che controllano i metodi di autenticazione consentiti.

### A proposito di questa attività

L'autenticazione Kerberos è necessaria quando si effettua una connessione di condivisione continuamente disponibile. Parte del processo VSS remoto utilizza l'autenticazione NTLMv2. Pertanto, le connessioni che utilizzano entrambi i metodi di autenticazione devono essere supportate per le configurazioni Hyper-V su SMB.

È necessario configurare le seguenti impostazioni per consentire l'autenticazione Kerberos e NTLMv2:

- I criteri di esportazione per SMB devono essere disattivati sulla macchina virtuale di storage (SVM).

L'autenticazione Kerberos e NTLMv2 è sempre abilitata sulle SVM, ma è possibile utilizzare i criteri di esportazione per limitare l'accesso in base al metodo di autenticazione.

I criteri di esportazione per SMB sono opzionali e sono disattivati per impostazione predefinita. Se i criteri di esportazione sono disattivati, l'autenticazione Kerberos e NTLMv2 è consentita per impostazione predefinita su un server CIFS.

- Il dominio a cui appartengono il server CIFS e i server Hyper-V deve consentire l'autenticazione Kerberos

e NTLMv2.

L'autenticazione Kerberos è attivata per impostazione predefinita nei domini Active Directory. Tuttavia, l'autenticazione NTLMv2 può essere non consentita, utilizzando le impostazioni dei criteri di protezione o i criteri di gruppo.

### Fasi

1. Eseguire le seguenti operazioni per verificare che i criteri di esportazione siano disattivati su SVM:

- a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- b. Verificare che il `-is-exportpolicy-enabled` L'opzione del server CIFS è impostata su `false`:

```
vserver cifs options show -vserver vserver_name -fields vserver,is-exportpolicy-enabled
```

- c. Tornare al livello di privilegio admin:

```
set -privilege admin
```

2. Se i criteri di esportazione per SMB non sono disattivati, disabilitarli:

```
vserver cifs options modify -vserver vserver_name -is-exportpolicy-enabled false
```

3. Verificare che l'autenticazione NTLMv2 e Kerberos sia consentita nel dominio.

Per informazioni sulla determinazione dei metodi di autenticazione consentiti nel dominio, consultare la Microsoft TechNet Library.

4. Se il dominio non consente l'autenticazione NTLMv2, attivare l'autenticazione NTLMv2 utilizzando uno dei metodi descritti nella documentazione Microsoft.

### Esempio

I seguenti comandi verificano che i criteri di esportazione per SMB siano disattivati su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-----  -
vs1      false

cluster1::*> set -privilege admin
```

## Verificare che gli account di dominio siano associati all'utente UNIX predefinito

Hyper-V e SQL Server utilizzano gli account di dominio per creare connessioni SMB alle condivisioni continuamente disponibili. Per creare correttamente la connessione, l'account del computer deve essere mappato correttamente a un utente UNIX. Il modo più conveniente per eseguire questa operazione consiste nel mappare l'account del computer all'utente UNIX predefinito.

### A proposito di questa attività

Hyper-V e SQL Server utilizzano gli account dei computer di dominio per creare connessioni SMB. Inoltre, SQL Server utilizza un account utente di dominio come account di servizio che effettua anche connessioni SMB.

Quando si crea una macchina virtuale per lo storage (SVM), ONTAP crea automaticamente l'utente predefinito "pcuser" (con un UID di 65534) e il gruppo denominato "pcuser" (con un GID di 65534) e aggiunge l'utente predefinito al gruppo "pcuser". Se si configura una soluzione Hyper-V su SMB su una SVM esistente prima dell'aggiornamento del cluster a Data ONTAP 8.2, l'utente e il gruppo predefiniti potrebbero non esistere. In caso contrario, è necessario crearli prima di configurare l'utente UNIX predefinito del server CIFS.

### Fasi

1. Determinare se esiste un utente UNIX predefinito:

```
vserver cifs options show -vserver vserver_name
```

2. Se l'opzione utente predefinita non è impostata, determinare se esiste un utente UNIX che può essere designato come utente UNIX predefinito:

```
vserver services unix-user show -vserver vserver_name
```

3. Se l'opzione utente predefinita non è impostata e non esiste un utente UNIX che può essere designato come utente UNIX predefinito, creare l'utente UNIX predefinito e il gruppo predefinito, quindi aggiungere l'utente predefinito al gruppo.

In genere, all'utente predefinito viene assegnato il nome utente "pcuser" e deve essere assegnato l'UID di 65534. Al gruppo predefinito viene generalmente assegnato il nome "pcuser". Il GID assegnato al gruppo deve essere 65534.

- a. Creare il gruppo predefinito:

```
vserver services unix-group create -vserver vserver_name -name pcuser -id 65534
```

- b. Creare l'utente predefinito e aggiungerlo al gruppo predefinito:

```
vserver services unix-user create -vserver vserver_name -user pcuser -id 65534 -primary-gid 65534
```

- c. Verificare che l'utente e il gruppo predefinito siano configurati correttamente:

```
vserver services unix-user show -vserver vserver_name+  
vserver services unix-group show -vserver vserver_name -members
```

4. Se l'utente predefinito del server CIFS non è configurato, eseguire le seguenti operazioni:

- a. Configurare l'utente predefinito:

```
vserver cifs options modify -vserver *vserver_name -default-unix-user
```

pcuser\*

- b. Verificare che l'utente UNIX predefinito sia configurato correttamente:

**vserver cifs options show -vserver vserver\_name**

5. Per verificare che l'account del computer del server applicazioni sia associato correttamente all'utente predefinito, mappare un'unità a una condivisione che risiede sulla SVM e confermare l'associazione dell'utente Windows all'utente UNIX utilizzando `vserver cifs session show` comando.

Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine man.

### Esempio

I seguenti comandi determinano che l'utente predefinito del server CIFS non è impostato, ma determinano l'esistenza dell'utente "pcuser" e del gruppo "pcuser". L'utente "pcuser" viene assegnato come utente predefinito del server CIFS su SVM vs1.

```
cluster1::> vserver cifs options show
```

```
Vserver: vs1
```

```
Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : -
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

```
cluster1::> vserver services unix-user show
```

Vserver	User Name	User ID	Group ID	Full Name
vs1	nobody	65535	65535	-
vs1	pcuser	65534	65534	-
vs1	root	0	1	-

```
cluster1::> vserver services unix-group show -members
```

Vserver	Name	ID
vs1	daemon	1
	Users: -	
vs1	nobody	65535
	Users: -	
vs1	pcuser	65534
	Users: -	
vs1	root	0

Users: -

```
cluster1::> vsserver cifs options modify -vsserver vs1 -default-unix-user pcuser
```

```
cluster1::> vsserver cifs options show
```

Vserver: vs1

```
Client Session Timeout : 900
Default Unix Group      : -
Default Unix User       : pcuser
Guest Unix User         : -
Read Grants Exec        : disabled
Read Only Delete        : disabled
WINS Servers            : -
```

### Verificare che lo stile di protezione del volume root SVM sia impostato su NTFS

Per garantire il successo delle operazioni senza interruzioni per Hyper-V e SQL Server su SMB, i volumi devono essere creati con lo stile di sicurezza NTFS. Poiché lo stile di sicurezza del volume root viene applicato per impostazione predefinita ai volumi creati sulla macchina virtuale di storage (SVM), lo stile di sicurezza del volume root deve essere impostato su NTFS.

#### A proposito di questa attività

- È possibile specificare lo stile di sicurezza del volume root al momento della creazione di SVM.
- Se SVM non viene creato con il volume root impostato sullo stile di protezione NTFS, è possibile modificare lo stile di protezione in un secondo momento utilizzando `volume modify` comando.

#### Fasi

1. Determinare lo stile di sicurezza corrente del volume root SVM:

```
volume show -vsserver vserver_name -fields vsserver,volume,security-style
```

2. Se il volume root non è un volume di sicurezza NTFS, impostare lo stile di protezione su NTFS:

```
volume modify -vsserver vserver_name -volume root_volume_name -security-style ntfs
```

3. Verificare che il volume root SVM sia impostato sullo stile di protezione NTFS:

```
volume show -vsserver vserver_name -fields vsserver,volume,security-style
```

#### Esempio

I seguenti comandi verificano che lo stile di protezione del volume root sia NTFS su SVM vs1:

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume      security-style
-----  -
vs1      vs1_root     unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume      security-style
-----  -
vs1      vs1_root     ntfs
```

### Verificare che le opzioni del server CIFS richieste siano configurate

È necessario verificare che le opzioni del server CIFS richieste siano attivate e configurate in base ai requisiti delle operazioni senza interruzioni per Hyper-V e SQL Server su SMB.

#### A proposito di questa attività

- SMB 2.x e SMB 3.0 devono essere abilitati.
- L'offload delle copie di ODX deve essere abilitato per utilizzare l'offload delle copie che migliora le performance.
- I servizi di copia shadow di VSS devono essere attivati se la soluzione Hyper-V su SMB utilizza servizi di backup abilitati per VSS remoto (solo Hyper-V).

#### Fasi

1. Verificare che le opzioni del server CIFS richieste siano attivate sulla macchina virtuale di storage (SVM):
  - a. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- b. Immettere il seguente comando:

```
vserver cifs options show -vserver vserver_name
```

Le seguenti opzioni devono essere impostate su `true`:

- `-smb2-enabled`
- `-smb3-enabled`
- `-copy-offload-enabled`
- `-shadowcopy-enabled` (Solo Hyper-V)

2. Se una delle opzioni non è impostata su `true`, eseguire le seguenti operazioni:
  - a. Impostarli su `true` utilizzando `vserver cifs options modify` comando.

- b. Verificare che le opzioni siano impostate su true utilizzando `vserver cifs options show` comando.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

### Esempio

I seguenti comandi verificano che le opzioni richieste per la configurazione Hyper-V su SMB siano attivate su SVM vs1. Nell'esempio, l'offload delle copie ODX deve essere abilitato per soddisfare i requisiti delle opzioni.

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
-----
vs1      true          true          false          true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-----
vs1      true

cluster1::*> set -privilege admin
```

### Configurare SMB multicanale per performance e ridondanza

A partire da ONTAP 9.4, è possibile configurare SMB multicanale in modo da fornire più connessioni tra ONTAP e client in una singola sessione SMB. In questo modo si migliora il throughput e la tolleranza agli errori per Hyper-V e SQL Server rispetto alle configurazioni SMB.

#### Di cosa hai bisogno

È possibile utilizzare la funzionalità SMB multicanale solo quando i client negoziano con SMB 3.0 o versioni successive. SMB 3.0 e versioni successive sono attivate sul server SMB ONTAP per impostazione predefinita.

#### A proposito di questa attività

I client SMB rilevano e utilizzano automaticamente più connessioni di rete se viene identificata una configurazione corretta nel cluster ONTAP.

Il numero di connessioni simultanee in una sessione SMB dipende dalle schede NIC implementate:

- **NIC 1G su client e cluster ONTAP**

Il client stabilisce una connessione per NIC e associa la sessione a tutte le connessioni.

- **NIC da 10 G e capacità superiore su cluster client e ONTAP**

Il client stabilisce fino a quattro connessioni per NIC e associa la sessione a tutte le connessioni. Il client può stabilire connessioni su più NIC da 10 G e capacità maggiore.

È inoltre possibile modificare i seguenti parametri (privilegio avanzato):

- **-max-connections-per-session**

Numero massimo di connessioni consentite per sessione multicanale. L'impostazione predefinita è 32 connessioni.

Se si desidera attivare più connessioni rispetto a quelle predefinite, è necessario apportare modifiche simili alla configurazione del client, che ha anche un valore predefinito di 32 connessioni.

- **-max-lifs-per-session**

Il numero massimo di interfacce di rete pubblicizzate per ogni sessione multicanale. L'impostazione predefinita è 256 interfacce di rete.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Abilitare SMB Multichannel sul server SMB:

```
vserver cifs options modify -vserver vserver_name -is-multichannel-enabled true
```

3. Verificare che ONTAP stia segnalando sessioni multicanale SMB:

```
vserver cifs session options show
```

4. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Esempio

Nell'esempio seguente vengono visualizzate informazioni su tutte le sessioni SMB, che mostrano più connessioni per una singola sessione:



```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                               Open
Idle
IDs      ID      Workstation      Windows User      Files
Time
-----
-----
138683,
138684,
138685    1      10.1.1.1      DOMAIN\
4s                                     Administrator
0
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate su una sessione SMB con id sessione 1:

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1

Node: node1
Session ID: 1
Connection IDs: 138683,138684,138685
Connection Count: 3
Incoming Data LIF IP Address: 192.1.1.1
Workstation IP Address: 10.1.1.1
Authentication Mechanism: NTLMv1
User Authenticated as: domain-user
Windows User: DOMAIN\administrator
UNIX User: root
Open Shares: 2
Open Files: 5
Open Other: 0
Connected Time: 5s
Idle Time: 5s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
```

### Creare volumi di dati NTFS

È necessario creare volumi di dati NTFS sulla macchina virtuale di storage (SVM) prima di poter configurare condivisioni continuamente disponibili per l'utilizzo con Hyper-V o


SQL Server su server applicazioni SMB. Utilizzare il foglio di lavoro per la configurazione del volume per creare i volumi di dati.

**A proposito di questa attività**

Per personalizzare un volume di dati, è possibile utilizzare parametri opzionali. Per ulteriori informazioni sulla personalizzazione dei volumi, vedere xref:./smb-hyper-v-sql/"Gestione dello storage logico".

Durante la creazione dei volumi di dati, non è necessario creare punti di giunzione all'interno di un volume contenente quanto segue:

- File Hyper-V per i quali ONTAP crea copie shadow
- File di database di SQL Server di cui viene eseguito il backup mediante SQL Server



Se si crea inavvertitamente un volume che utilizza uno stile di sicurezza misto o UNIX, non è possibile modificare il volume in un volume di sicurezza NTFS e utilizzarlo direttamente per creare condivisioni continuamente disponibili per operazioni senza interruzioni. Le operazioni senza interruzioni per Hyper-V e SQL Server su SMB non funzionano correttamente, a meno che i volumi utilizzati nella configurazione non vengano creati come volumi di sicurezza NTFS. È necessario eliminare il volume e ricrearlo con lo stile di protezione NTFS. In alternativa, è possibile mappare il volume su un host Windows e applicare un ACL nella parte superiore del volume e propagare l'ACL a tutti i file e cartelle del volume.

**Fasi**

1. Creare il volume di dati immettendo il comando appropriato:

Se si desidera creare un volume in una SVM in cui lo stile di sicurezza del volume root è...	Immettere il comando...
NTFS	<code>volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -junction-path path</code>
Non NTFS	<code>volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size integer[KB MB GB TB PB] -security-style ntfs -junction-path path</code>

2. Verificare che la configurazione del volume sia corretta:

```
volume show -vserver vservice_name -volume volume_name
```

**Creare condivisioni SMB continuamente disponibili**

Dopo aver creato i volumi di dati, è possibile creare le condivisioni continuamente disponibili utilizzate dai server applicazioni per accedere alla macchina virtuale Hyper-V, ai file di configurazione e ai file di database di SQL Server. È necessario utilizzare il foglio di lavoro di configurazione della condivisione per creare le condivisioni SMB.

## Fasi

1. Visualizzare informazioni sui volumi di dati esistenti e sui relativi percorsi di giunzione:

```
volume show -vserver vserver_name -junction
```

2. Creare una condivisione SMB sempre disponibile:

```
vserver cifs share create -vserver vserver_name -share-name share_name -path  
path -share-properties oplocks,continuously-available -symlink "" [-comment  
text]
```

- È possibile aggiungere un commento alla configurazione della condivisione.
  - Per impostazione predefinita, la proprietà di condivisione dei file offline è configurata sulla condivisione ed è impostata su `manual`.
  - ONTAP crea la condivisione con l'autorizzazione di condivisione predefinita di `Everyone / Full Control`.
3. Ripetere il passaggio precedente per tutte le condivisioni nel foglio di lavoro di configurazione della condivisione.
  4. Verificare che la configurazione sia corretta utilizzando `vserver cifs share show` comando.
  5. Configurare le autorizzazioni dei file NTFS sulle condivisioni continuamente disponibili mappando un disco a ciascuna condivisione e configurando le autorizzazioni dei file utilizzando la finestra **Proprietà di Windows**.

## Esempio

I seguenti comandi creano una condivisione continuamente disponibile denominata "data2" su una macchina virtuale di storage (SVM, precedentemente nota come Vserver) vs1. I collegamenti simbolici vengono disattivati impostando `-symlink` parametro a. "":

```

cluster1::> volume show -vserver vs1 -junction

```

Vserver	Volume	Active	Junction Path	Junction Path Source
vs1	data	true	/data	RW_volume
vs1	data1	true	/data/data1	RW_volume
vs1	data2	true	/data/data2	RW_volume
vs1	vs1_root	-	/	-

```

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

```

```

Vserver: vs1
Share: data2
CIFS Server NetBIOS Name: VS1
Path: /data/data2
Share Properties: oplocks
continuously-available
Symlink Properties: -
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: -
Offline Files: manual
Vscan File-Operations Profile: standard

```

## Aggiungere il privilegio SeSecurityPrivilege all'account utente (per SQL Server delle condivisioni SMB)

All'account utente di dominio utilizzato per l'installazione del server SQL deve essere assegnato il privilegio "SeSecurityPrivilege" per eseguire determinate azioni sul server CIFS che richiedono privilegi non assegnati per impostazione predefinita agli utenti di dominio.

### Di cosa hai bisogno

L'account di dominio utilizzato per l'installazione di SQL Server deve già esistere.

### A proposito di questa attività

Quando si aggiunge il privilegio all'account del programma di installazione di SQL Server, ONTAP potrebbe validare l'account contattando il controller di dominio. Il comando potrebbe non riuscire se ONTAP non riesce a contattare il controller di dominio.

### Fasi

1. Aggiungere il privilegio "SeSecurityPrivilege":

```
vserver cifs users-and-groups privilege add-privilege -vserver vserver_name  
-user-or-group-name account_name -privileges SeSecurityPrivilege
```

Il valore di `-user-or-group-name` Parameter è il nome dell'account utente di dominio utilizzato per l'installazione di SQL Server.

2. Verificare che il privilegio sia applicato all'account:

```
vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-  
group-name account_name
```

### Esempio

Il seguente comando aggiunge il privilegio "SeSecurityPrivilege" all'account del programma di installazione di SQL Server nel dominio DI ESEMPIO per la macchina virtuale di storage (SVM) vs1:

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver  
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges  
SeSecurityPrivilege
```

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
```

Vserver	User or Group Name	Privileges
vs1	EXAMPLE\SQLinstaller	SeSecurityPrivilege

### Configurare la profondità della directory della copia shadow VSS (per Hyper-V su condivisioni SMB)

Facoltativamente, è possibile configurare la profondità massima delle directory all'interno delle condivisioni SMB su cui creare le copie shadow. Questo parametro è utile se si desidera controllare manualmente il livello massimo di sottodirectory in cui ONTAP deve creare copie shadow.

#### Di cosa hai bisogno

La funzione di copia shadow del VSS deve essere attivata.

#### A proposito di questa attività

L'impostazione predefinita prevede la creazione di copie shadow per un massimo di cinque sottodirectory. Se il valore è impostato su 0, ONTAP crea copie shadow per tutte le sottodirectory.



Sebbene sia possibile specificare che la profondità della directory shadow set copy includa più di cinque sottodirectory o tutte le sottodirectory, Microsoft richiede che la creazione del set di copie shadow venga completata entro 60 secondi. La creazione del set di copie shadow non riesce se non può essere completata entro questo intervallo di tempo. La profondità della directory di copia shadow scelta non deve far superare il tempo di creazione.

### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Impostare la profondità della directory della copia shadow del VSS al livello desiderato:

```
vserver cifs options modify -vserver vserver_name -shadowcopy-dir-depth  
integer
```

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

## Gestire le configurazioni Hyper-V e SQL Server su SMB

### Configurare le condivisioni esistenti per la disponibilità continua

È possibile modificare le condivisioni esistenti per diventare condivisioni continuamente disponibili utilizzate dai server applicativi Hyper-V e SQL Server per accedere senza interruzioni ai file di configurazione e alla macchina virtuale Hyper-V e ai file di database SQL Server.

#### A proposito di questa attività

Non è possibile utilizzare una condivisione esistente come condivisione continuamente disponibile per operazioni senza interruzioni con server applicazioni su SMB se la condivisione ha le seguenti caratteristiche:

- Se il `homedirectory` la proprietà share viene impostata su tale condivisione
- Se la condivisione contiene link simbolici o `widelink` abilitati
- Se la condivisione contiene volumi congiunti al di sotto della radice della condivisione

Verificare che i due seguenti parametri di condivisione siano impostati correttamente:

- Il `-offline-files` il parametro è impostato su uno dei due `manual` (impostazione predefinita) o. `none`.
- I link simbolici devono essere disattivati.

È necessario configurare le seguenti proprietà di condivisione:

- `continuously-available`
- `oplocks`

Le seguenti proprietà di condivisione non devono essere impostate. Se sono presenti nell'elenco delle proprietà di condivisione correnti, devono essere rimosse dalla condivisione continuamente disponibile:

- `attributecache`
- `branchcache`

#### Fasi

1. Visualizza le impostazioni correnti dei parametri di condivisione e l'elenco corrente delle proprietà di condivisione configurate:

```
vserver cifs share show -vserver vserver_name -share-name share_name
```

2. Se necessario, modificare i parametri di condivisione per disattivare i collegamenti simbolici e impostare i file offline su manuale utilizzando `vserver cifs share properties modify` comando.

È possibile disattivare i collegamenti simbolici impostando il valore di `-symlink` parametro a `""`.

- È possibile disattivare i collegamenti simbolici impostando il valore di `-symlink` parametro a `""`.
- È possibile impostare `-offline-files` impostare correttamente il parametro specificando `manual`.

3. Aggiungere il `continuously-available` condividere la proprietà e, se necessario, il `oplocks` proprietà di condivisione:

```
vserver cifs share properties add -vserver vserver_name -share-name share_name  
-share-properties continuously-available[,oplock]
```

Se il `oplocks` la proprietà di condivisione non è già impostata, è necessario aggiungerla con `continuously-available` condividere la proprietà.

4. Rimuovere eventuali proprietà di condivisione non supportate nelle condivisioni a disponibilità continua:

```
vserver cifs share properties remove -vserver vserver_name -share-name  
share_name -share-properties properties[,...]
```

È possibile rimuovere una o più proprietà di condivisione specificando le proprietà di condivisione con un elenco delimitato da virgole.

5. Verificare che il `-symlink` e `-offline-files` i parametri sono impostati correttamente:

```
vserver cifs share show -vserver vserver_name -share-name share_name -fields  
symlink-properties,offline-files
```

6. Verificare che l'elenco delle proprietà di condivisione configurate sia corretto:

```
vserver cifs shares properties show -vserver vserver_name -share-name  
share_name
```

## Esempi

L'esempio seguente mostra come configurare una condivisione esistente denominata "hare1 `s`" su una macchina virtuale di storage (SVM) vs1 per NDOS con un server applicativo su SMB:

- I collegamenti simbolici vengono disattivati nella condivisione impostando `-symlink` parametro su `""`.
- Il `-offline-file` il parametro viene modificato e impostato su `manual`.
- Il `continuously-available` la proprietà share viene aggiunta alla condivisione.
- Il `oplocks` la proprietà di condivisione è già presente nell'elenco delle proprietà di condivisione, pertanto non è necessario aggiungerla.
- Il `attributecache` la proprietà share viene rimossa dalla condivisione.
- Il `browsable` La proprietà Share è opzionale per una condivisione a disponibilità continua utilizzata per NDOS con server applicazioni su SMB e viene conservata come una delle proprietà di condivisione.

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name share1
```

```

        Vserver: vs1
        Share: share1
CIFS Server NetBIOS Name: vs1
        Path: /data
    Share Properties: oplocks
                     browsable
                     attributecache
    Symlink Properties: enable
    File Mode Creation Mask: -
    Directory Mode Creation Mask: -
        Share Comment: -
        Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
        Volume Name: data
        Offline Files: documents
Vscan File-Operations Profile: standard
```

```
cluster1::> vsserver cifs share modify -vsserver vs1 -share-name share1
-offline-file manual -symlink ""
```

```
cluster1::> vsserver cifs share properties add -vsserver vs1 -share-name
share1 -share-properties continuously-available
```

```
cluster1::> vsserver cifs share properties remove -vsserver vs1 -share-name
share1 -share-properties attributecache
```

```
cluster1::> vsserver cifs share show -vsserver vs1 -share-name share1
-fields symlink-properties,offline-files
vsserver  share-name symlink-properties offline-files
```

```
-----
vs1      share1      -                      manual
```

```
cluster1::> vsserver cifs share properties show -vsserver vs1 -share-name
share1
```

```

        Vserver: vs1
        Share: share1
Share Properties: oplocks
                 browsable
                 continuously-available
```



**Abilitare o disabilitare le copie shadow VSS per i backup Hyper-V su SMB**

Se si utilizza un'applicazione di backup VSS-aware per eseguire il backup dei file di macchine virtuali Hyper-V memorizzati nelle condivisioni SMB, è necessario attivare la copia shadow VSS. Se non si utilizzano applicazioni di backup compatibili con VSS, è possibile disattivare la copia shadow del VSS. L'impostazione predefinita prevede l'attivazione della copia shadow del VSS.

**A proposito di questa attività**

È possibile attivare o disattivare le copie shadow VSS in qualsiasi momento.

**Fasi**

- 1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

- 2. Eseguire una delle seguenti operazioni:

Se si desidera che le copie shadow di VSS siano...	Immettere il comando...
Attivato	<code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled true</code>
Disattivato	<code>vserver cifs options modify -vserver vserver_name -shadowcopy-enabled false</code>

- 3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

**Esempio**

I seguenti comandi abilitano le copie shadow VSS su SVM vs1:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

## Utilizza le statistiche per monitorare l'attività di Hyper-V e SQL Server su SMB

### Determinare quali oggetti e contatori statistici sono disponibili

Prima di ottenere informazioni su CIFS, SMB, audit e statistiche hash BranchCache e monitorare le performance, è necessario sapere quali oggetti e contatori sono disponibili per ottenere i dati.

#### Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Eseguire una delle seguenti operazioni:

Se si desidera determinare...	Inserisci...
Quali oggetti sono disponibili	<b>statistics catalog object show</b>
Oggetti specifici disponibili	<b>statistics catalog object show object <i>object_name</i></b>
Quali contatori sono disponibili	<b>statistics catalog counter show object <i>object_name</i></b>

Per ulteriori informazioni sugli oggetti e i contatori disponibili, consultare le pagine man.

3. Tornare al livello di privilegio admin:

```
set -privilege admin
```

#### Esempi

Il seguente comando visualizza le descrizioni degli oggetti statistici selezionati relativi all'accesso CIFS e SMB nel cluster, come si vede al livello di privilegio avanzato:

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog object show -object audit
      audit_ng          CM object for exporting audit_ng
performance counters
```

```
cluster1::*> statistics catalog object show -object cifs
      cifs              The CIFS object reports activity of the
                        Common Internet File System protocol
                        ...
```

```
cluster1::*> statistics catalog object show -object nblade_cifs
      nblade_cifs       The Common Internet File System (CIFS)
                        protocol is an implementation of the
Server
                        ...
```

```
cluster1::*> statistics catalog object show -object smb1
      smb1              These counters report activity from the
SMB
                        revision of the protocol. For information
                        ...
```

```
cluster1::*> statistics catalog object show -object smb2
      smb2              These counters report activity from the
                        SMB2/SMB3 revision of the protocol. For
                        ...
```

```
cluster1::*> statistics catalog object show -object hashd
      hashd             The hashd object provides counters to
measure
                        the performance of the BranchCache hash
daemon.
```

```
cluster1::*> set -privilege admin
```

Il seguente comando visualizza informazioni su alcuni contatori di `cifs` oggetto visto a livello di privilegi avanzati:



In questo esempio non vengono visualizzati tutti i contatori disponibili per `cifs` oggetto; l'output è troncato.

```
cluster1::> set -privilege advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by support personnel.

Do you want to continue? {y|n}: y

```
cluster1::*> statistics catalog counter show -object cifs
```

Object: cifs

Counter	Description
active_searches	Number of active searches over SMB and SMB2
auth_reject_too_many	Authentication refused after too many requests were made in rapid succession
avg_directory_depth	Average number of directories crossed by SMB and SMB2 path-based commands
...	...

```
cluster2::> statistics start -object client -sample-id
```

Object: client

Counter	Value
cifs_ops	0
cifs_read_ops	0
cifs_read_recv_ops	0
cifs_read_recv_size	0B
cifs_read_size	0B
cifs_write_ops	0
cifs_write_recv_ops	0
cifs_write_recv_size	0B
cifs_write_size	0B
instance_name	vserver_1:10.72.205.179
instance_uuid	2:10.72.205.179
local_ops	0
mount_ops	0

[...]

## Visualizzare le statistiche SMB

È possibile visualizzare varie statistiche SMB per monitorare le performance e

diagnosticare i problemi.

## Fasi

1. Utilizzare `statistics start` e opzionale `statistics stop` comandi per raccogliere un campione di dati.
2. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le statistiche per...	Immettere il seguente comando...
Tutte le versioni di SMB	<code>statistics show -object cifs</code>
SMB 1.0	<code>statistics show -object smb1</code>
SMB 2.x e SMB 3.0	<code>statistics show -object smb2</code>
Sottosistema SMB del nodo	<code>statistics show -object nblade_cifs</code>

Scopri di più su `statistics` comandi:

- ["vengono visualizzate le statistiche"](#)
- ["le statistiche iniziano"](#)
- ["le statistiche si interrompono"](#)

## Verificare che la configurazione sia in grado di eseguire operazioni senza interruzioni

**Utilizzare il monitoraggio dello stato di salute per determinare se lo stato delle operazioni senza interruzioni è integro**

Il monitoraggio dello stato di salute fornisce informazioni sullo stato di salute del sistema nel cluster. Il monitor dello stato di salute monitora le configurazioni di Hyper-V e SQL Server su SMB per garantire operazioni senza interruzioni (NDOS) per gli application server. Se lo stato è degradato, è possibile visualizzare i dettagli del problema, incluse la probabile causa e le azioni di ripristino consigliate.

Sono disponibili diversi monitor di stato. ONTAP monitora sia lo stato generale del sistema che lo stato di salute dei singoli monitor. Il monitor di stato della connettività del nodo contiene il sottosistema CIFS-NDO. Il monitor dispone di una serie di policy di salute che attivano avvisi se determinate condizioni fisiche possono causare interruzioni e, se esiste una condizione di interruzione, genera avvisi e fornisce informazioni sulle azioni correttive. Per le configurazioni NDO su SMB, vengono generati avvisi per le due seguenti condizioni:

ID avviso	Severità	Condizione
<b>HaNotReadyCifsNdo_Alert</b>	Maggiore	Uno o più file ospitati da un volume in un aggregato sul nodo sono stati aperti attraverso una condivisione SMB continuamente disponibile con la promessa di persistenza in caso di guasto; tuttavia, la relazione ha con il partner non è configurata o non è integro.
<b>NoStandbyLifCifsNdo_Alert</b>	Minore	La macchina virtuale di storage (SVM) sta fornendo attivamente i dati tramite SMB attraverso un nodo e ci sono file SMB aperti in modo persistente su condivisioni continuamente disponibili; tuttavia, il nodo partner non sta esponendo alcun LIF di dati attivo per SVM.

### Visualizzazione dello stato delle operazioni senza interruzioni mediante il monitoraggio dello stato di salute del sistema

È possibile utilizzare `system health` Comandi per visualizzare informazioni sullo stato generale del sistema del cluster e sullo stato del sottosistema CIFS-NDO, per rispondere agli avvisi, per configurare gli avvisi futuri e per visualizzare informazioni sulla configurazione del monitoraggio dello stato di salute.

#### Fasi

1. Monitorare lo stato di salute eseguendo l'azione appropriata:

Se si desidera visualizzare...	Immettere il comando...
Lo stato di salute del sistema, che riflette lo stato generale dei singoli monitor di salute	<b>system health status show</b>
Informazioni sullo stato di salute del sottosistema CIFS-NDO	<b>system health subsystem show -subsystem CIFS-NDO -instance</b>

2. Visualizzare le informazioni sulla configurazione del monitoraggio degli avvisi CIFS-NDO eseguendo le azioni appropriate:

Se si desidera visualizzare informazioni su...	Immettere il comando...
La configurazione e lo stato del monitor di stato per il sottosistema CIFS-NDO, ad esempio i nodi monitorati, lo stato di inizializzazione e lo stato	<b>system health config show -subsystem CIFS-NDO</b>

Se si desidera visualizzare informazioni su...	Immettere il comando...
CIFS-NDO avvisa che un monitor di stato può potenzialmente generare	<b>system health alert definition show -subsystem CIFS-NDO</b>
Criteri di monitoraggio dello stato CIFS-NDO, che determinano quando vengono generati gli avvisi	<b>system health policy definition show -monitor node-connect</b>



Utilizzare `-instance` per visualizzare informazioni dettagliate.

## Esempi

Il seguente output mostra informazioni sullo stato di salute generale del cluster e del sottosistema CIFS-NDO:

```
cluster1::> system health status show
Status
-----
ok

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                Subsystem: CIFS-NDO
                Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
  Number of Suppressed Alerts: 0
                Node: node2
  Subsystem Refresh Interval: 5m
```

Il seguente output mostra informazioni dettagliate sulla configurazione e lo stato del monitor di stato del sottosistema CIFS-NDO:

```

cluster1::> system health config show -subsystem CIFS-NDO -instance

Node: node1
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

Node: node2
Monitor: node-connect
Subsystem: SAS-connect, HA-health, CIFS-NDO
Health: ok
Monitor Version: 2.0
Policy File Version: 1.0
Context: node_context
Aggregator: system-connect
Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

```

### Verificare la configurazione della condivisione SMB continuamente disponibile

Per supportare operazioni senza interruzioni, le condivisioni SMB di Hyper-V e SQL Server devono essere configurate come condivisioni a disponibilità continua. Inoltre, è necessario controllare alcune altre impostazioni di condivisione. È necessario verificare che le condivisioni siano configurate correttamente per fornire operazioni senza interruzioni per i server di applicazioni in caso di eventi di interruzione pianificati o non pianificati.

#### A proposito di questa attività

Verificare che i due seguenti parametri di condivisione siano impostati correttamente:



- Il `-offline-files` il parametro è impostato su uno dei due `manual` (impostazione predefinita) o. `none`.
- I link simbolici devono essere disattivati.

Per operazioni corrette senza interruzioni, è necessario impostare le seguenti proprietà di condivisione:

- `continuously-available`
- `oplocks`

Le seguenti proprietà di condivisione non devono essere impostate:

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

### Fasi

1. Verificare che i file offline siano impostati su `manual` oppure `disabled` e che i link simbolici sono disabilitati:

```
vserver cifs shares show -vserver vserver_name
```

2. Verificare che le condivisioni SMB siano configurate per la disponibilità continua:

```
vserver cifs shares properties show -vserver vserver_name
```

### Esempi

Nell'esempio seguente viene visualizzata l'impostazione di condivisione per una condivisione denominata "share1" su una macchina virtuale di storage (SVM, precedentemente nota come Vserver) `vs1`. I file offline sono impostati su `manual` i collegamenti simbolici e sono disattivati (indicati da un trattino in `Symlink Properties` output di campo):

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
      Vserver: vs1
      Share: share1
      CIFS Server NetBIOS Name: VS1
      Path: /data/share1
      Share Properties: oplocks
                      continuously-available
      Symlink Properties: -
      File Mode Creation Mask: -
      Directory Mode Creation Mask: -
      Share Comment: -
      Share ACL: Everyone / Full Control
      File Attribute Cache Lifetime: -
      Volume Name: -
      Offline Files: manual
      Vscan File-Operations Profile: standard
```

Nell'esempio seguente vengono visualizzate le proprietà di condivisione di una condivisione denominata "share1" su SVM vs1:

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver      Share      Properties
-----
vs1          share1    oplocks
                      continuously-available
```

## Verificare lo stato LIF

Anche se si configurano le macchine virtuali di storage (SVM) con configurazioni Hyper-V e SQL Server su SMB in modo che dispongano di LIF su ciascun nodo di un cluster, durante le operazioni quotidiane, alcune LIF potrebbero spostarsi sulle porte di un altro nodo. È necessario verificare lo stato LIF e intraprendere le azioni correttive necessarie.

### A proposito di questa attività

Per fornire un supporto operativo senza interruzioni, ciascun nodo di un cluster deve disporre di almeno una LIF per la SVM e tutte le LIF devono essere associate a una porta home. Se alcune delle LIF configurate non sono attualmente associate alla porta home, è necessario risolvere eventuali problemi di porta e ripristinare le LIF alla porta home.

### Fasi

1. Visualizzare le informazioni sui LIF configurati per SVM:

```
network interface show -vserver vserver_name
```

In questo esempio, "lif1" non si trova sulla porta home.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
vs1	lif1	up/up	10.0.0.128/24	node2	e0d
false	lif2	up/up	10.0.0.129/24	node2	e0d
true					

2. Se alcune delle LIF non si trovano sulle porte home, attenersi alla seguente procedura:

a. Per ogni LIF, determinare quale sia la porta home di LIF:

```
network interface show -vserver vserver_name -lif lif_name -fields home-node,home-port
```

```
network interface show -vserver vs1 -lif lif1 -fields home-node,home-port
```

vserver	lif	home-node	home-port
-----	----	-----	-----
vs1	lif1	node1	e0d

b. Per ciascun LIF, determinare se la porta home del LIF è attiva:

```
network port show -node node_name -port port -fields port,link
```

```
network port show -node node1 -port e0d -fields port,link
```

node	port	link
-----	----	----
node1	e0d	up

+

In questo esempio, “lif1” deve essere nuovamente migrato alla porta home, node1:e0d.

3. Se una delle interfacce di rete della porta home a cui devono essere associate le LIF non si trovano in up risolvere il problema in modo che queste interfacce siano in funzione.

4. Se necessario, ripristinare le LIF alle porte home:

```
network interface revert -vserver vserver_name -lif lif_name
```

```
network interface revert -vserver vs1 -lif lif1
```

5. Verificare che ciascun nodo del cluster disponga di una LIF attiva per SVM:

```
network interface show -vserver vserver_name
```

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
-----	-----	-----	-----	-----	-----	-----
----						
vs1						
	lif1	up/up	10.0.0.128/24	node1	e0d	
true						
	lif2	up/up	10.0.0.129/24	node2	e0d	
true						

## Determinare se le sessioni SMB sono continuamente disponibili

### Visualizzare le informazioni sulla sessione SMB

È possibile visualizzare informazioni sulle sessioni SMB stabilite, tra cui la connessione SMB, l'ID della sessione e l'indirizzo IP della workstation che utilizza la sessione. È possibile visualizzare informazioni sulla versione del protocollo SMB della sessione e sul livello di protezione continuamente disponibile, per identificare se la sessione supporta operazioni senza interruzioni.

### A proposito di questa attività

È possibile visualizzare le informazioni relative a tutte le sessioni della SVM in forma di riepilogo. Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali:

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output relativo ai campi scelti.

È possibile immettere `-fields ?` per determinare quali campi è possibile utilizzare.

- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sulle sessioni SMB stabilite.
- È possibile utilizzare `-fields` o il `-instance` parametro da solo o in combinazione con altri parametri opzionali.

### Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare le informazioni sulla sessione SMB...	Immettere il seguente comando...
Per tutte le sessioni su SVM in forma di riepilogo	<b>vserver cifs session show -vserver <i>vserver_name</i></b>
Su un ID di connessione specificato	<b>vserver cifs session show -vserver <i>vserver_name</i> -connection-id integer</b>
Da un indirizzo IP della workstation specificato	<b>vserver cifs session show -vserver <i>vserver_name</i> -address <i>workstation_IP_address</i></b>
Su un indirizzo IP LIF specificato	<b>vserver cifs session show -vserver <i>vserver_name</i> -lif -address <i>LIF_IP_address</i></b>
Su un nodo specificato	<b><i>**vserver cifs session show -vserver vserver_name -node {node_name</i></b>
<b>local}**</b>	Da un utente Windows specificato
<b>vserver cifs session show -vserver <i>vserver_name</i> -windows-user <i>user_name</i></b>  Il formato per <i>user_name</i> è <i>[domain]\user</i> .	Con un meccanismo di autenticazione specificato

Se si desidera visualizzare le informazioni sulla sessione SMB...	Immettere il seguente comando...
<pre> <b>vserver cifs</b> <b>session show</b> <b>-vserver</b> <b>vserver_name -auth</b> <b>-mechanism</b> <b>authentication_mec</b> <b>hanism</b> </pre> <p>Il valore per <code>-auth</code>  <code>-mechanism</code> può essere  uno dei seguenti:</p> <ul style="list-style-type: none"> <li>• NTLMv1</li> <li>• NTLMv2</li> <li>• Kerberos</li> <li>• Anonymous</li> </ul>	Con una versione del protocollo specificata

Se si desidera visualizzare le informazioni sulla sessione SMB...

Immettere il seguente comando...

```
vserver cifs  
session show  
-vserver  
vserver_name  
-protocol-version  
protocol_version
```

Con un livello specifico di protezione a disponibilità continua

Il valore per `-protocol-version` può essere uno dei seguenti:

- SMB1
- SMB2
- SMB2\_1
- SMB3
- SMB3\_1

Se si desidera visualizzare le informazioni sulla sessione SMB...	Immettere il seguente comando...
<pre> <b>vserver cifs</b> <b>session show</b> <b>-vserver</b> <b>vserver_name</b> <b>-continuously</b> <b>-available</b> <b>continuously_avail</b> <b>able_protection_le</b> <b>vel</b> </pre> <p>Il valore per          -continuously          -available può essere          uno dei seguenti:</p> <ul style="list-style-type: none"> <li>• No</li> <li>• Yes</li> <li>• Partial</li> </ul>	Con uno stato di sessione SMB Signing specificato



Esempi

Il seguente comando visualizza le informazioni sulla sessione per le sessioni su SVM vs1 stabilite da una workstation con indirizzo IP 10.1.1.1:

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:      node1
Vserver:   vs1
Connection Session
ID          ID      Workstation      Windows User      Open      Idle
-----
3151272279,
3151272280,
3151272281  1        10.1.1.1        DOMAIN\joe        2         23s
```

Il seguente comando visualizza informazioni dettagliate sulla sessione per le sessioni con protezione continuamente disponibile su SVM vs1. La connessione è stata effettuata utilizzando l'account di dominio.

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

Node: node1
Vserver: vs1
Session ID: 1
Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
Workstation IP address: 10.1.1.2
Authentication Mechanism: Kerberos
Windows User: DOMAIN\SERVER1$
UNIX User: pcuser
Open Shares: 1
Open Files: 1
Open Other: 0
Connected Time: 10m 43s
Idle Time: 1m 19s
Protocol Version: SMB3
Continuously Available: Yes
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

Il seguente comando visualizza le informazioni di sessione su una sessione che utilizza SMB 3.0 e SMB Multichannel su SVM vs1. Nell'esempio, l'utente si è connesso a questa condivisione da un client SMB 3.0 utilizzando l'indirizzo IP LIF; pertanto, il meccanismo di autenticazione è stato impostato su NTLMv2 per impostazione predefinita. La connessione deve essere effettuata utilizzando l'autenticazione Kerberos per

connettersi con la protezione continuamente disponibile.

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

Node: node1
Vserver: vs1
Session ID: 1
**Connection IDs: 3151272607,31512726078,3151272609
Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
Workstation IP address: 10.1.1.3
Authentication Mechanism: NTLMv2
Windows User: DOMAIN\administrator
UNIX User: pcuser
Open Shares: 1
Open Files: 0
Open Other: 0
Connected Time: 6m 22s
Idle Time: 5m 42s
Protocol Version: SMB3
Continuously Available: No
Is Session Signed: false
User Authenticated as: domain-user
NetBIOS Name: -
SMB Encryption Status: Unencrypted
```

#### Visualizzare le informazioni sui file SMB aperti

È possibile visualizzare informazioni sui file SMB aperti, tra cui la connessione SMB e l'ID sessione, il volume di hosting, il nome della condivisione e il percorso di condivisione. È inoltre possibile visualizzare informazioni sul livello di protezione continuamente disponibile di un file, utile per determinare se un file aperto si trova in uno stato che supporta operazioni senza interruzioni.

#### A proposito di questa attività

È possibile visualizzare informazioni sui file aperti in una sessione SMB stabilita. Le informazioni visualizzate sono utili quando è necessario determinare le informazioni della sessione SMB per determinati file all'interno di una sessione SMB.

Ad esempio, se si dispone di una sessione SMB in cui alcuni dei file aperti sono aperti con una protezione continuamente disponibile e alcuni non sono aperti con una protezione continuamente disponibile (il valore per `-continuously-available` campo in `vserver cifs session show` l'output del comando è `Partial`), è possibile determinare quali file non sono continuamente disponibili utilizzando questo comando.

È possibile visualizzare le informazioni relative a tutti i file aperti nelle sessioni SMB stabilite sulle macchine virtuali di storage (SVM) in forma riepilogativa utilizzando `vserver cifs session file show` senza parametri opzionali.


Tuttavia, in molti casi, la quantità di output restituita è elevata. È possibile personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali. Ciò può essere utile quando si desidera visualizzare informazioni solo per un piccolo sottoinsieme di file aperti.

- È possibile utilizzare il opzionale `-fields` parametro per visualizzare l'output nei campi scelti.  
È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.
- È possibile utilizzare `-instance` Parametro per visualizzare informazioni dettagliate sui file SMB aperti.  
È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.

## Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera visualizzare i file SMB aperti...	Immettere il seguente comando...
Sul modulo SVM in forma di riepilogo	<b><code>vserver cifs session file show -vserver vserver_name</code></b>
Su un nodo specificato	<code>`*vserver cifs session file show -vserver vserver_name -node {node_name</code>
<code>local}*</code>	Su un ID file specificato
<b><code>vserver cifs session file show -vserver vserver_name -file-id integer</code></b>	Su un ID connessione SMB specificato
<b><code>vserver cifs session file show -vserver vserver_name -connection-id integer</code></b>	Su un ID sessione SMB specificato
<b><code>vserver cifs session file show -vserver vserver_name -session-id integer</code></b>	Sull'aggregato di hosting specificato
<b><code>vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name</code></b>	Sul volume specificato
<b><code>vserver cifs session file show -vserver vserver_name -hosting-volume volume_name</code></b>	Sulla condivisione SMB specificata
<b><code>vserver cifs session file show -vserver vserver_name -share share_name</code></b>	Sul percorso SMB specificato

Se si desidera visualizzare i file SMB aperti...	Immettere il seguente comando...
<b>vserver cifs session file show</b> <b>-vserver <i>vserver_name</i> -path <i>path</i></b>	Con il livello specificato di protezione a disponibilità continua
<b>vserver cifs session file show</b> <b>-vserver <i>vserver_name</i> -continuously</b> <b>-available</b> <b><i>continuously_available_status</i></b>  Il valore per <code>-continuously-available</code> può essere uno dei seguenti: <ul style="list-style-type: none"> <li>• No</li> <li>• Yes</li> </ul> <div>  <p>Se lo stato di disponibilità continua è No, questo significa che questi file aperti non sono in grado di eseguire il ripristino senza interruzioni dal takeover e dal giveback. Inoltre, non possono essere ripristinati dal trasferimento generale di aggregati tra partner in una relazione ad alta disponibilità.</p> </div>	Con lo stato di riconnessione specificato

Sono disponibili ulteriori parametri opzionali che è possibile utilizzare per perfezionare i risultati di output. Per ulteriori informazioni, consulta la pagina `man`.

## Esempi

Nell'esempio seguente vengono visualizzate informazioni sui file aperti su SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1
Node:      node1
Vserver:   vs1
Connection: 3151274158
Session:    1
File      File      Open Hosting      Continuously
ID        Type        Mode Volume      Share      Available
-----
41        Regular    r    data      data      Yes
Path: \mytest.rtf
```

Nell'esempio seguente vengono visualizzate informazioni dettagliate sui file SMB aperti con ID file 82 su SVM vs1:

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance
```

```
        Node: node1
        Vserver: vs1
        File ID: 82
    Connection ID: 104617
        Session ID: 1
        File Type: Regular
        Open Mode: rw
Aggregate Hosting File: aggr1
    Volume Hosting File: data1
        CIFS Share: data1
    Path from CIFS Share: windows\win8\test\test.txt
        Share Mode: rw
        Range Locks: 1
Continuously Available: Yes
        Reconnected: No
```

# Gestione dello storage SAN

## Concetti SAN

### Provisioning SAN con iSCSI

Negli ambienti SAN, i sistemi storage sono destinazioni che dispongono di dispositivi di destinazione dello storage. Per iSCSI e FC, i dispositivi di destinazione dello storage sono denominati LUN (unità logiche). Per NVMe (non-volatile Memory Express) su Fibre Channel, i dispositivi di destinazione dello storage vengono definiti namespace.

È possibile configurare lo storage creando LUN per iSCSI e FC o spazi dei nomi per NVMe. Gli host accedono quindi ai LUN o agli spazi dei nomi utilizzando le reti con protocollo iSCSI (Internet Small computer Systems Interface) o FC (Fibre Channel).

Per connettersi alle reti iSCSI, gli host possono utilizzare schede di rete Ethernet (NIC) standard, schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o HBA (host bus adapter) iSCSI dedicati.

Per connettersi alle reti FC, gli host richiedono HBA o CNA FC.

I protocolli FC supportati includono:

- FC
- FCoE
- NVMe

### Nomi e connessioni di rete del nodo di destinazione iSCSI

I nodi di destinazione iSCSI possono connettersi alla rete in diversi modi:

- Interfacce su Ethernet che utilizzano software integrato in ONTAP.
- Su più interfacce di sistema, con un'interfaccia utilizzata per iSCSI che può anche trasmettere il traffico per altri protocolli, come SMB e NFS.
- Utilizzando un adattatore di destinazione unificato (UTA) o un adattatore di rete convergente (CNA).

Ogni nodo iSCSI deve avere un nome di nodo.

I due formati, o designatori di tipo, per i nomi dei nodi iSCSI sono *iqn* e *eui*. La destinazione iSCSI SVM utilizza sempre il designatore di tipo *iqn*. L'iniziatore può utilizzare il designatore di tipo *iqn* o *eui*.

### Nome del nodo del sistema di storage

Ogni SVM che esegue iSCSI ha un nome di nodo predefinito basato su un nome di dominio inverso e un numero di codifica univoco.

Il nome del nodo viene visualizzato nel seguente formato:

`iqn.1992-08.com.netapp:sn.unique-encoding-number`

L'esempio seguente mostra il nome del nodo predefinito per un sistema di storage con un numero di codifica

univoco:

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

## Porta TCP per iSCSI

Il protocollo iSCSI è configurato in ONTAP per utilizzare la porta TCP numero 3260.

ONTAP non supporta la modifica del numero di porta per iSCSI. La porta numero 3260 è registrata come parte della specifica iSCSI e non può essere utilizzata da altre applicazioni o servizi.

### Informazioni correlate

["Documentazione NetApp: Configurazione host SAN ONTAP"](#)

## Gestione dei servizi iSCSI

### Gestione dei servizi iSCSI

È possibile gestire la disponibilità del servizio iSCSI sulle interfacce logiche iSCSI della macchina virtuale di storage (SVM) utilizzando `vserver iscsi interface enable` oppure `vserver iscsi interface disable` comandi.

Per impostazione predefinita, il servizio iSCSI è attivato su tutte le interfacce logiche iSCSI.

### Come viene implementato iSCSI sull'host

iSCSI può essere implementato sull'host utilizzando hardware o software.

È possibile implementare iSCSI in uno dei seguenti modi:

- Utilizzo di un software initiator che utilizza le interfacce Ethernet standard dell'host.
- Tramite un HBA (host bus adapter) iSCSI: Un HBA iSCSI viene visualizzato nel sistema operativo host come un adattatore disco SCSI con dischi locali.
- Utilizzando un adattatore TCP Offload Engine (TOE) che scarica l'elaborazione TCP/IP.

L'elaborazione del protocollo iSCSI viene ancora eseguita dal software host.

### Come funziona l'autenticazione iSCSI

Durante la fase iniziale di una sessione iSCSI, l'iniziatore invia una richiesta di accesso al sistema di storage per avviare una sessione iSCSI. Il sistema di storage quindi consente o nega la richiesta di accesso o determina che non è richiesto un accesso.

I metodi di autenticazione iSCSI sono:

- Challenge Handshake Authentication Protocol (CHAP): L'iniziatore effettua l'accesso utilizzando un nome utente e una password CHAP.

È possibile specificare una password CHAP o generare una password segreta esadecimale. Esistono due tipi di nomi utente e password CHAP:

- Inbound — il sistema storage autentica l'iniziatore.

Se si utilizza l'autenticazione CHAP, sono necessarie le impostazioni in entrata.

- Outbound (in uscita) - questa è un'impostazione opzionale che consente all'iniziatore di autenticare il sistema di storage.

È possibile utilizzare le impostazioni in uscita solo se si definiscono un nome utente e una password in entrata nel sistema di storage.

- Nega: All'iniziatore viene negato l'accesso al sistema di storage.
- Nessuno: Il sistema storage non richiede l'autenticazione per l'iniziatore.

È possibile definire l'elenco degli iniziatori e i relativi metodi di autenticazione. È inoltre possibile definire un metodo di autenticazione predefinito che si applica agli iniziatori non presenti nell'elenco.

### Informazioni correlate

["Opzioni di multipathing Windows con Data ONTAP: Fibre Channel e iSCSI"](#)

### Gestione della sicurezza di iSCSI Initiator

ONTAP offre una serie di funzionalità per la gestione della sicurezza per gli iniziatori iSCSI. È possibile definire un elenco di iniziatori iSCSI e il metodo di autenticazione per ciascuno di essi, visualizzare gli iniziatori e i relativi metodi di autenticazione nell'elenco di autenticazione, aggiungere e rimuovere gli iniziatori dall'elenco di autenticazione e definire il metodo di autenticazione iSCSI Initiator predefinito per gli iniziatori non presenti nell'elenco.

### Isolamento degli endpoint iSCSI

A partire da ONTAP 9.1, i comandi di sicurezza iSCSI esistenti sono stati migliorati per accettare un intervallo di indirizzi IP o più indirizzi IP.

Tutti gli iniziatori iSCSI devono fornire indirizzi IP di origine quando si stabilisce una sessione o una connessione con una destinazione. Questa nuova funzionalità impedisce a un iniziatore di accedere al cluster se l'indirizzo IP di origine non è supportato o è sconosciuto, fornendo uno schema di identificazione univoco. Qualsiasi iniziatore che ha origine da un indirizzo IP non supportato o sconosciuto avrà il proprio login rifiutato nel layer di sessione iSCSI, impedendo all'iniziatore di accedere a qualsiasi LUN o volume all'interno del cluster.

Implementare questa nuova funzionalità con due nuovi comandi per gestire le voci preesistenti.

### Aggiungere l'intervallo di indirizzi dell'iniziatore

Migliorare la gestione della sicurezza di iSCSI Initiator aggiungendo un intervallo di indirizzi IP o più indirizzi IP con `vserver iscsi security add-initiator-address-range` comando.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

### Rimuovere l'intervallo di indirizzi dell'iniziatore

Rimuovere un intervallo di indirizzi IP o più indirizzi IP con `vserver iscsi security remove-`



initiator-address-range comando.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

## Che cos'è l'autenticazione CHAP

Il protocollo CHAP (Challenge Handshake Authentication Protocol) consente la comunicazione autenticata tra gli iniziatori iSCSI e le destinazioni. Quando si utilizza l'autenticazione CHAP, si definiscono i nomi utente e le password CHAP sia sull'iniziatore che sul sistema di storage.

Durante la fase iniziale di una sessione iSCSI, l'iniziatore invia una richiesta di accesso al sistema di storage per iniziare la sessione. La richiesta di accesso include il nome utente CHAP dell'iniziatore e l'algoritmo CHAP. Il sistema storage risponde con una sfida CHAP. L'iniziatore fornisce una risposta CHAP. Il sistema storage verifica la risposta e autentica l'iniziatore. La password CHAP viene utilizzata per calcolare la risposta.

## Linee guida per l'utilizzo dell'autenticazione CHAP

Quando si utilizza l'autenticazione CHAP, seguire alcune linee guida.

- Se si definiscono un nome utente e una password in entrata nel sistema di storage, è necessario utilizzare lo stesso nome utente e password per le impostazioni CHAP in uscita sull'iniziatore. Se si definiscono anche un nome utente e una password in uscita sul sistema di storage per abilitare l'autenticazione bidirezionale, è necessario utilizzare lo stesso nome utente e la stessa password per le impostazioni CHAP in entrata sull'iniziatore.
- Non è possibile utilizzare lo stesso nome utente e password per le impostazioni in entrata e in uscita sul sistema di storage.
- I nomi utente CHAP possono essere da 1 a 128 byte.

Non è consentito un nome utente nullo.

- Le password CHAP (segreto) possono essere da 1 a 512 byte.

Le password possono essere valori esadecimali o stringhe. Per i valori esadecimali, inserire il valore con il prefisso "0x" o "0X". Non è consentita una password nulla.

ONTAP consente l'utilizzo di caratteri speciali, lettere non inglesi, numeri e spazi per le password CHAP (segreti). Tuttavia, questo è soggetto a restrizioni per l'host. Se uno di questi non è consentito dal tuo host specifico, non può essere utilizzato.



Ad esempio, l'iniziatore software iSCSI Microsoft richiede che le password CHAP di destinazione e di iniziatore siano almeno 12 byte se non viene utilizzata la crittografia IPsec. La lunghezza massima della password è di 16 byte, indipendentemente dall'utilizzo o meno di IPsec.

Per ulteriori restrizioni, consultare la documentazione dell'iniziatore.

## L'utilizzo degli elenchi di accesso alle interfacce iSCSI per limitare le interfacce initiator può aumentare le performance e la sicurezza

Gli elenchi DI accesso alle interfacce iSCSI possono essere utilizzati per limitare il numero di LIF in una SVM a cui un iniziatore può accedere, aumentando in tal modo le

performance e la sicurezza.

Quando un iniziatore avvia una sessione di rilevamento utilizzando un iSCSI `SendTargets` Riceve gli indirizzi IP associati alla LIF (interfaccia di rete) presente nell'elenco degli accessi. Per impostazione predefinita, tutti gli iniziatori hanno accesso a tutte le LIF iSCSI nella SVM. È possibile utilizzare l'elenco di accesso per limitare il numero di LIF in una SVM a cui un iniziatore ha accesso.

### **iSNS (Internet Storage Name Service)**

Internet Storage Name Service (iSNS) è un protocollo che consente il rilevamento e la gestione automatici dei dispositivi iSCSI su una rete di storage TCP/IP. Un server iSNS conserva informazioni sui dispositivi iSCSI attivi sulla rete, inclusi i relativi indirizzi IP, i nomi dei nodi iSCSI IQN e i gruppi di portali.

È possibile ottenere un server iSNS da un fornitore di terze parti. Se si dispone di un server iSNS sulla rete configurato e abilitato per l'utilizzo da parte dell'iniziatore e della destinazione, è possibile utilizzare la LIF di gestione per una macchina virtuale di storage (SVM) per registrare tutte le LIF iSCSI per tale SVM sul server iSNS. Una volta completata la registrazione, iSCSI Initiator può eseguire una query sul server iSNS per rilevare tutte le LIF relative a una specifica SVM.

Se si decide di utilizzare un servizio iSNS, è necessario assicurarsi che le macchine virtuali dello storage (SVM) siano registrate correttamente con un server iSNS (Internet Storage Name Service).

Se non si dispone di un server iSNS sulla rete, è necessario configurare manualmente ciascuna destinazione in modo che sia visibile all'host.

#### **Cosa fa un server iSNS**

Un server iSNS utilizza il protocollo iSNS (Internet Storage Name Service) per mantenere le informazioni sui dispositivi iSCSI attivi sulla rete, inclusi i relativi indirizzi IP, i nomi dei nodi iSCSI (IQN) e i gruppi di portali.

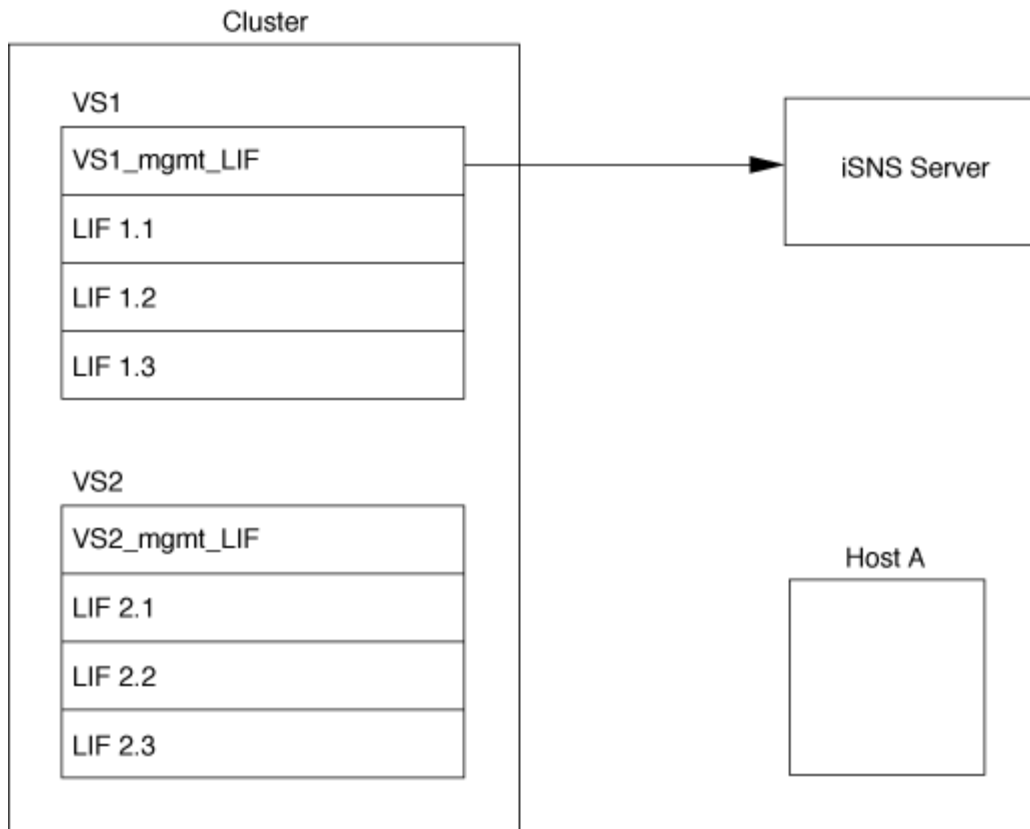
Il protocollo iSNS consente il rilevamento e la gestione automatizzati dei dispositivi iSCSI su una rete di storage IP. Un iniziatore iSCSI può eseguire query sul server iSNS per rilevare i dispositivi di destinazione iSCSI.

NetApp non fornisce o rivende server iSNS. È possibile ottenere questi server da un vendor supportato da NetApp.

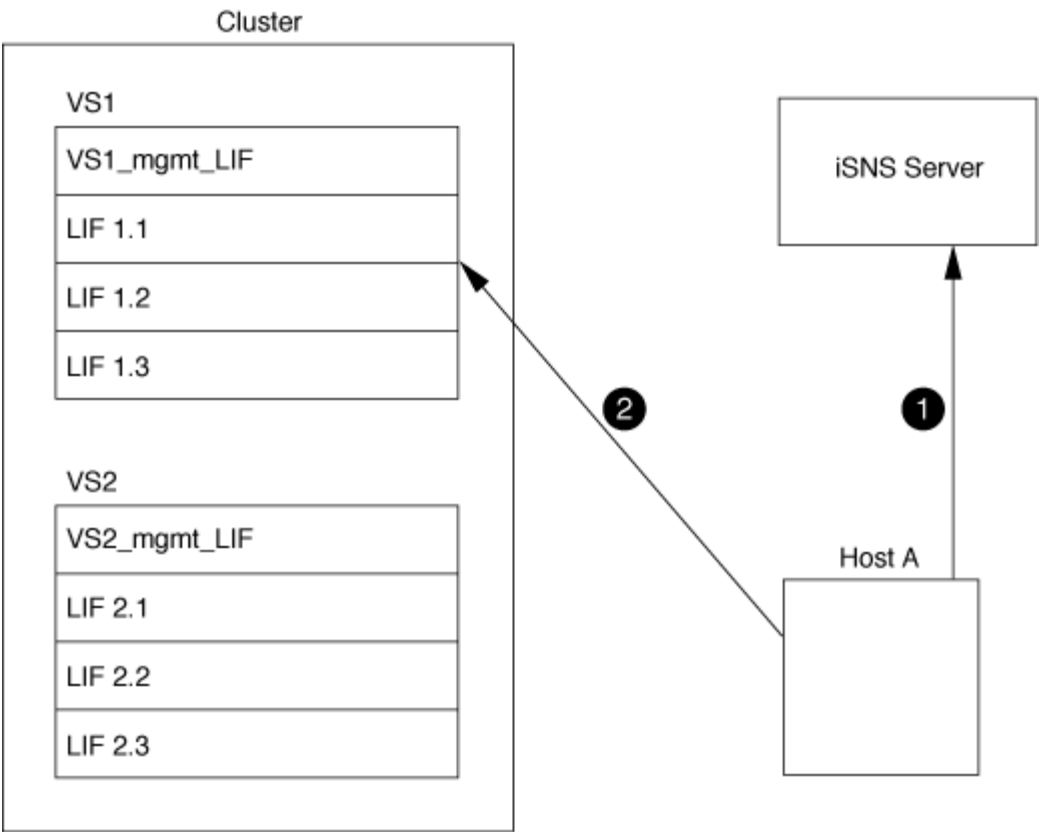
#### **Come le SVM interagiscono con un server iSNS**

Il server iSNS comunica con ciascuna macchina virtuale di storage (SVM) attraverso la LIF di gestione SVM. La LIF di gestione registra tutte le informazioni relative a nome, alias e portale del nodo di destinazione iSCSI con il servizio iSNS per una SVM specifica.

Nell'esempio seguente, SVM "VS1" utilizza la LIF di gestione SVM "VS1\_mgmt\_lif" per la registrazione con il server iSNS. Durante la registrazione iSNS, una SVM invia tutte le LIF iSCSI attraverso la LIF di gestione SVM al server iSNS. Una volta completata la registrazione iSNS, il server iSNS dispone di un elenco di tutti i LIF che servono iSCSI in "VS1". Se un cluster contiene più SVM, ciascuna SVM deve registrarsi singolarmente con il server iSNS per utilizzare il servizio iSNS.



Nell'esempio successivo, dopo che il server iSNS ha completato la registrazione con la destinazione, l'host A è in grado di rilevare tutte le LIF per "VS1" attraverso il server iSNS, come indicato nella fase 1. Dopo che l'host A ha completato il rilevamento dei LIF per "VS1", l'host A può stabilire una connessione con una qualsiasi delle LIF in "VS1", come illustrato nella fase 2. L'host A non è a conoscenza di alcuna LIF in "VS2" fino a quando la LIF di gestione "VS2\_Mgmt\_LIF" per "VS2" non si registra con il server iSNS.



Tuttavia, se si definiscono gli elenchi di accesso all'interfaccia, l'host può utilizzare solo i LIF definiti nell'elenco di accesso all'interfaccia per accedere alla destinazione.

Una volta configurato iSNS, ONTAP aggiorna automaticamente il server iSNS quando cambiano le impostazioni di configurazione di SVM.

Potrebbe verificarsi un ritardo di alcuni minuti tra il momento in cui vengono apportate le modifiche alla configurazione e il momento in cui ONTAP invia l'aggiornamento al server iSNS. Forzare un aggiornamento immediato delle informazioni iSNS sul server iSNS: `vserver iscsi isns update`

**Comandi per la gestione di iSNS**

ONTAP fornisce comandi per gestire il servizio iSNS.

Se si desidera...	Utilizzare questo comando...
Configurare un servizio iSNS	<code>vserver iscsi isns create</code>
Avviare un servizio iSNS	<code>vserver iscsi isns start</code>
Modificare un servizio iSNS	<code>vserver iscsi isns modify</code>
Visualizzare la configurazione del servizio iSNS	<code>vserver iscsi isns show</code>
Forzare un aggiornamento delle informazioni iSNS registrate	<code>vserver iscsi isns update</code>

Arrestare un servizio iSNS	<code>vserver iscsi isns stop</code>
Rimuovere un servizio iSNS	<code>vserver iscsi isns delete</code>
Visualizzare la pagina man per un comando	<code>man <i>command name</i></code>

Per ulteriori informazioni, consulta la pagina man relativa a ciascun comando.

## Provisioning SAN con FC

È necessario conoscere i concetti importanti necessari per comprendere come ONTAP implementa una SAN FC.

### Modalità di connessione dei nodi di destinazione FC alla rete

I sistemi storage e gli host dispongono di adattatori che consentono di collegarli agli switch FC tramite cavi.

Quando un nodo è connesso alla SAN FC, ogni SVM registra il World Wide Port Name (WWPN) della propria LIF con lo switch Fabric Name Service. Il WWNN della SVM e il WWPN di ogni LIF vengono assegnati automaticamente da ONTAP.



La connessione diretta ai nodi dagli host con FC non è supportata, è necessario NPIV e questo richiede l'utilizzo di uno switch. con le sessioni iSCSI, la comunicazione funziona con connessioni che sono instradate in rete o a connessione diretta. Tuttavia, entrambi questi metodi sono supportati con ONTAP.

### Come vengono identificati i nodi FC

Ogni SVM configurato con FC è identificato da un nome di nodo mondiale (WWNN).

### Come vengono utilizzate le WWPN

Le WWPN identificano ogni LIF in una SVM configurata per supportare FC. Queste LIF utilizzano le porte FC fisiche di ciascun nodo del cluster, che possono essere schede di destinazione FC, UTA o UTA2 configurate come FC o FCoE nei nodi.

- Creazione di un gruppo iniziatore

Le WWPN degli HBA dell'host vengono utilizzate per creare un gruppo di iniziatori (igroup). Un igroup viene utilizzato per controllare l'accesso host a LUN specifiche. È possibile creare un igroup specificando una raccolta di WWPN di iniziatori in una rete FC. Quando si esegue il mapping di un LUN su un sistema storage a un igroup, è possibile concedere a tutti gli iniziatori di quel gruppo l'accesso a tale LUN. Se la WWPN di un host non si trova in un igroup mappato a una LUN, tale host non ha accesso alla LUN. Ciò significa che i LUN non vengono visualizzati come dischi su quell'host.

È inoltre possibile creare set di porte per rendere visibile un LUN solo su porte di destinazione specifiche. Un set di porte è costituito da un gruppo di porte di destinazione FC. È possibile associare un igroup a un set di porte. Qualsiasi host del igroup può accedere ai LUN solo connettendosi alle porte di destinazione del set di porte.

- Identificazione univoca delle LIF FC

Le WWPN identificano in modo univoco ogni interfaccia logica FC. Il sistema operativo host utilizza la combinazione di WWNN e WWPN per identificare le SVM e le LIF FC. Alcuni sistemi operativi richiedono un binding persistente per garantire che il LUN appaia sullo stesso ID di destinazione sull'host.

## Come funzionano le assegnazioni dei nomi in tutto il mondo

I nomi in tutto il mondo vengono creati in sequenza in ONTAP. Tuttavia, a causa del modo in cui ONTAP li assegna, potrebbero sembrare assegnati in un ordine non sequenziale.

Ogni adattatore dispone di WWPN e WWNN preconfigurati, ma ONTAP non utilizza questi valori preconfigurati. Invece, ONTAP assegna le proprie WWPN o WWN, in base agli indirizzi MAC delle porte Ethernet integrate.

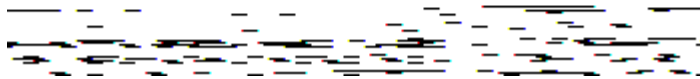
I nomi internazionali potrebbero sembrare non sequenziali se assegnati per i seguenti motivi:

- I nomi in tutto il mondo vengono assegnati a tutti i nodi e alle macchine virtuali di storage (SVM) del cluster.
- I nomi liberati in tutto il mondo vengono riciclati e aggiunti al pool di nomi disponibili.

## Identificazione degli switch FC

Gli switch Fibre Channel hanno un nome di nodo mondiale (WWNN) per il dispositivo stesso e un nome di porta mondiale (WWPN) per ciascuna delle porte.

Ad esempio, il seguente diagramma mostra come le WWPN vengono assegnate a ciascuna delle porte di uno switch Brocade a 16 porte. Per ulteriori informazioni sul numero delle porte per uno switch specifico, consultare la documentazione fornita dal vendor.



Port **0**, WWPN 20:**00**:00:60:69:51:06:b4

Port **1**, WWPN 20:**01**:00:60:69:51:06:b4

Port **14**, WWPN 20:**0e**:00:60:69:51:06:b4

Port **15**, WWPN 20:**0f**:00:60:69:51:06:b4

## Provisioning SAN con NVMe

A partire da ONTAP 9.4, NVMe/FC è supportato in ambiente SAN. NVMe/FC consente agli amministratori dello storage di eseguire il provisioning degli spazi dei nomi e dei sottosistemi e di mappare gli spazi dei nomi ai sottosistemi, in modo simile al modo in cui i LUN vengono forniti e mappati a igroups per FC e iSCSI.

Uno spazio dei nomi NVMe è una quantità di memoria non volatile che può essere formattata in blocchi logici. Gli spazi dei nomi sono l'equivalente dei LUN per i protocolli FC e iSCSI e un sottosistema NVMe è analogo a un igroup. Un sottosistema NVMe può essere associato agli iniziatori in modo che gli iniziatori associati possano accedere agli spazi dei nomi all'interno del sottosistema.



Sebbene funzioni analoghe, gli spazi dei nomi NVMe non supportano tutte le funzionalità supportate dalle LUN.

A partire da ONTAP 9.5, è necessaria una licenza per supportare l'accesso ai dati rivolti all'host con NVMe. Se NVMe è attivato in ONTAP 9.4, viene concesso un periodo di valutazione di 90 giorni per l'acquisizione della licenza dopo l'aggiornamento a ONTAP 9.5. Se lo hai fatto **"ONTAP uno"**, Sono incluse le licenze NVMe. È possibile attivare la licenza utilizzando il seguente comando:

```
system license add -license-code NVMe_license_key
```

#### Informazioni correlate

["Report tecnico di NetApp 4684: Implementazione e configurazione di SAN moderne con NVMe/FC"](#)

## Volumi SAN

### Panoramica sui volumi SAN

ONTAP offre tre opzioni di base per il provisioning dei volumi: Thick provisioning, thin provisioning e provisioning semi-thick. Ciascuna opzione utilizza diversi modi per gestire lo spazio del volume e i requisiti di spazio per le tecnologie di condivisione a blocchi di ONTAP. La comprensione del funzionamento delle opzioni consente di scegliere l'opzione migliore per il proprio ambiente.



Si sconsiglia di inserire LUN SAN e condivisioni NAS nello stesso volume FlexVol. È necessario eseguire il provisioning di volumi FlexVol separati specifici per LE LUN SAN e fornire volumi FlexVol separati in modo specifico alle condivisioni NAS. Ciò semplifica le implementazioni di gestione e replica e consente di utilizzare i volumi FlexVol supportati in Active IQ Unified Manager (in precedenza OnCommand Unified Manager).

### Thin provisioning per i volumi

Quando viene creato un volume con thin provisioning, ONTAP non riserva spazio extra quando viene creato il volume. Quando i dati vengono scritti nel volume, il volume richiede all'aggregato lo storage necessario per consentire l'operazione di scrittura. L'utilizzo di volumi con thin provisioning consente di eseguire l'overcommit dell'aggregato, il che introduce la possibilità che il volume non sia in grado di proteggere lo spazio necessario quando l'aggregato esaurisce lo spazio libero.

È possibile creare un volume FlexVol con thin provisioning impostandone l'impostazione `-space-guarantee` opzione a `none`.

### Thick provisioning per i volumi

Quando viene creato un volume con thick provisioning, ONTAP mette a disposizione una quantità di storage sufficiente dall'aggregato per garantire che qualsiasi blocco del volume possa essere scritto in qualsiasi momento. Quando si configura un volume per l'utilizzo del thick provisioning, è possibile utilizzare una qualsiasi delle funzionalità di efficienza dello storage ONTAP, come compressione e deduplica, per compensare i requisiti di storage anticipati più ampi.

È possibile creare un volume FlexVol con thick provisioning impostandone l'impostazione `-space-slo` (obiettivo del livello di servizio) opzione a `thick`.

## Provisioning semi-spessi per i volumi

Quando viene creato un volume che utilizza il provisioning semi-thick, ONTAP mette da parte lo spazio di storage dell'aggregato per tenere conto delle dimensioni del volume. Se il volume sta esaurendo lo spazio libero perché i blocchi vengono utilizzati dalle tecnologie di condivisione dei blocchi, ONTAP si impegna a eliminare gli oggetti dati di protezione (copie Snapshot, file FlexClone e LUN) per liberare spazio. Fino a quando ONTAP può eliminare gli oggetti dati di protezione abbastanza velocemente da tenere il passo con lo spazio richiesto per le sovrascritture, le operazioni di scrittura continuano a avere successo. Si tratta di una garanzia di scrittura "Best effort".

**Nota:** le seguenti funzionalità non sono supportate sui volumi che utilizzano il provisioning semi-spessi:

- tecnologie per l'efficienza dello storage come deduplica, compressione e compattazione
- ODX (Microsoft Offloaded Data Transfer)

È possibile creare un volume FlexVol con provisioning semi-thick impostandone il valore `-space-slo` (obiettivo del livello di servizio) opzione a. `semi-thick`.

## Da utilizzare con file e LUN con spazio riservato

Un file o LUN con spazio riservato è un file per il quale lo storage viene allocato al momento della creazione. Storicamente, NetApp ha utilizzato il termine "LUN con thin provisioning" per indicare un LUN per il quale la prenotazione dello spazio è disattivata (un LUN non riservato allo spazio).

**Nota:** i file non riservati allo spazio non sono generalmente denominati "thin-provisioning Files".

La seguente tabella riassume le principali differenze di utilizzo delle tre opzioni di provisioning dei volumi con file e LUN con spazio riservato:

Provisioning di volumi	Prenotazione di spazio LUN/file	Sovrascrive	Dati di protezione <sup>2</sup>	Efficienza dello storage <sup>3</sup>
Spesso	Supportato	Garantito <sup>1</sup>	Garantito	Supportato
Sottile	Nessun effetto	Nessuno	Garantito	Supportato
Semi-spessa	Supportato	Best effort <sup>1</sup>	Il massimo sforzo	Non supportato

## Note

1. La capacità di garantire le sovrascritture o fornire una garanzia di sovrascrittura con il massimo sforzo richiede che la riserva di spazio sia attivata sul LUN o sul file.
2. I dati di protezione includono copie Snapshot, file FlexClone e LUN contrassegnati per l'eliminazione automatica (cloni di backup).
3. L'efficienza dello storage include deduplica, compressione, qualsiasi file FlexClone e LUN non contrassegnati per l'eliminazione automatica (cloni attivi) e file secondari FlexClone (utilizzati per l'offload delle copie).

## Supporto per LUN con thin provisioning SCSI

ONTAP supporta LUN con thin provisioning SCSI T10 e LUN con thin provisioning NetApp. Il thin provisioning SCSI T10 consente alle applicazioni host di supportare funzionalità SCSI, tra cui funzionalità di recupero dello



spazio del LUN e di monitoraggio dello spazio del LUN per gli ambienti a blocchi. Il thin provisioning SCSI T10 deve essere supportato dal software host SCSI.

Si utilizza ONTAP `space-allocation` Impostazione per abilitare/disabilitare il supporto per il thin provisioning T10 su un LUN. Si utilizza ONTAP `space-allocation enable` Impostazione per abilitare il thin provisioning SCSI T10 su un LUN.

Il `[-space-allocation {enabled|disabled}]` Nel Manuale di riferimento dei comandi ONTAP sono disponibili ulteriori informazioni per attivare/disattivare il supporto per il thin provisioning T10 e per abilitare il thin provisioning SCSI T10 su un LUN.

## "Comandi di ONTAP 9"

### Configurare le opzioni di provisioning dei volumi

È possibile configurare un volume per il thin provisioning, il thick provisioning o il provisioning semi-thick.

#### A proposito di questa attività

Impostazione di `-space-slo` opzione a. `thick` garantisce quanto segue:

- L'intero volume viene preallocato nell'aggregato. Non è possibile utilizzare `volume create` oppure `volume modify` per configurare i volumi `-space-guarantee` opzione.
- il 100% dello spazio richiesto per le sovrascritture è riservato. Non è possibile utilizzare `volume modify` per configurare i volumi `-fractional-reserve` opzione

Impostazione di `-space-slo` opzione a. `semi-thick` garantisce quanto segue:

- L'intero volume viene preallocato nell'aggregato. Non è possibile utilizzare `volume create` oppure `volume modify` per configurare i volumi `-space-guarantee` opzione.
- Nessuno spazio riservato per le sovrascritture. È possibile utilizzare `volume modify` per configurare i volumi `-fractional-reserve` opzione.
- L'eliminazione automatica delle copie Snapshot è attivata.

#### Fase

1. Configurare le opzioni di provisioning dei volumi:

```
volume create -vserver vserver_name -volume volume_name -aggregate  
aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

Il `-space-guarantee` l'opzione predefinita è `none` Per sistemi AFF e volumi DP non AFF. In caso contrario, l'impostazione predefinita è `volume`. Per i volumi FlexVol esistenti, utilizzare `volume modify` per configurare le opzioni di provisioning.

Il seguente comando configura vol1 su SVM vs1 per il thin provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee  
none
```

Il seguente comando configura vol1 su SVM vs1 per il thick provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

Il seguente comando configura vol1 su SVM vs1 per il provisioning semi-spesso:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-thick
```

## Opzioni di configurazione del volume SAN

È necessario impostare diverse opzioni sul volume contenente il LUN. Il modo in cui si impostano le opzioni del volume determina la quantità di spazio disponibile per le LUN del volume.

### Crescita automatica

È possibile attivare o disattivare la crescita automatica. Se si attiva, la funzione di crescita automatica consente a ONTAP di aumentare automaticamente le dimensioni del volume fino a un massimo di dimensioni predeterminate. Per supportare la crescita automatica del volume, deve essere disponibile spazio nell'aggregato contenente. Pertanto, se si attiva la funzione di crescita automatica, è necessario monitorare lo spazio libero nell'aggregato contenente e aggiungerne di più quando necessario.

Impossibile attivare la crescita automatica per supportare la creazione di Snapshot. Se si tenta di creare una copia Snapshot e lo spazio sul volume è insufficiente, la creazione di Snapshot non riesce, anche con l'opzione di crescita automatica attivata.

Se la funzione di crescita automatica è disattivata, le dimensioni del volume rimangono invariate.

### Riduzione automatica

È possibile attivare o disattivare la riduzione automatica. Se la si attiva, la funzione di riduzione automatica consente a ONTAP di ridurre automaticamente le dimensioni complessive di un volume quando la quantità di spazio consumata nel volume diminuisce una soglia predeterminata. Ciò aumenta l'efficienza dello storage attivando i volumi per liberare automaticamente lo spazio libero inutilizzato.

### Eliminazione automatica di Snapshot

L'eliminazione automatica di Snapshot elimina automaticamente le copie Snapshot quando si verifica una delle seguenti condizioni:

- Il volume è quasi pieno.
- Lo spazio di riserva Snapshot è quasi pieno.
- Lo spazio riservato di sovrascrittura è pieno.

È possibile configurare l'eliminazione automatica di Snapshot per eliminare le copie Snapshot dalla meno recente alla più recente o dalla più recente alla meno recente. L'eliminazione automatica di Snapshot non elimina le copie Snapshot collegate alle copie Snapshot nei volumi clonati o nelle LUN.

Se il volume necessita di spazio aggiuntivo e sono state attivate sia la crescita automatica che l'eliminazione automatica delle snapshot, per impostazione predefinita ONTAP tenta di acquisire lo spazio necessario attivando prima la crescita automatica. Se non viene acquisita una quantità sufficiente di spazio attraverso la crescita automatica, viene attivata l'eliminazione automatica di Snapshot.

### Riserva di Snapshot

Snapshot Reserve definisce la quantità di spazio nel volume riservato alle copie Snapshot. Lo spazio allocato a Snapshot Reserve non può essere utilizzato per altri scopi. Se viene utilizzato tutto lo spazio allocato per Snapshot Reserve, le copie Snapshot iniziano a consumare spazio aggiuntivo sul volume.

### Requisito per lo spostamento di volumi in ambienti SAN

Prima di spostare un volume contenente LUN o spazi dei nomi, è necessario soddisfare determinati requisiti.

- Per i volumi contenenti una o più LUN, è necessario disporre di almeno due percorsi per LUN (LIF) connessi a ciascun nodo del cluster.

In questo modo si eliminano i singoli punti di errore e si consente al sistema di sopravvivere ai guasti dei componenti.

- Per i volumi contenenti spazi dei nomi, il cluster deve eseguire ONTAP 9.6 o versione successiva.

Lo spostamento del volume non è supportato per le configurazioni NVMe che eseguono ONTAP 9.5.

### Considerazioni per l'impostazione della riserva frazionale

La riserva frazionale, detta anche *riserva di sovrascrittura LUN*, consente di disattivare la riserva di sovrascrittura per i LUN e i file con spazio riservato in un volume FlexVol. In questo modo è possibile massimizzare l'utilizzo dello storage, ma se l'ambiente viene influenzato negativamente da operazioni di scrittura non riuscite a causa della mancanza di spazio, è necessario comprendere i requisiti imposti da questa configurazione.

L'impostazione della riserva frazionale viene espressa in percentuale; gli unici valori validi sono 0 e 100 percentuale. L'impostazione della riserva frazionale è un attributo del volume.

Impostazione della riserva frazionale a 0 aumenta l'utilizzo dello storage. Tuttavia, un'applicazione che accede ai dati che risiedono nel volume potrebbe riscontrare un'interruzione dei dati se il volume non dispone di spazio libero, anche se la garanzia del volume è impostata su `volume`. Tuttavia, con una configurazione e un utilizzo corretti del volume, è possibile ridurre al minimo il rischio di errori di scrittura. ONTAP offre una garanzia di scrittura "Best effort" per i volumi con riserva frazionale impostata su 0 quando *tutti* i seguenti requisiti sono soddisfatti:

- La deduplica non è in uso
- La compressione non è in uso
- I file secondari FlexClone non sono in uso
- Tutti i file FlexClone e i LUN FlexClone sono abilitati per l'eliminazione automatica

Questa non è l'impostazione predefinita. È necessario attivare esplicitamente l'eliminazione automatica, al momento della creazione o modificando il file FlexClone o il LUN FlexClone dopo la creazione.

- L'offload delle copie di ODX e FlexClone non è in uso
- La garanzia del volume è impostata su `volume`
- La prenotazione dello spazio del file o del LUN è `enabled`
- Volume Snapshot Reserve (Riserva snapshot volume) è impostato su 0
- L'eliminazione automatica della copia Snapshot del volume è `enabled` con un livello di impegno di `destroy`, un elenco di `destroy` di `lun_clone`, `vol_clone`, `cifs_share`, `file_clone`, `sfsr` è un trigger di ``volume`

Questa impostazione garantisce inoltre che i file FlexClone e le LUN FlexClone vengano cancellati quando necessario.

Si noti che se il tasso di cambiamento è elevato, in rari casi l'eliminazione automatica della copia Snapshot potrebbe restare indietro, con conseguente esaurimento dello spazio del volume, anche con tutte le impostazioni di configurazione richieste in precedenza in uso.

Inoltre, è possibile utilizzare la funzione di crescita automatica del volume per ridurre la probabilità che le copie Snapshot del volume debbano essere eliminate automaticamente. Se si attiva la funzione di crescita automatica, è necessario monitorare lo spazio libero nell'aggregato associato. Se l'aggregato diventa sufficientemente pieno da impedire la crescita del volume, è probabile che vengano eliminate più copie Snapshot man mano che lo spazio libero nel volume si esaurisce.

Se non si riesce a soddisfare tutti i requisiti di configurazione sopra indicati ed è necessario assicurarsi che il volume non esaurisca lo spazio, è necessario impostare la riserva frazionale del volume su 100. Ciò richiede più spazio libero in anticipo, ma garantisce che le operazioni di modifica dei dati avranno successo anche quando le tecnologie sopra elencate sono in uso.

Il valore predefinito e i valori consentiti per l'impostazione della riserva frazionale dipendono dalla garanzia del volume:

Garanzia di volume	Riserva frazionaria predefinita	Valori consentiti
Volume	100	0, 100
Nessuno	0	0, 100

## Gestione dello spazio lato host SAN

In un ambiente con thin provisioning, la gestione dello spazio lato host completa il processo di gestione dello spazio dal sistema storage liberato nel file system host.

Un file system host contiene metadati per tenere traccia di quali blocchi sono disponibili per memorizzare nuovi dati e quali blocchi contengono dati validi che non devono essere sovrascritti. Questi metadati vengono memorizzati all'interno del LUN. Quando un file viene cancellato nel file system host, i metadati del file system vengono aggiornati per contrassegnare i blocchi del file come spazio libero. Lo spazio libero totale del file system viene quindi ricalcolato per includere i blocchi appena liberati. Nel sistema di storage, questi aggiornamenti dei metadati non appaiono diversi da qualsiasi altra scrittura eseguita dall'host. Pertanto, il sistema di storage non è a conoscenza di eventuali eliminazioni.

In questo modo si crea una discrepanza tra la quantità di spazio libero indicata dall'host e la quantità di spazio libero indicata dal sistema di storage sottostante. Ad esempio, si supponga di disporre di un LUN da 200 GB

appena fornito assegnato all'host dal sistema storage. Sia l'host che il sistema di storage riportano 200 GB di spazio libero. L'host scrive quindi 100 GB di dati. A questo punto, sia l'host che il sistema di storage riportano 100 GB di spazio utilizzato e 100 GB di spazio inutilizzato.

Quindi, si eliminano 50 GB di dati dall'host. A questo punto, l'host segnalerà 50 GB di spazio utilizzato e 150 GB di spazio inutilizzato. Tuttavia, il sistema di storage riporta 100 GB di spazio utilizzato e 100 GB di spazio inutilizzato.

La gestione dello spazio sul lato host utilizza diversi metodi per riconciliare la differenza di spazio tra l'host e il sistema di storage.

### **Gestione semplificata degli host con SnapCenter**

È possibile utilizzare il software SnapCenter per semplificare alcune delle attività di gestione e protezione dei dati associate allo storage iSCSI e FC. SnapCenter è un pacchetto di gestione opzionale per host Windows e UNIX.

È possibile utilizzare il software SnapCenter per creare facilmente dischi virtuali da pool di storage che possono essere distribuiti tra diversi sistemi storage e per automatizzare le attività di provisioning dello storage e semplificare il processo di creazione di copie Snapshot e cloni da copie Snapshot coerenti con i dati host.

Per ulteriori informazioni su, consultare la documentazione dei prodotti NetApp "[SnapCenter](#)".

#### **Link correlati**

["Abilitare l'allocazione dello spazio per LUN con thin provisioning SCSI"](#)

### **A proposito di igroups**

I gruppi di iniziatori (igroups) sono tabelle di nomi di host WWPN del protocollo FC o di nodi host iSCSI. È possibile definire igroups e mapparli alle LUN per controllare quali iniziatori hanno accesso alle LUN.

In genere, si desidera che tutte le porte iniziatore dell'host o gli iniziatori software abbiano accesso a un LUN. Se si utilizza un software multipathing o si dispone di host in cluster, ogni porta iniziatore o iniziatore software di ciascun host in cluster necessita di percorsi ridondanti verso la stessa LUN.

È possibile creare igroups che specifichino quali iniziatori hanno accesso alle LUN prima o dopo la creazione delle LUN, ma è necessario creare igroups prima di poter mappare una LUN a un igroup.

I gruppi iniziatori possono avere più iniziatori e più igroups possono avere lo stesso iniziatore. Tuttavia, non è possibile mappare un LUN a più igroups con lo stesso iniziatore. Un iniziatore non può essere un membro di igroups di diversi ostype.

### **Esempio di come gli igroups forniscono l'accesso al LUN**

È possibile creare più igroups per definire quali LUN sono disponibili per gli host. Ad esempio, se si dispone di un cluster host, è possibile utilizzare igroups per garantire che LUN specifiche siano visibili a un solo host del cluster o a tutti gli host del cluster.

La seguente tabella illustra come quattro igroups consentono l'accesso alle LUN per quattro diversi host che accedono al sistema di storage. Gli host in cluster (Host3 e Host4) sono entrambi membri dello stesso igroup (group3) e possono accedere alle LUN mappate a questo igroup. L'igroup denominato group4 contiene le WWPN di Host4 per memorizzare informazioni locali che non sono destinate al partner.

Host con HBA WWPN, IQN o EUI	igroups	WWPN, IQN, EUI aggiunti a igroups	LUN mappati a igroups
Host 1, percorso singolo (iSCSI software initiator)  iqn.1991-05.com.microsoft:host1	gruppo 1	iqn.1991-05.com.microsoft:host1	/vol/vol2/lun1
Host2, multipath (due HBA)  10:00:00:00:c9:2b:6b:3c  10:00:00:00:c9:2b:02:3c	gruppo 2	10:00:00:00:c9:2b:6b:3c  10:00:00:00:c9:2b:02:3c	/vol/vol2/lun2
Host3, multipath, in cluster con host 4  10:00:00:00:c9:2b:32:1b  10:00:00:00:c9:2b:41:02	gruppo 3	10:00:00:00:c9:2b:32:1b  10:00:00:00:c9:2b:41:02  10:00:00:00:c9:2b:51:2c  10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees1/lun3
Host4, multipath, in cluster (non visibile all'host 3)  10:00:00:00:c9:2b:51:2c  10:00:00:00:c9:2b:47:a2	gruppo 4	10:00:00:00:c9:2b:51:2c  10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees2/lun4  /vol/vol2/qtrees1/lun5

## Specificare le WWPN dell'iniziatore e i nomi dei nodi iSCSI per un igroup

È possibile specificare i nomi dei nodi iSCSI e le WWPN degli iniziatori quando si crea un igroup oppure aggiungerli in un secondo momento. Se si sceglie di specificare i nomi dei nodi iSCSI e le WWPN dell'iniziatore quando si crea il LUN, è possibile rimuoverli in un secondo momento, se necessario.

Seguire le istruzioni nella documentazione delle utility host per ottenere le WWPN e per trovare i nomi dei nodi iSCSI associati a un host specifico. Per gli host che eseguono il software ESX, utilizzare Virtual Storage Console.

## Virtualizzazione dello storage con offload delle copie VMware e Microsoft

### Panoramica sulla virtualizzazione dello storage con VMware e sull'offload delle copie Microsoft

VMware e Microsoft supportano le operazioni di offload delle copie per aumentare le performance e il throughput di rete. È necessario configurare il sistema in modo che soddisfi i requisiti degli ambienti dei sistemi operativi VMware e Windows per utilizzare le

rispettive funzioni di offload delle copie.

Quando si utilizza l'offload delle copie VMware e Microsoft in ambienti virtualizzati, le LUN devono essere allineate. Le LUN non allineate possono degradare le performance.

#### **Vantaggi dell'utilizzo di un ambiente SAN virtualizzato**

La creazione di un ambiente virtualizzato utilizzando le macchine virtuali di storage (SVM) e le LIF consente di espandere l'ambiente SAN a tutti i nodi del cluster.

- Gestione distribuita

È possibile accedere a qualsiasi nodo della SVM per amministrare tutti i nodi di un cluster.

- Maggiore accesso ai dati

Con MPIO e ALUA, puoi accedere ai tuoi dati attraverso qualsiasi LIF iSCSI o FC attiva per SVM.

- Accesso LUN controllato

Se si utilizzano SLM e portsets, è possibile limitare le LIF che un iniziatore può utilizzare per accedere alle LUN.

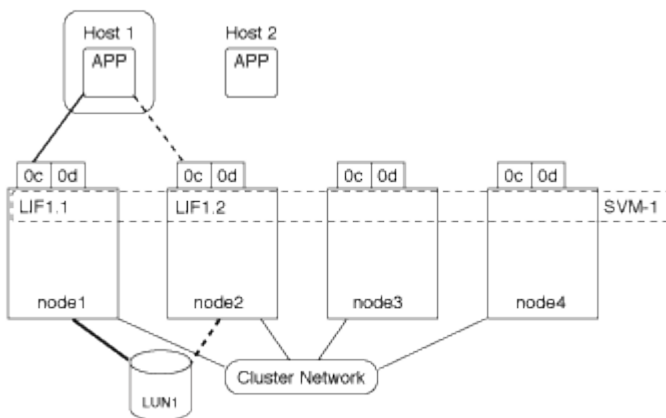
#### **Come funziona l'accesso al LUN in un ambiente virtualizzato**

In un ambiente virtualizzato, le LIF consentono agli host (client) di accedere alle LUN attraverso percorsi ottimizzati e non ottimizzati.

Una LIF è un'interfaccia logica che collega la SVM a una porta fisica. Sebbene più SVM possano avere più LIF sulla stessa porta, una LIF appartiene a una SVM. È possibile accedere alle LUN tramite le LIF SVM.

#### **Esempio di accesso LUN con una singola SVM in un cluster**

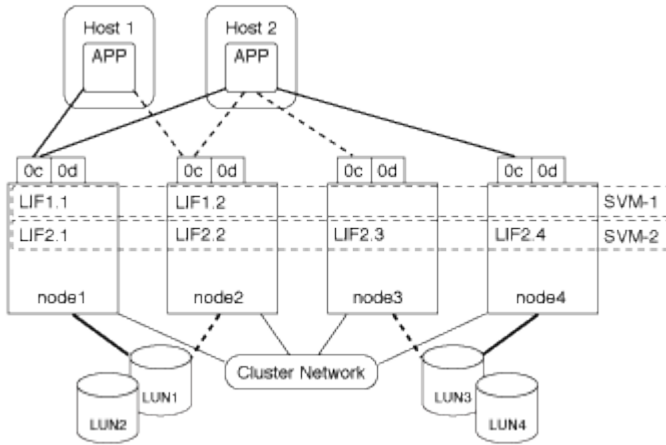
Nell'esempio seguente, l'host 1 si connette a LIF1.1 e LIF1.2 in SVM-1 per accedere a LUN1. LIF 1.1 utilizza la porta fisica node1:0c e LIF 1.2 utilizza il node2:0c. LIF1.1 e LIF1.2 appartengono solo a SVM-1. Se viene creata una nuova LUN sul nodo 1 o sul nodo 2, per SVM-1, è possibile utilizzare le stesse LIF. Se viene creata una nuova SVM, è possibile creare nuove LIF utilizzando le porte fisiche 0c o 0d su entrambi i nodi.



#### **Esempio di accesso LUN con più SVM in un cluster**

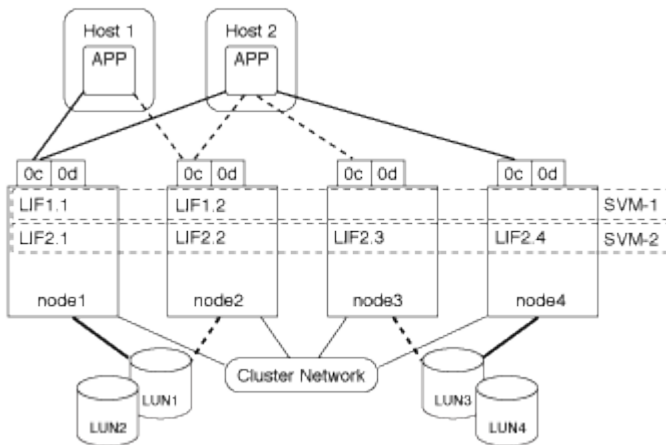
Una porta fisica può supportare più LIF che servono diverse SVM. Poiché le LIF sono associate a una specifica SVM, i nodi del cluster possono inviare il traffico dati in entrata alla SVM corretta. Nell'esempio

seguente, ciascun nodo da 1 a 4 ha una LIF per SVM-2 che utilizza la porta fisica 0c su ciascun nodo. L'host 1 si connette a LIF1.1 e LIF1.2 in SVM-1 per accedere a LUN1. L'host 2 si connette a LIF2.1 e LIF2.2 in SVM-2 per accedere a LUN2. Entrambi gli SVM condividono la porta fisica 0c sui nodi 1 e 2. SVM-2 dispone di LIF aggiuntive utilizzate dall'host 2 per accedere alle LUN 3 e 4. Queste LIF utilizzano la porta fisica 0c sui nodi 3 e 4. Più SVM possono condividere le porte fisiche sui nodi.



### Esempio di percorso attivo o ottimizzato a una LUN da un sistema host

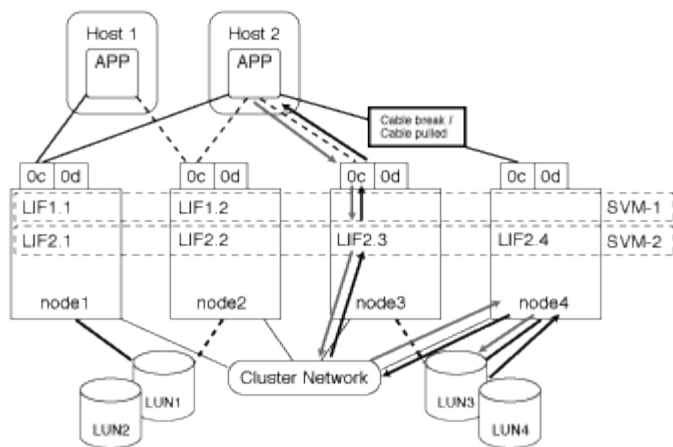
In un percorso attivo o ottimizzato, il traffico di dati non passa sulla rete del cluster, ma percorre il percorso più diretto verso il LUN. Il percorso attivo o ottimizzato per LUN1 è attraverso LIF 1.1 in node1, utilizzando la porta fisica 0c. L'host 2 dispone di due percorsi attivi o ottimizzati, un percorso verso il nodo 1, LIF2.1, che condivide la porta fisica 0c e l'altro percorso verso il nodo 4, LIF2.4, che utilizza la porta fisica 0c.



### Esempio di percorso (indiretto) attivo o non ottimizzato verso un LUN da un sistema host

In un percorso (indiretto) attivo o non ottimizzato, il traffico dati viaggia sulla rete del cluster. Questo problema si verifica solo se tutti i percorsi attivi o ottimizzati da un host non sono disponibili per gestire il traffico. Se il percorso dall'host 2 a SVM-2 LIF2.4 viene perso, l'accesso a LUN3 e LUN4 attraversa la rete del cluster. L'accesso dall'host 2 utilizza LIF 2.3 al nodo 3. Quindi, il traffico entra nello switch di rete del cluster ed esegue il backup fino al node4 per l'accesso a LUN3 e LUN4. Quindi, passa nuovamente sullo switch di rete del cluster e torna all'host 2 attraverso LIF 2.3. Questo percorso attivo o non ottimizzato viene utilizzato fino al ripristino del percorso a LIF 2.4 o fino a quando non viene stabilito un nuovo LIF per SVM-2 su un'altra porta fisica sul nodo 4.





=  
:allow-uri-read:

### Migliorare le performance di VMware VAAI per gli host ESX

ONTAP supporta alcune API vStorage VMware per l'integrazione degli array (VAAI) quando l'host ESX esegue ESX 4.1 o versioni successive. Queste funzionalità consentono di trasferire le operazioni dall'host ESX al sistema storage e aumentare il throughput di rete. L'host ESX attiva automaticamente le funzioni nell'ambiente corretto.

La funzione VAAI supporta i seguenti comandi SCSI:

- EXTENDED\_COPY

Questa funzione consente all'host di avviare il trasferimento dei dati tra le LUN o all'interno di una LUN senza coinvolgere l'host nel trasferimento dei dati. Ciò consente di risparmiare i cicli della CPU ESX e di aumentare il throughput di rete. La funzione di copia estesa, nota anche come "offload delle copie", viene utilizzata in scenari come la clonazione di una macchina virtuale. Quando viene richiamata dall'host ESX, la funzione di offload delle copie copia i dati all'interno del sistema di storage piuttosto che passare attraverso la rete host. L'offload della copia trasferisce i dati nei seguenti modi:

- All'interno di un LUN
- Tra LUN all'interno di un volume
- Tra LUN su diversi volumi all'interno di una macchina virtuale per lo storage (SVM)
- Tra LUN su SVM diverse all'interno di un cluster se questa funzione non può essere richiamata, l'host ESX utilizza automaticamente i comandi di LETTURA e SCRITTURA standard per l'operazione di copia.

- WRITE\_SAME

Questa funzionalità consente di trasferire il lavoro di scrittura di un modello ripetuto, ad esempio tutti gli zeri, a un array di storage. L'host ESX utilizza questa funzionalità in operazioni come lo zero-filling di un file.

- COMPARE\_AND\_WRITE

Questa funzionalità ignora alcuni limiti di concorrenza per l'accesso ai file, che accelerano le operazioni come l'avvio delle macchine virtuali.

## Requisiti per l'utilizzo dell'ambiente VAAI

Le funzionalità VAAI fanno parte del sistema operativo ESX e vengono richiamate automaticamente dall'host ESX una volta configurato l'ambiente corretto.

I requisiti ambientali sono i seguenti:

- L'host ESX deve eseguire ESX 4.1 o versione successiva.
- Il sistema storage NetApp che ospita il datastore VMware deve eseguire ONTAP.
- (Solo offload delle copie) l'origine e la destinazione dell'operazione di copia VMware devono essere ospitati sullo stesso sistema di storage all'interno dello stesso cluster.



La funzione di offload delle copie attualmente non supporta la copia dei dati tra gli archivi dati VMware ospitati su sistemi storage diversi.

### Determinare se le funzionalità VAAI sono supportate da ESX

Per verificare se il sistema operativo ESX supporta le funzionalità VAAI, è possibile controllare il client vSphere o utilizzare qualsiasi altro mezzo per accedere all'host. Per impostazione predefinita, ONTAP supporta i comandi SCSI.

È possibile controllare le impostazioni avanzate dell'host ESX per determinare se le funzioni VAAI sono attivate. La tabella indica i comandi SCSI corrispondenti ai nomi dei controlli ESX.

Comando SCSI	Nome del controllo ESX (funzione VAAI)
COPIA_ESTESA	HardwareAcceleratedMove
WRITE_SAME	HardwareAcceleratedInit
COMPARE_AND_WRITE	HardwareAcceleratedLocking

### ODX (Microsoft Offloaded Data Transfer)

Microsoft Offloaded Data Transfer (ODX), noto anche come *copy offload*, consente il trasferimento diretto dei dati all'interno di un dispositivo di storage o tra dispositivi di storage compatibili senza trasferire i dati attraverso il computer host.

ONTAP supporta ODX per i protocolli SMB e SAN.

Nei trasferimenti di file non ODX, i dati vengono letti dall'origine e trasferiti attraverso la rete all'host. L'host trasferisce i dati di nuovo sulla rete alla destinazione. Nel trasferimento di file ODX, i dati vengono copiati direttamente dall'origine alla destinazione senza passare attraverso l'host.

Poiché le copie con offload di ODX vengono eseguite direttamente tra origine e destinazione, si ottengono significativi vantaggi in termini di performance se le copie vengono eseguite nello stesso volume, inclusi tempo di copia più rapido per le stesse copie del volume, utilizzo ridotto di CPU e memoria sul client e utilizzo ridotto della larghezza di banda di i/o di rete. Se le copie sono tra i volumi, potrebbe non esserci un aumento significativo delle performance rispetto alle copie basate su host.

Per gli ambienti SAN, ODX è disponibile solo quando è supportato sia dall'host che dal sistema storage. I

computer client che supportano ODX e che hanno ODX abilitato automaticamente e in modo trasparente utilizzano il trasferimento di file offload durante lo spostamento o la copia dei file. ODX viene utilizzato indipendentemente dal fatto che si trascinino i file tramite Esplora risorse o si utilizzino comandi di copia dei file dalla riga di comando o che un'applicazione client avvii richieste di copia dei file.

### Requisiti per l'utilizzo di ODX

Se si intende utilizzare ODX per gli offload delle copie, è necessario conoscere le considerazioni sul supporto dei volumi, i requisiti di sistema e i requisiti di funzionalità software.

Per utilizzare ODX, il sistema deve disporre di quanto segue:

- ONTAP

ODX viene attivato automaticamente nelle versioni supportate di ONTAP.

- Volume di origine minimo di 2 GB

Per ottenere prestazioni ottimali, il volume di origine deve essere superiore a 260 GB.

- Supporto di ODX sul client Windows

ODX è supportato in Windows Server 2012 o versioni successive e in Windows 8 o versioni successive. La matrice di interoperabilità contiene le informazioni più recenti sui client Windows supportati.

["Tool di matrice di interoperabilità NetApp"](#)

- Supporto dell'applicazione di copia per ODX

L'applicazione che esegue il trasferimento dei dati deve supportare ODX. Le operazioni applicative che supportano ODX includono:

- Operazioni di gestione di Hyper-V, come la creazione e la conversione di dischi rigidi virtuali (VHD), la gestione di copie Snapshot e la copia di file tra macchine virtuali
  - Operazioni di Esplora risorse
  - Comandi di copia di Windows PowerShell
  - Comandi di copia del prompt dei comandi di Windows la Microsoft TechNet Library contiene ulteriori informazioni sulle applicazioni ODX supportate su server e client Windows.
- Se si utilizzano volumi compressi, la dimensione del gruppo di compressione deve essere 8K.

Le dimensioni del gruppo di compressione 32K non sono supportate.

ODX non funziona con i seguenti tipi di volume:

- Volumi di origine con capacità inferiori a 2 GB
- Volumi di sola lettura
- ["Volumi FlexCache"](#)



ODX è supportato sui volumi di origine FlexCache.

- ["Volumi con provisioning semi-spessi"](#)

## Requisiti speciali per i file di sistema

È possibile eliminare i file ODX trovati in qtree. Non rimuovere o modificare altri file di sistema ODX a meno che non venga richiesto dal supporto tecnico.

Quando si utilizza la funzione ODX, esistono file di sistema ODX in ogni volume del sistema. Questi file consentono la rappresentazione point-in-time dei dati utilizzati durante il trasferimento ODX. I seguenti file di sistema si trovano nel livello root di ogni volume che contiene LUN o file in cui sono stati scaricati i dati:

- `.copy-offload` (una directory nascosta)
- `.tokens` (file sotto il nascosto `.copy-offload` directory)

È possibile utilizzare `copy-offload delete-tokens -path dir_path -node node_name` Comando per eliminare un qtree contenente un file ODX.

## Casi di utilizzo per ODX

È necessario conoscere i casi di utilizzo per l'utilizzo di ODX su SVM in modo da poter determinare in quali circostanze ODX offre vantaggi in termini di performance.

I server e i client Windows che supportano ODX utilizzano l'offload delle copie come metodo predefinito per copiare i dati tra server remoti. Se il server o il client Windows non supporta ODX o l'offload delle copie ODX non riesce in qualsiasi momento, l'operazione di copia o spostamento ritorna alle tradizionali operazioni di lettura e scrittura per l'operazione di copia o spostamento.

I seguenti casi di utilizzo supportano l'utilizzo di copie e spostamenti ODX:

- Intra-volume

I file di origine e di destinazione o LUN si trovano all'interno dello stesso volume.

- Intervolume, stesso nodo, stessa SVM

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà della stessa SVM.

- Intervolume, nodi diversi, stessa SVM

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà della stessa SVM.

- Inter-SVM, stesso nodo

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano sullo stesso nodo. I dati sono di proprietà di diverse SVM.

- Inter-SVM, nodi diversi

I file di origine e di destinazione o LUN si trovano su volumi diversi che si trovano su nodi diversi. I dati sono di proprietà di diverse SVM.

- Tra cluster

Le LUN di origine e di destinazione si trovano su volumi diversi che si trovano su nodi diversi tra cluster. Questo è supportato solo per SAN e non per SMB.

Esistono alcuni casi di utilizzo speciali aggiuntivi:

- Con l'implementazione di ONTAP ODX, è possibile utilizzare ODX per copiare i file tra le condivisioni SMB e le unità virtuali FC o iSCSI collegate.

È possibile utilizzare Esplora risorse, la CLI di Windows o PowerShell, Hyper-V o altre applicazioni che supportano ODX per copiare o spostare i file senza problemi utilizzando l'offload delle copie ODX tra le condivisioni SMB e le LUN connesse, a condizione che le condivisioni SMB e le LUN si trovino sullo stesso cluster.

- Hyper-V offre alcuni casi di utilizzo aggiuntivi per l'offload delle copie ODX:
  - È possibile utilizzare il pass-through di offload delle copie ODX con Hyper-V per copiare i dati all'interno o tra file di dischi rigidi virtuali (VHD) o per copiare i dati tra le condivisioni SMB mappate e le LUN iSCSI connesse all'interno dello stesso cluster.

Ciò consente il passaggio delle copie dai sistemi operativi guest allo storage sottostante.

- Quando si creano VHD di dimensioni fisse, ODX viene utilizzato per inizializzare il disco con zero, utilizzando un token azzerato ben noto.
- L'offload delle copie ODX viene utilizzato per la migrazione dello storage delle macchine virtuali se lo storage di origine e di destinazione si trova sullo stesso cluster.



Per sfruttare i casi di utilizzo del pass-through di offload delle copie ODX con Hyper-V, il sistema operativo guest deve supportare ODX e i dischi del sistema operativo guest devono essere dischi SCSI supportati dallo storage (SMB o SAN) che supporti ODX. I dischi IDE sul sistema operativo guest non supportano il pass-through ODX.

## Amministrazione SAN

### Provisioning SAN

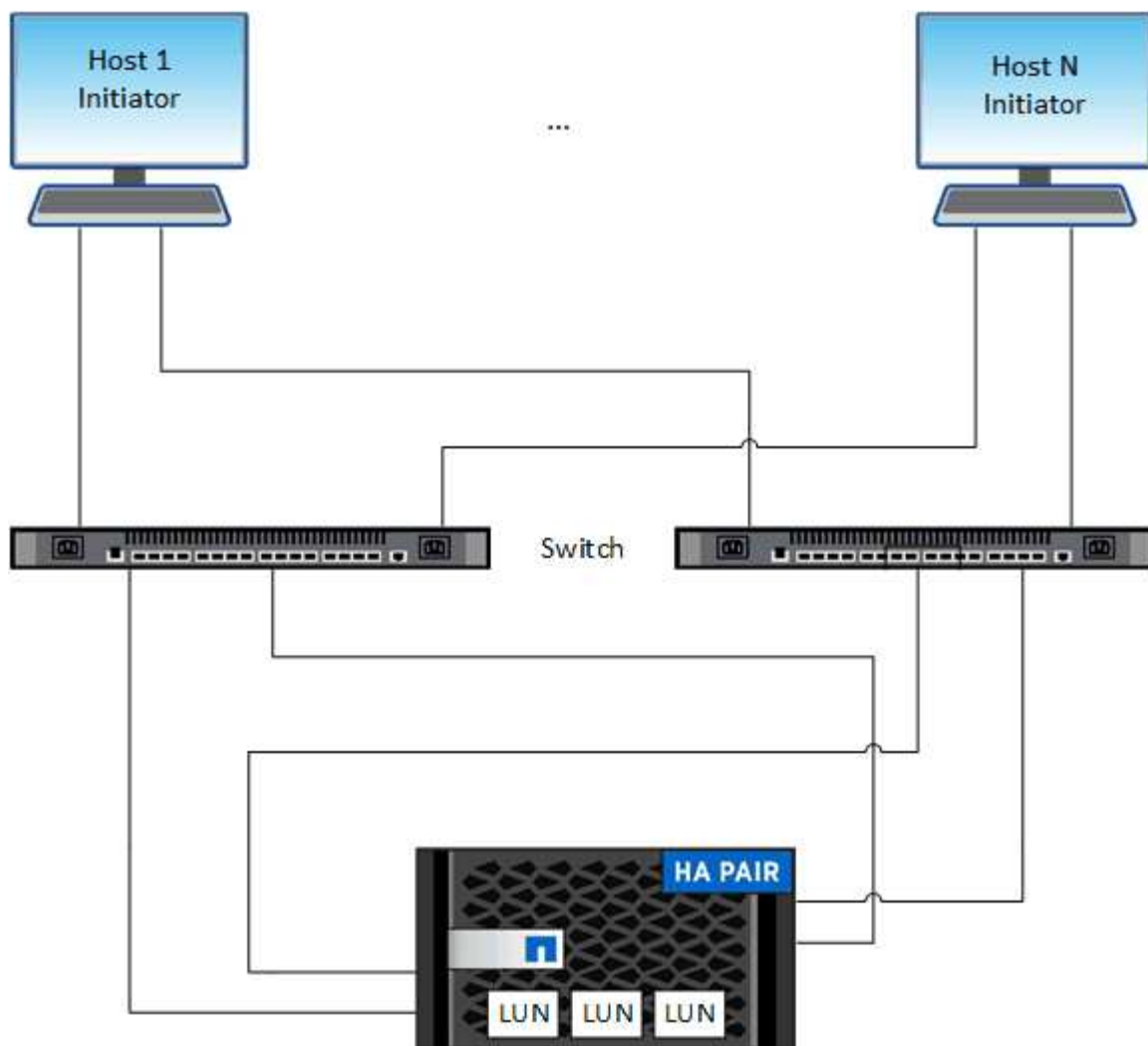
#### Panoramica sulla gestione SAN

Il contenuto di questa sezione illustra come configurare e gestire gli ambienti SAN con l'interfaccia a riga di comando (CLI) di ONTAP e Gestione di sistema in ONTAP 9.7 e versioni successive.

Se si utilizza Gestione di sistema classico (disponibile solo in ONTAP 9.7 e versioni precedenti), consultare i seguenti argomenti:

- ["Protocollo iSCSI"](#)
- ["Protocollo FC/FCoE"](#)

È possibile utilizzare i protocolli iSCSI e FC per fornire storage in un ambiente SAN.



Con iSCSI e FC, le destinazioni di storage sono denominate LUN (unità logiche) e vengono presentate agli host come dispositivi a blocchi standard. Si creano LUN e quindi le si associano ai gruppi di iniziatori (igroups). I gruppi di iniziatori sono tabelle di WWP host FC e nomi di nodi host iSCSI e controllano quali iniziatori hanno accesso a quali LUN.

Le destinazioni FC si connettono alla rete tramite switch FC e adattatori lato host e sono identificate da nomi di porte mondiali (WWPN). Le destinazioni iSCSI si collegano alla rete tramite schede di rete Ethernet standard (NIC), schede TOE (TCP offload Engine) con iniziatori software, adattatori di rete convergenti (CNA) o adattatori host busto dedicati (HBA) e sono identificate da nomi qualificati iSCSI (IQN).

### Configurare gli switch per FCoE

È necessario configurare gli switch per FCoE prima che il servizio FC possa essere eseguito sull'infrastruttura Ethernet esistente.

#### Di cosa hai bisogno

- La configurazione SAN deve essere supportata.

Per ulteriori informazioni sulle configurazioni supportate, consultare ["Tool di matrice di interoperabilità NetApp"](#).

- È necessario installare un Unified Target Adapter (UTA) sul sistema storage.

Se si utilizza un UTA2, è necessario impostarlo su `cna` modalità.

- Sull'host deve essere installato un adattatore di rete convergente (CNA).

### Fasi

1. Utilizzare la documentazione dello switch per configurare gli switch per FCoE.
2. Verificare che le impostazioni DCB di ogni nodo nel cluster siano state configurate correttamente.

```
run -node node1 -command dcb show
```

Le impostazioni DCB sono configurate sullo switch. Se le impostazioni non sono corrette, consultare la documentazione dello switch.

3. Verificare che l'accesso FCoE funzioni quando lo stato online della porta di destinazione FC è `true`.

```
fcp adapter show -fields node,adapter,status,state,speed,fabric-  
established,physical-protocol
```

Se lo stato in linea della porta di destinazione FC è `false`, consultare la documentazione dello switch.

### Informazioni correlate

- ["Tool di matrice di interoperabilità NetApp"](#)
- ["Report tecnico di NetApp 3800: Guida all'implementazione end-to-end Fibre Channel over Ethernet \(FCoE\)"](#)
- ["Cisco MDS 9000 NX-OS e SAN-OS Software Configuration Guide"](#)
- ["Prodotti Brocade"](#)

### Requisiti di sistema

La configurazione dei LUN implica la creazione di un LUN, la creazione di un igroup e la mappatura del LUN all'igroup. Il sistema deve soddisfare determinati prerequisiti prima di poter configurare le LUN.

- La matrice di interoperabilità deve elencare la configurazione SAN come supportata.
- L'ambiente SAN deve soddisfare i limiti di configurazione del controller e dell'host SAN specificati nella ["NetApp Hardware Universe"](#) Per la versione del software ONTAP in uso.
- È necessario installare una versione supportata delle utility host.

La documentazione relativa alle utility host fornisce ulteriori informazioni.

- È necessario disporre di LIF SAN nel nodo proprietario del LUN e nel partner ha del nodo proprietario.

### Informazioni correlate

- ["Tool di matrice di interoperabilità NetApp"](#)
- ["Configurazione host SAN ONTAP"](#)

- ["Report tecnico di NetApp 4017: Best Practice SAN Fibre Channel"](#)

## **Cosa fare prima di creare un LUN**

### **Perché le dimensioni effettive del LUN variano leggermente**

Per quanto riguarda le dimensioni dei LUN, è necessario conoscere quanto segue.

- Quando si crea un LUN, le dimensioni effettive del LUN potrebbero variare leggermente in base al tipo di sistema operativo del LUN. Il tipo di sistema operativo LUN non può essere modificato dopo la creazione del LUN.
- Se si crea un LUN con le dimensioni massime del LUN, tenere presente che le dimensioni effettive del LUN potrebbero essere leggermente inferiori. ONTAP arrotonda il limite per essere leggermente inferiore.
- I metadati per ogni LUN richiedono circa 64 KB di spazio nell'aggregato contenente. Quando si crea un LUN, è necessario assicurarsi che l'aggregato contenente disponga di spazio sufficiente per i metadati del LUN. Se l'aggregato non contiene spazio sufficiente per i metadati del LUN, alcuni host potrebbero non essere in grado di accedere al LUN.

### **Linee guida per l'assegnazione degli ID LUN**

In genere, l'ID LUN predefinito inizia con 0 e viene assegnato in incrementi di 1 per ogni LUN mappato aggiuntivo. L'host associa l'ID LUN alla posizione e al nome del percorso del LUN. L'intervallo di numeri ID LUN validi dipende dall'host. Per informazioni dettagliate, consultare la documentazione fornita con le utility host.

### **Linee guida per la mappatura delle LUN in igroups**

- È possibile mappare un LUN solo una volta su un igroup.
- Come Best practice, è necessario mappare un LUN a un solo iniziatore specifico attraverso l'igroup.
- È possibile aggiungere un singolo iniziatore a più igroups, ma l'iniziatore può essere mappato a un solo LUN.
- Non è possibile utilizzare lo stesso ID LUN per due LUN mappati allo stesso igroup.
- È necessario utilizzare lo stesso tipo di protocollo per igroups e set di porte.

## **Verificare e aggiungere la licenza FC o iSCSI del protocollo**

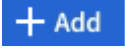
Prima di abilitare l'accesso a blocchi per una macchina virtuale di storage (SVM) con FC o iSCSI, è necessario disporre di una licenza. Le licenze FC e iSCSI sono incluse in ["ONTAP uno"](#).



## Esempio 6. Fasi

### System Manager

Se non si dispone di ONTAP ONE, verificare e aggiungere la licenza FC o iSCSI con Gestione sistema ONTAP (9,7 e versioni successive).

1. In System Manager, selezionare **Cluster > Settings > Licenses** (Cluster > Impostazioni > licenze)
2. Se la licenza non è presente nell'elenco, selezionare  e inserire la chiave di licenza.
3. Selezionare **Aggiungi**.

### CLI

Se non si dispone di ONTAP ONE, verificare e aggiungere la licenza FC o iSCSI con la CLI ONTAP.

1. Verificare di disporre di una licenza attiva per FC o iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. Se non si dispone di una licenza attiva per FC o iSCSI, aggiungere il codice di licenza.

```
license add -license-code <your_license_code>
```

## Eseguire il provisioning dello storage SAN

Questa procedura crea nuovi LUN su una VM di storage esistente che ha già configurato il protocollo FC o iSCSI.

Se è necessario creare una nuova VM di storage e configurare il protocollo FC o iSCSI, vedere ["Configurare una SVM per FC"](#) oppure ["Configurare una SVM per iSCSI"](#).

Se la licenza FC non è abilitata, le LIF e le SVM sembrano essere in linea ma lo stato operativo è inattivo.

I LUN vengono visualizzati sull'host come dispositivi disco.



L'ALUA (Asymmetric Logical Unit Access) è sempre abilitato durante la creazione del LUN. Non è possibile modificare l'impostazione ALUA.

Per ospitare gli iniziatori, è necessario utilizzare lo zoning initiator singolo per tutte le LIF FC nella SVM.

A partire da ONTAP 9.8, quando si esegue il provisioning dello storage, la qualità del servizio viene attivata per impostazione predefinita. È possibile disattivare la QoS o scegliere una policy QoS personalizzata durante il processo di provisioning o in un secondo momento.

## Esempio 7. Fasi

### System Manager

Creare LUN per fornire storage a un host SAN utilizzando il protocollo FC o iSCSI con Gestione di sistema di ONTAP (9.7 e versioni successive).

Per completare questa attività utilizzando System Manager Classic (disponibile con 9.7 e versioni precedenti), fare riferimento a. ["Configurazione iSCSI per Red Hat Enterprise Linux"](#)

### Fasi

1. Installare il appropriato ["Utility host SAN"](#) sul tuo host.
2. In System Manager, fare clic su **Storage > LUN**, quindi su **Add**.
3. Inserire le informazioni richieste per creare il LUN.
4. È possibile fare clic su **altre opzioni** per eseguire una delle seguenti operazioni, a seconda della versione di ONTAP in uso.

Opzione	Disponibile a partire da
<ul style="list-style-type: none"><li>• Assegnare il criterio QoS ai LUN anziché al volume padre<ul style="list-style-type: none"><li>◦ <b>Altre opzioni &gt; Storage and Optimization</b></li><li>◦ Selezionare <b>Performance Service Level</b>.</li><li>◦ Per applicare il criterio QoS ai singoli LUN anziché all'intero volume, selezionare <b>Applica questi limiti di performance a ogni LUN</b>.</li></ul><p>Per impostazione predefinita, i limiti di performance vengono applicati a livello di volume.</p></li></ul>	ONTAP 9.10.1
<ul style="list-style-type: none"><li>• Creare un nuovo gruppo di iniziatori utilizzando i gruppi di iniziatori esistenti<ul style="list-style-type: none"><li>◦ <b>Altre opzioni &gt; INFORMAZIONI HOST</b></li><li>◦ Selezionare <b>New Initiator group using existing initiator groups</b> (nuovo gruppo iniziatore che utilizza</li></ul><p><b>NOTA:</b> Il tipo di sistema operativo per un igroup contenente altri igroups non può essere modificato dopo che è stato creato.</p></li></ul>	ONTAP 9.9.1
<ul style="list-style-type: none"><li>• Aggiungere una descrizione all'igroup o all'iniziatore host</li></ul> <p>La descrizione funge da alias per igroup o host initiator.</p> <ul style="list-style-type: none"><li>◦ <b>Altre opzioni &gt; INFORMAZIONI HOST</b></li></ul>	ONTAP 9.9.1

<ul style="list-style-type: none"> <li>• Creare il LUN su un volume esistente</li> </ul> <p>Per impostazione predefinita, viene creata una nuova LUN in un nuovo volume.</p> <ul style="list-style-type: none"> <li>◦ <b>Altre opzioni &gt; Aggiungi LUN</b></li> <li>◦ Selezionare <b>LUN correlati al gruppo</b>.</li> </ul>	ONTAP 9.9.1
<ul style="list-style-type: none"> <li>• Disattivare QoS o scegliere un criterio QoS personalizzato</li> <li>◦ <b>Altre opzioni &gt; Storage and Optimization</b></li> <li>◦ Selezionare <b>Performance Service Level</b>.</li> </ul> <p><b>NOTA:</b> In ONTAP 9.9.1 e versioni successive, se si seleziona un criterio QoS personalizzato, è possibile anche selezionare il posizionamento manuale su un livello locale specificato.</p>	ONTAP 9.8

5. Per gli switch FC, eseguire la zona degli switch FC in base al numero WWPN. Utilizzare una zona per iniziatore e includere tutte le porte di destinazione in ciascuna zona.

6. Scopri le LUN sul tuo host.

Per VMware vSphere, utilizzare Virtual Storage Console (VSC) per rilevare e inizializzare le LUN.

7. Inizializzare le LUN e, facoltativamente, creare file system.

8. Verificare che l'host sia in grado di scrivere e leggere i dati sul LUN.

## CLI

Creare LUN per fornire storage a un host SAN utilizzando il protocollo FC o iSCSI con l'interfaccia CLI ONTAP.

1. Verificare di disporre di una licenza per FC o iSCSI.

```
system license show
```

Package	Type	Description	Expiration
Base	site	Cluster Base License	-
NFS	site	NFS License	-
CIFS	site	CIFS License	-
iSCSI	site	iSCSI License	-
FCP	site	FCP License	-

2. Se non si dispone di una licenza per FC o iSCSI, utilizzare `license add` comando.

```
license add -license-code <your_license_code>
```

3. Abilitare il servizio di protocollo su SVM:

**Per iSCSI:**

```
vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
```

**Per FC:**

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. Creare due LIF per le SVM su ciascun nodo:

```
network interface create -vserver <svm_name> -lif <lif_name> -role  
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port  
<port_name> -address <ip_address> -netmask <netmask>
```

NetApp supporta almeno un LIF iSCSI o FC per nodo per ogni SVM che fornisce dati. Tuttavia, per la ridondanza sono necessari due LIFS per nodo. Per iSCSI, si consiglia di configurare un minimo di due LIF per nodo in reti Ethernet separate.

5. Verificare che i file LIF siano stati creati e che il loro stato operativo sia *online*:

```
network interface show -vserver <svm_name> <lif_name>
```

6. Crea le tue LUN:

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>  
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

Il nome del LUN non può superare i 255 caratteri e non può contenere spazi.



L'opzione NVFAIL viene attivata automaticamente quando viene creata una LUN in un volume.

7. Crea i tuoi igroups:

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol  
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. Mappare i LUN a igroups:

```
lun mapping create -vserver <svm__name> -volume <volume_name> -lun  
<lun_name> -igroup <igroup_name>
```

9. Verificare che i LUN siano configurati correttamente:

```
lun show -vserver <svm_name>
```

10. Facoltativamente, ["Creare un set di porte e associarlo a un igroup"](#).

11. Seguire i passaggi nella documentazione dell'host per abilitare l'accesso a blocchi su host specifici.

12. Utilizzare le utility host per completare la mappatura FC o iSCSI e rilevare le LUN sull'host.

### Informazioni correlate

- ["Panoramica sull'amministrazione SAN"](#)
- ["Configurazione host SAN ONTAP"](#)
- ["Visualizzare e gestire i gruppi SAN Initiator in System Manager"](#)
- ["Report tecnico di NetApp 4017: Best Practice SAN Fibre Channel"](#)

## Provisioning NVMe

### Panoramica di NVMe

È possibile utilizzare il protocollo NVMe (non-volatile Memory Express) per fornire storage in un ambiente SAN. Il protocollo NVMe è ottimizzato per le performance con lo storage a stato solido.

Per NVMe, le destinazioni di storage sono chiamate namespace. Uno spazio dei nomi NVMe è una quantità di storage non volatile che può essere formattata in blocchi logici e presentata a un host come dispositivo a blocchi standard. È possibile creare spazi dei nomi e sottosistemi, quindi mappare gli spazi dei nomi ai sottosistemi, in modo simile al modo in cui i LUN vengono forniti e mappati a igroups per FC e iSCSI.

Le destinazioni NVMe sono connesse alla rete attraverso un'infrastruttura FC standard utilizzando switch FC o un'infrastruttura TCP standard utilizzando switch Ethernet e adattatori lato host.

Il supporto per NVMe varia in base alla versione di ONTAP in uso. Vedere ["Supporto e limitazioni NVMe"](#) per ulteriori informazioni.

### Che cos'è NVMe

Il protocollo NVMe (nonvolatile memory express) è un protocollo di trasporto utilizzato per accedere a supporti di storage non volatili.

NVMe over Fabrics (NVMeoF) è un'estensione di NVMe definita dalle specifiche che consente la comunicazione basata su NVMe su connessioni diverse da PCIe. Questa interfaccia consente di collegare enclosure di storage esterne a un server.

NVMe è progettato per fornire un accesso efficiente ai dispositivi di storage costruiti con memoria non volatile, dalla tecnologia flash alle tecnologie di memoria persistente dalle performance più elevate. Pertanto, non presenta le stesse limitazioni dei protocolli di storage progettati per i dischi rigidi. I dispositivi flash e a stato solido (SSD) sono un tipo di memoria non volatile (NVM). NVM è un tipo di memoria che mantiene il contenuto durante un'interruzione dell'alimentazione. NVMe è un modo per accedere a tale memoria.

I vantaggi di NVMe includono maggiori velocità, produttività, throughput e capacità per il trasferimento dei dati. Le caratteristiche specifiche includono:

- NVMe è progettato per avere fino a 64 mila code.

Ciascuna coda può avere fino a 64 mila comandi simultanei.

- NVMe è supportato da più fornitori di hardware e software
- NVMe è più produttivo grazie alle tecnologie Flash che consentono tempi di risposta più rapidi
- NVMe consente più richieste di dati per ogni "request" inviata all'SSD.

NVMe richiede meno tempo per decodificare una "request" e non richiede il blocco dei thread in un programma multithread.

- NVMe supporta funzionalità che impediscono i colli di bottiglia a livello di CPU e consentono un'elevata scalabilità con l'espansione dei sistemi.

#### **Informazioni sugli spazi dei nomi NVMe**

Uno spazio dei nomi NVMe è una quantità di memoria non volatile (NVM) che può essere formattata in blocchi logici. Gli spazi dei nomi vengono utilizzati quando una macchina virtuale di storage viene configurata con il protocollo NVMe e sono l'equivalente dei LUN per i protocolli FC e iSCSI.

Uno o più spazi dei nomi vengono forniti e connessi a un host NVMe. Ogni namespace può supportare blocchi di varie dimensioni.

Il protocollo NVMe fornisce l'accesso agli spazi dei nomi attraverso più controller. Utilizzando i driver NVMe, supportati dalla maggior parte dei sistemi operativi, gli spazi dei nomi dei dischi a stato solido (SSD) vengono visualizzati come dispositivi a blocchi standard su cui i file system e le applicazioni possono essere implementati senza alcuna modifica.

Un NSID (Namespace ID) è un identificatore utilizzato da un controller per fornire l'accesso a uno spazio dei nomi. Quando si imposta l'NSID per un host o un gruppo di host, è anche possibile configurare l'accessibilità a un volume da parte di un host. Un blocco logico può essere mappato solo a un singolo gruppo host alla volta e un dato gruppo host non dispone di NSID duplicati.

#### **Informazioni sui sottosistemi NVMe**

Un sottosistema NVMe include uno o più controller NVMe, spazi dei nomi, porte del sottosistema NVM, un supporto di storage NVM e un'interfaccia tra il controller e il supporto di storage NVM. Quando si crea uno spazio dei nomi NVMe, per impostazione predefinita, non viene mappato a un sottosistema. È inoltre possibile scegliere di mappare un sottosistema nuovo o esistente.

#### **Informazioni correlate**

- ["Eseguire il provisioning dello storage NVMe"](#)
- ["Mappare uno spazio dei nomi NVMe in un sottosistema"](#)
- ["Configurare gli host SAN e i client cloud"](#)

### Requisiti di licenza NVMe

A partire da ONTAP 9.5 è necessaria una licenza per supportare NVMe. Se NVMe è attivato in ONTAP 9.4, viene concesso un periodo di valutazione di 90 giorni per l'acquisizione della licenza dopo l'aggiornamento a ONTAP 9.5.

È possibile attivare la licenza utilizzando il seguente comando:

```
system license add -license-code NVMe_license_key
```

### Configurazione, supporto e limitazioni NVMe

A partire da ONTAP 9.4, la ["NVMe \(non-volatile Memory Express\)"](#) il protocollo è disponibile per gli ambienti SAN. FC-NVMe utilizza le stesse procedure di configurazione fisica e di zoning delle reti FC tradizionali, ma consente una maggiore larghezza di banda, IOPS aumentati e latenza ridotta rispetto a FC-SCSI.

Il supporto e le limitazioni di NVMe variano in base alla versione di ONTAP, alla piattaforma e alla configurazione. Per ulteriori informazioni sulla configurazione specifica, consultare la ["Tool di matrice di interoperabilità NetApp"](#). Per i limiti supportati, vedere ["Hardware Universe"](#).



Il numero massimo di nodi per cluster è disponibile in Hardware Universe in **combinazione di piattaforme supportate**.

### Configurazione

- Puoi configurare la tua configurazione NVMe utilizzando un singolo fabric o multi-fabric.
- È necessario configurare una LIF di gestione per ogni SVM che supporti SAN.
- L'utilizzo di fabric switch FC eterogenei non è supportato, tranne nel caso di switch blade integrati.

Le eccezioni specifiche sono elencate nella ["Tool di matrice di interoperabilità NetApp"](#).

- Cascade, Partial Mesh, full mesh, core-edge e director fabric sono tutti metodi standard di settore per collegare switch FC a un fabric e sono tutti supportati.

Un fabric può essere costituito da uno o più switch e i controller di storage possono essere collegati a più switch.

### Caratteristiche

Le seguenti funzionalità NVMe sono supportate in base alla tua versione di ONTAP.

Inizio con ONTAP...	NVMe supporta
9.12.1	Configurazioni IP MetroCluster a 4 nodi su NVMe/FC. <ul style="list-style-type: none"><li>• Le configurazioni MetroCluster non sono supportate per NVMe precedenti alla 9.12.1.</li><li>• Le configurazioni MetroCluster non sono supportate su NVMe/TCP.</li></ul>



9.10.1	Ridimensionamento di uno spazio dei nomi
9.9.1	<ul style="list-style-type: none"> <li>La coesistenza di namespace e LUN nello stesso volume.</li> </ul>
9.8	<ul style="list-style-type: none"> <li>Coesistenza del protocollo</li> </ul> <p>I protocolli SCSI, NAS e NVMe possono esistere sulla stessa Storage Virtual Machine (SVM).</p> <p>Prima di ONTAP 9,8, NVMe può essere l'unico protocollo sulla SVM.</p> <p>*</p>
9.6	<ul style="list-style-type: none"> <li>blocchi da 512 byte e blocchi da 4096 byte per namespace</li> </ul> <p>4096 è il valore predefinito. 512 deve essere utilizzato solo se il sistema operativo host non supporta blocchi da 4096 byte.</p> <ul style="list-style-type: none"> <li>Spostamento del volume con spazi dei nomi mappati</li> </ul>
9.5	Failover/sconto per coppia ha multipath.

## Protocolli

Sono supportati i seguenti protocolli NVMe.

Protocollo	Inizio con ONTAP...	Consentito da...
TCP	9.10.1	Predefinito
FC	9.4	Predefinito

A partire da ONTAP 9.8, è possibile configurare i protocolli SCSI, NAS e NVMe sulla stessa macchina virtuale per lo storage (SVM).

In ONTAP 9.7 e versioni precedenti, NVMe può essere l'unico protocollo su SVM.

## Spazi dei nomi

Quando si utilizzano gli namespace NVMe, devi essere consapevole di quanto segue:

- In caso di perdita di dati in un LUN, non è possibile ripristinarli da uno spazio dei nomi o viceversa.
- La garanzia di spazio per gli spazi dei nomi è la stessa della garanzia di spazio del volume contenente.
- Non è possibile creare uno spazio dei nomi su una transizione di volume da Data ONTAP in modalità 7.
- Gli spazi dei nomi non supportano quanto segue:
  - Ridenominazione
  - Spostamento tra volumi

- Copia inter-volume
- Copia su richiesta

#### **Ulteriori limitazioni**

**Le seguenti funzioni di ONTAP non sono supportate dalle configurazioni NVMe:**

- Sincronizza
- Virtual Storage Console

**Quanto segue si applica solo ai nodi che eseguono ONTAP 9.4:**

- Le LIF e gli spazi dei nomi NVMe devono essere ospitati sullo stesso nodo.
- Il servizio NVMe deve essere creato prima della creazione di NVMe LIF.

#### **Informazioni correlate**

["Best practice per LE SAN moderne"](#)

#### **Configurare una VM di storage per NVMe**

Se si desidera utilizzare il protocollo NVMe su un nodo, è necessario configurare la SVM in modo specifico per NVMe.


#### **Prima di iniziare**

Gli adattatori FC o Ethernet devono supportare NVMe. Gli adattatori supportati sono elencati nella ["NetApp Hardware Universe"](#).

### Esempio 8. Fasi

#### System Manager

Configurazione di una VM di storage per NVMe con Gestore di sistema di ONTAP (9.7 e versioni successive).

Per configurare NVMe su una nuova VM di storage	Per configurare NVMe su una VM di storage esistente
<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VMS</b>, quindi su <b>Add</b>.</li><li>2. Immettere un nome per la VM di storage.</li><li>3. Selezionare <b>NVMe</b> per il protocollo di accesso*.</li><li>4. Selezionare <b>Enable NVMe/FC</b> or <b>Enable NVMe/TCP</b> and <b>Save</b>.</li></ol>	<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VM</b>.</li><li>2. Fare clic sulla VM di storage che si desidera configurare.</li><li>3. Fare clic sulla scheda <b>Impostazioni</b>, quindi su  Accanto al protocollo NVMe.</li><li>4. Selezionare <b>Enable NVMe/FC</b> or <b>Enable NVMe/TCP</b> and <b>Save</b>.</li></ol>

#### CLI

Configurare una VM di storage per NVMe con l'interfaccia utente di ONTAP.

1. Se non si desidera utilizzare una SVM esistente, crearne una:

```
vserver create -vserver <SVM_name>
```

- a. Verificare che la SVM sia stata creata:

```
vserver show
```

2. Verificare che nel cluster siano installati adattatori compatibili con NVMe o TCP:

Per NVMe:

```
network fcp adapter show -data-protocols-supported fc-nvme
```

Per TCP:

```
network port show
```

3. Se si utilizza ONTAP 9.7 o versioni precedenti, rimuovere tutti i protocolli da SVM:

```
vserver remove-protocols -vserver <SVM_name> -protocols  
iscsi, fcp, nfs, cifs, ndmp
```

A partire da ONTAP 9.8, non è necessario rimuovere altri protocolli quando si aggiunge NVMe.

4. Aggiungere il protocollo NVMe a SVM:

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. Se si utilizza ONTAP 9.7 o versioni precedenti, verificare che NVMe sia l'unico protocollo consentito su SVM:

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe deve essere l'unico protocollo visualizzato in `allowed protocols` colonna.

6. Creare il servizio NVMe:

```
vserver nvme create -vserver <SVM_name>
```

7. Verificare che il servizio NVMe sia stato creato:

```
vserver nvme show -vserver <SVM_name>
```

Il `Administrative Status Della SVM` deve essere elencata come `up`.

8. Creare una LIF NVMe/FC:

- Per ONTAP 9.9.1 o versione precedente, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>  
-role data -data-protocol fc-nvme -home-node <home_node> -home  
-port <home_port>
```

- Per ONTAP 9.10.1 o versione successiva, FC o TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>  
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>  
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>  
-home-port <home_port> -status-admin up -failover-policy disabled  
-firewall-policy data -auto-revert false -failover-group  
<failover_group> -is-dns-update-enabled false
```

9. Creare una LIF NVMe/FC sul nodo partner ha:

- Per ONTAP 9.9.1 o versione precedente, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

- Per ONTAP 9.10.1 o versione successiva, FC o TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fcp | fc-nvme | nvme-tcp> -home-node <home_node>
-home-port <home_port> -status-admin up -failover-policy disabled
-firewall-policy data -auto-revert false -failover-group
<failover_group> -is-dns-update-enabled false
```

10. Verificare che le LIF NVMe/FC siano state create:

```
network interface show -vserver <SVM_name>
```

11. Creare un volume sullo stesso nodo di LIF:

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

Se viene visualizzato un messaggio di avviso relativo al criterio di efficienza automatica, è possibile ignorarlo in modo sicuro.

## Eeguire il provisioning dello storage NVMe

Utilizza questi passaggi per creare namespace ed eseguire il provisioning dello storage per qualsiasi host NVMe supportato su una VM di storage esistente.

A partire da ONTAP 9.8, quando si esegue il provisioning dello storage, la qualità del servizio viene attivata per impostazione predefinita. È possibile disattivare la QoS o scegliere una policy QoS personalizzata durante il processo di provisioning o in un secondo momento.

### Prima di iniziare

La VM di storage deve essere configurata per NVME e il trasporto FC o TCP deve essere già impostato.

## System Manager

Utilizzando Gestione di sistema di ONTAP (9.7 e versioni successive), creare spazi dei nomi per fornire lo storage utilizzando il protocollo NVMe.

### Fasi

1. In System Manager, fare clic su **Storage > NVMe Namespaces**, quindi fare clic su **Add**.

Per creare un nuovo sottosistema, fare clic su **altre opzioni**.

2. Se si utilizza ONTAP 9.8 o versione successiva e si desidera disattivare la qualità del servizio o scegliere un criterio di qualità del servizio personalizzato, fare clic su **altre opzioni**, quindi in **archiviazione e ottimizzazione** selezionare **livello di servizio delle prestazioni**.
3. Zone your FC switch by WWPN (zone switch FC in base al numero WWPN Utilizzare una zona per iniziatore e includere tutte le porte di destinazione in ciascuna zona).
4. Sul tuo host, scopri i nuovi spazi dei nomi.
5. Inizializzare lo spazio dei nomi e formattarlo con un file system.
6. Verificare che l'host sia in grado di scrivere e leggere i dati sullo spazio dei nomi.

### CLI

Utilizzando l'interfaccia CLI di ONTAP, creare spazi dei nomi per fornire storage utilizzando il protocollo NVMe.

Questa procedura crea uno spazio dei nomi e un sottosistema NVMe su una VM di storage esistente già configurata per il protocollo NVMe, quindi mappa lo spazio dei nomi al sottosistema per consentire l'accesso ai dati dal sistema host.

Per configurare la VM di storage per NVMe, vedere ["Configurare una SVM per NVMe"](#).

### Fasi

1. Verificare che la SVM sia configurata per NVMe:

```
vserver show -vserver <svm_name> -fields allowed-protocols
```

NVMe dovrebbe essere visualizzato sotto `allowed-protocols` colonna.

2. Creare lo spazio dei nomi NVMe:

```
vserver nvme namespace create -vserver <svm_name> -path <path> -size  
<size_of_namespace> -ostype <OS_type>
```

3. Creare il sottosistema NVMe:

```
vserver nvme subsystem create -vserver <svm_name> -subsystem  
<name_of_subsystem> -ostype <OS_type>
```

Il nome del sottosistema NVMe rileva la distinzione tra maiuscole e minuscole. Deve contenere da 1 a 96 caratteri. Sono consentiti caratteri speciali.

4. Verificare che il sottosistema sia stato creato:

```
vserver nvme subsystem show -vserver <svm_name>
```

Il nvme il sottosistema deve essere visualizzato sotto Subsystem colonna.

5. Ottenere l'NQN dall'host.

6. Aggiungere l'NQN host al sottosistema:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN>
```

7. Mappare lo spazio dei nomi nel sottosistema:

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem  
<subsystem_name> -path <path>
```

Uno spazio dei nomi può essere mappato solo a un singolo sottosistema.

8. Verificare che lo spazio dei nomi sia mappato al sottosistema:

```
vserver nvme namespace show -vserver <svm_name> -instance
```

Il sottosistema deve essere elencato come Attached subsystem.

## Mappare uno spazio dei nomi NVMe in un sottosistema

L'associazione di un namespace NVMe a un sottosistema consente l'accesso ai dati dall'host. È possibile mappare un namespace NVMe a un sottosistema quando si esegue il provisioning dello storage oppure è possibile farlo dopo che è stato eseguito il provisioning dello storage.

A partire da ONTAP 9.14.1, è possibile assegnare priorità all'allocazione delle risorse per host specifici. Per impostazione predefinita, quando un host viene aggiunto al sottosistema NVMe, viene assegnata una priorità regolare. È possibile utilizzare l'interfaccia a riga di comando (CLI) di ONTAP per modificare manualmente la priorità predefinita da normale ad alta. Agli host assegnati una priorità alta viene assegnato un numero maggiore di code i/o e profondità di coda.



Se si desidera assegnare una priorità elevata a un host aggiunto a un sottosistema in ONTAP 9.13.1 o versioni precedenti, è possibile farlo [modificare la priorità dell'host](#).

## Prima di iniziare

Lo spazio dei nomi e il sottosistema devono essere già creati. Per creare uno spazio dei nomi e un sottosistema, vedere ["Eseguire il provisioning dello storage NVMe"](#).

## Fasi

1. Ottenere l'NQN dall'host.
2. Aggiungere l'NQN host al sottosistema:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

Se si desidera modificare la priorità predefinita dell'host da normale ad alta, utilizzare `-priority high` opzione. Questa opzione è disponibile a partire da ONTAP 9.14.1.

3. Mappare lo spazio dei nomi nel sottosistema:

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem  
<subsystem_name> -path <path>
```

Uno spazio dei nomi può essere mappato solo a un singolo sottosistema.

4. Verificare che lo spazio dei nomi sia mappato al sottosistema:

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

Il sottosistema deve essere elencato come `Attached subsystem`.

## Gestire le LUN

### Modificare il gruppo di criteri QoS LUN

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per assegnare o rimuovere i criteri di qualità del servizio (QoS) su più LUN contemporaneamente.



Se il criterio QoS è assegnato a livello di volume, deve essere modificato a livello di volume. È possibile modificare il criterio QoS a livello di LUN solo se è stato originariamente assegnato a livello di LUN.

## Fasi

1. In System Manager, fare clic su **Storage > LUN**.
2. Selezionare il LUN o i LUN che si desidera modificare.

Se si modificano più LUN alla volta, le LUN devono appartenere alla stessa Storage Virtual Machine (SVM). Se si selezionano LUN che non appartengono alla stessa SVM, l'opzione per modificare il gruppo di criteri QoS non viene visualizzata.



3. Fare clic su **More** (Altro) e selezionare **Edit QoS Policy Group** (Modifica gruppo policy QoS).

### Convertire un LUN in uno spazio dei nomi

A partire da ONTAP 9.11.1, è possibile utilizzare l'interfaccia CLI di ONTAP per convertire un LUN esistente in uno spazio dei nomi NVMe.

#### Di cosa hai bisogno

- Il LUN specificato non deve avere mappe esistenti per un igroup.
- Il LUN non deve trovarsi in una SVM configurata con MetroCluster o in una relazione SM-BC.
- Il LUN non deve essere un endpoint del protocollo o un endpoint del protocollo.
- Il LUN non deve avere un prefisso diverso da zero e/o un flusso di suffissi diverso da zero.
- Il LUN non deve far parte di uno snapshot o della relazione di destinazione di SnapMirror come LUN di sola lettura.

#### Fase

1. Convertire una LUN in un namespace NVMe:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```


### Portare un LUN offline

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione di sistema per disattivare le LUN. Prima di ONTAP 9.10.1, è necessario utilizzare l'interfaccia utente di ONTAP per disattivare le LUN.

## System Manager

### Fasi

1. In System Manager, fare clic su **Storage>LUN**.
2. Portare una singola LUN o più LUN offline

Se si desidera...	Eeguire questa operazione...
Portare una singola LUN offline	Accanto al nome del LUN, fare clic su  E selezionare <b>take Offline</b> .
Portare più LUN offline	<ol style="list-style-type: none"><li>1. Selezionare i LUN che si desidera disattivare.</li><li>2. Fare clic su <b>More</b> (Altro) e selezionare <b>take Offline</b> (non in linea).</li></ol>

### CLI

Quando si utilizza l'interfaccia CLI, è possibile scollegare un solo LUN alla volta.

### Fase

1. Portare il LUN offline:

```
lun offline <lun_name> -vserver <SVM_name>
```

## Ridimensionare un LUN

È possibile aumentare o diminuire le dimensioni di un LUN.



Impossibile ridimensionare le LUN Solaris.

### Aumentare le dimensioni di un LUN

Le dimensioni del LUN possono variare a seconda della versione di ONTAP in uso.

Versione di ONTAP	Dimensione massima del LUN
ONTAP 9.12.1P2 e versioni successive	128 TB per piattaforme AFF, FAS e ASA
ONTAP 9.8 e versioni successive	<ul style="list-style-type: none"><li>• 128 TB per le piattaforme ASA (All-Flash SAN Array)</li><li>• 16 TB per piattaforme non ASA</li></ul>
ONTAP 9.5, 9.6, 9.7	16 TB

ONTAP 9.4 o versioni precedenti	10 volte la dimensione del LUN originale, ma non superiore a 16 TB, che corrisponde alla dimensione massima del LUN. Ad esempio, se si crea un LUN da 100 GB, è possibile farlo crescere solo fino a 1,000 GB. La dimensione massima effettiva del LUN potrebbe non essere esattamente di 16 TB. ONTAP arrotonda il limite per essere leggermente inferiore.
---------------------------------	--


Non è necessario portare il LUN offline per aumentare le dimensioni. Tuttavia, dopo aver aumentato le dimensioni, è necessario eseguire nuovamente la scansione del LUN sull'host per consentire all'host di riconoscere la modifica delle dimensioni.

Vedere la pagina di riferimento dei comandi per `lun resize` Per ulteriori informazioni sul ridimensionamento di un LUN.

### Esempio 9. Fasi

#### System Manager

Aumenta le dimensioni di un LUN con Gestione di sistema di ONTAP (9.7 e versioni successive).

1. In System Manager, fare clic su **Storage > LUN**.
2. Fare clic su  E selezionare **Modifica**.
3. In **Storage and Optimization** (Storage e ottimizzazione), aumentare le dimensioni del LUN e di **Save** (Salva).

#### CLI

Aumentare le dimensioni di un LUN con l'interfaccia CLI di ONTAP.

1. Aumentare le dimensioni del LUN:

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

2. Verificare l'aumento delle dimensioni del LUN:

```
lun show -vserver <SVM_name_>
```

Le operazioni ONTAP arrotondano la dimensione massima effettiva del LUN, in modo che sia leggermente inferiore al valore previsto. Inoltre, le dimensioni effettive del LUN potrebbero variare leggermente in base al tipo di sistema operativo del LUN. Per ottenere il valore esatto ridimensionato, eseguire i seguenti comandi in modalità avanzata:

```
set -unit B
```

```
lun show -fields max-resize-size -volume volume_name -lun lun_name
```

1. Eseguire nuovamente la scansione del LUN sull'host.
2. Seguire la documentazione dell'host per rendere visibile la dimensione del LUN appena creato al file system host.

### Ridurre le dimensioni di un LUN

Prima di ridurre le dimensioni di un LUN, l'host deve migrare i blocchi contenenti i dati del LUN nel limite delle dimensioni del LUN più piccole. È necessario utilizzare uno strumento come SnapCenter per garantire che il LUN venga ridotto correttamente senza troncature i blocchi contenenti dati LUN. Si sconsiglia di ridurre manualmente le dimensioni del LUN.

Una volta ridotte le dimensioni del LUN, ONTAP notifica automaticamente all'iniziatore che le dimensioni del LUN sono diminuite. Tuttavia, potrebbero essere necessari ulteriori passaggi sull'host per il riconoscimento delle nuove dimensioni del LUN. Consultare la documentazione dell'host per informazioni specifiche sulla riduzione delle dimensioni della struttura del file host.

### Spostare un LUN

È possibile spostare un LUN tra i volumi all'interno di una macchina virtuale di storage (SVM), ma non è possibile spostare un LUN tra le SVM. Le LUN spostate tra i volumi all'interno di una SVM vengono spostate immediatamente e senza perdita di connettività.

#### Di cosa hai bisogno

Se il LUN utilizza la mappa LUN selettiva (SLM, Selective LUN Map), è necessario farlo ["Modificare l'elenco dei nodi di reporting SLM"](#) Includere il nodo di destinazione e il partner ha prima di spostare la LUN.

#### A proposito di questa attività

Le funzionalità di efficienza dello storage, come deduplica, compressione e compattazione, non vengono mantenute durante uno spostamento del LUN. Devono essere riapplicati una volta completato lo spostamento del LUN.

La protezione dei dati attraverso le copie Snapshot avviene a livello di volume. Pertanto, quando si sposta un LUN, questo rientra nello schema di protezione dei dati del volume di destinazione. Se non sono state create copie Snapshot per il volume di destinazione, le copie Snapshot del LUN non vengono create. Inoltre, tutte le copie Snapshot del LUN rimangono nel volume originale fino all'eliminazione delle copie Snapshot.

Non è possibile spostare un LUN nei seguenti volumi:

- Un volume di destinazione SnapMirror
- Il volume root SVM

Non è possibile spostare i seguenti tipi di LUN:

- LUN creata da un file
- LUN in stato NVFail
- Un LUN che si trova in una relazione di condivisione del carico
- Un LUN di classe protocollo-endpoint



Per i LUN Solaris os\_TYPE di 1 TB o superiore, l'host potrebbe riscontrare un timeout durante lo spostamento del LUN. Per questo tipo di LUN, è necessario smontare il LUN prima di iniziare lo spostamento.


## Esempio 10. Fasi

### System Manager

Spostamento di un LUN con Gestore di sistema di ONTAP (9.7 e versioni successive).

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per creare un nuovo volume quando si sposta una singola LUN. In ONTAP 9.8 e 9.9.1, il volume su cui si sposta il LUN deve esistere prima di iniziare lo spostamento del LUN.

#### Fasi

1. In System Manager, fare clic su **Storage>LUN**.
2. Fare clic con il pulsante destro del mouse sul LUN che si desidera spostare, quindi fare clic su  E selezionare **Move LUN** (Sposta LUN).

In ONTAP 9.10.1, selezionare per spostare il LUN su **un volume esistente** o su **nuovo volume**.

Se si sceglie di creare un nuovo volume, fornire le specifiche del volume.

3. Fare clic su **Sposta**.

### CLI

Spostare un LUN con l'interfaccia utente di ONTAP.

1. Spostare il LUN:

```
lun move start
```

Durante un breve periodo di tempo, il LUN è visibile sia sul volume di origine che su quello di destinazione. Questo è previsto e viene risolto al termine del trasferimento.

2. Tenere traccia dello stato dello spostamento e verificare che il completamento sia stato completato correttamente:

```
lun move show
```

### Informazioni correlate

- ["Mappa LUN selettiva"](#)

### Elimina LUN

È possibile eliminare un LUN da una macchina virtuale di storage (SVM) se non è più necessario il LUN.

## Di cosa hai bisogno

Il LUN deve essere dismappato dal relativo igroup prima di poterlo eliminare.

## Fasi

1. Verificare che l'applicazione o l'host non stia utilizzando il LUN.
2. Dismappare il LUN dall'igroup:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun  
<LUN_name> -igroup <igroup_name>
```

3. Eliminare il LUN:

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Verificare che il LUN sia stato eliminato:

```
lun show -vserver <SVM_name>
```

Vserver	Path	State	Mapped	Type	Size
vs5	/vol/vol16/lun8	online	mapped	windows	10.00GB

## Cosa fare prima di copiare le LUN

Prima di copiare un LUN, è necessario essere a conoscenza di alcuni elementi.

Gli amministratori dei cluster possono copiare un LUN tra le macchine virtuali di storage (SVM) all'interno del cluster utilizzando `lun copy` comando. Gli amministratori dei cluster devono stabilire la relazione di peering della macchina virtuale di storage (SVM) utilizzando `vserver peer create` Prima di eseguire un'operazione di copia del LUN tra SVM. Lo spazio nel volume di origine deve essere sufficiente per un clone del SIS.

Le LUN nelle copie Snapshot possono essere utilizzate come LUN di origine per `lun copy` comando. Quando si copia un LUN utilizzando `lun copy` La copia del LUN è immediatamente disponibile per l'accesso in lettura e scrittura. Il LUN di origine rimane invariato grazie alla creazione di una copia del LUN. Sia il LUN di origine che la copia del LUN esistono come LUN univoci con numeri di serie LUN diversi. Le modifiche apportate al LUN di origine non si riflettono nella copia del LUN e le modifiche apportate alla copia del LUN non si riflettono nel LUN di origine. La mappatura LUN del LUN di origine non viene copiata nel nuovo LUN; la copia del LUN deve essere mappata.

La protezione dei dati attraverso le copie Snapshot avviene a livello di volume. Pertanto, se si copia un LUN in un volume diverso dal volume del LUN di origine, il LUN di destinazione rientra nello schema di protezione dei dati del volume di destinazione. Se non sono state create copie Snapshot per il volume di destinazione, le copie Snapshot della copia LUN non vengono create.

La copia delle LUN è un'operazione senza interruzioni.

Non è possibile copiare i seguenti tipi di LUN:

- LUN creata da un file
- LUN in stato NVFAIL
- Un LUN che si trova in una relazione di condivisione del carico
- Un LUN di classe protocollo-endpoint

### Esaminare lo spazio configurato e utilizzato di un LUN

Conoscere lo spazio configurato e lo spazio effettivo utilizzato per le LUN può aiutare a determinare la quantità di spazio che può essere recuperato durante la rigenerazione dello spazio, la quantità di spazio riservato contenente dati e la dimensione totale configurata rispetto alla dimensione effettiva utilizzata per una LUN.

#### Fase

1. Visualizzare lo spazio configurato rispetto allo spazio effettivo utilizzato per un LUN:

```
lun show
```

L'esempio seguente mostra lo spazio configurato rispetto allo spazio effettivo utilizzato dalle LUN nella SVM (Storage Virtual Machine) vs3:

```
lun show -vserver vs3 -fields path, size, size-used, space-reserve
```

vserver	path	size	space-reserve	size-used
vs3	/vol/vol10/lun1	50.01GB	disabled	25.00GB
vs3	/vol/vol10/lun1_backup	50.01GB	disabled	32.15GB
vs3	/vol/vol10/lun2	75.00GB	disabled	0B
vs3	/vol/volspace/lun0	5.00GB	enabled	4.50GB

4 entries were displayed.

### Abilitare l'allocazione dello spazio per LUN con thin provisioning SCSI

Se l'host supporta il thin provisioning SCSI, è possibile attivare l'allocazione dello spazio per i LUN SCSI con thin provisioning in ONTAP. Quando l'allocazione dello spazio è attivata, ONTAP invia una notifica all'host quando lo spazio del volume è esaurito e il LUN del volume non può accettare scritture. ONTAP recupera automaticamente anche spazio quando l'host elimina i dati.

Negli host che non supportano il thin provisioning SCSI, quando il volume contenente il LUN esaurisce lo spazio e non può crescere automaticamente, ONTAP porta il LUN offline. Sugli host che supportano il thin provisioning SCSI, ONTAP non porta il LUN offline quando si esaurisce lo spazio. Il LUN rimane in linea in modalità di sola lettura e all'host viene notificato che il LUN non può più accettare le scritture.

Inoltre, quando i dati vengono eliminati su un host che supporta il thin provisioning SCSI, la gestione dello

spazio sul lato host identifica i blocchi di dati eliminati sul file system host ed emette automaticamente uno o più SCSI UNMAP comandi per liberare i blocchi corrispondenti sul sistema storage.

### Prima di iniziare

Per attivare l'allocazione dello spazio, il thin provisioning SCSI deve essere supportato dall'host. Il thin provisioning SCSI utilizza il provisioning a blocchi logici come definito nello standard SCSI SBC-3. Solo gli host che supportano questo standard possono utilizzare il thin provisioning SCSI in ONTAP.

I seguenti host attualmente supportano il thin provisioning SCSI quando si attiva l'allocazione dello spazio:

- Citrix XenServer 6,5 e versioni successive
- ESXi 5,0 e versioni successive
- Kernel Oracle Linux 6,2 UEK o versione successiva
- RHEL 6,2 e versioni successive
- SLES11 e versioni successive
- Solaris 11,1 e versioni successive
- Windows

### A proposito di questa attività

Per impostazione predefinita, l'allocazione dello spazio è disattivata per tutti i LUN. Per attivare l'allocazione dello spazio, è necessario portare il LUN in modalità non in linea; quindi è necessario eseguire la ricerca sull'host prima che l'host riconosca che l'allocazione dello spazio è stata abilitata.

### Fasi

1. Portare il LUN offline.

```
lun modify -vserver vserver_name -volume volume_name -lun lun_name  
-state offline
```

2. Attiva allocazione spazio:

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-space-allocation enabled
```

3. Verificare che l'allocazione dello spazio sia attivata:

```
lun show -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-fields space-allocation
```

4. Portare il LUN online:

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-state online
```



5. Sull'host, eseguire nuovamente la scansione di tutti i dischi per assicurarsi che la modifica apportata a `-space-allocation` l'opzione è stata rilevata correttamente.

## Controllo e monitoraggio delle performance i/o per le LUN utilizzando la QoS dello storage

È possibile controllare le prestazioni di input/output (i/o) alle LUN assegnando LUN ai gruppi di criteri Storage QoS. È possibile controllare le performance di i/o per garantire che i carichi di lavoro raggiungano specifici obiettivi di performance o per ridurre il carico di lavoro che ha un impatto negativo su altri carichi di lavoro.

### A proposito di questa attività

I gruppi di policy applicano un limite massimo di throughput (ad esempio, 100 MB/s). È possibile creare un gruppo di criteri senza specificare un throughput massimo, che consente di monitorare le performance prima di controllare il carico di lavoro.

È inoltre possibile assegnare le macchine virtuali di storage (SVM) con volumi FlexVol e LUN ai gruppi di policy.

Tenere presente i seguenti requisiti relativi all'assegnazione di un LUN a un gruppo di criteri:

- Il LUN deve essere contenuto dalla SVM a cui appartiene il gruppo di criteri.

Specificare la SVM quando si crea il gruppo di criteri.

- Se si assegna un LUN a un gruppo di criteri, non è possibile assegnare il volume o la SVM contenente i LUN a un gruppo di criteri.

Per ulteriori informazioni sull'utilizzo di Storage QoS, consultare ["Riferimento per l'amministrazione del sistema"](#).

### Fasi

1. Utilizzare `qos policy-group create` per creare un gruppo di criteri.
2. Utilizzare `lun create` o il `lun modify` con il `-qos-policy-group` Parametro per assegnare un LUN a un gruppo di criteri.
3. Utilizzare `qos statistics` comandi per visualizzare i dati delle performance.
4. Se necessario, utilizzare `qos policy-group modify` comando per regolare il limite massimo di throughput del gruppo di criteri.

## Strumenti disponibili per monitorare efficacemente le LUN

Sono disponibili strumenti che consentono di monitorare efficacemente le LUN ed evitare di esaurire lo spazio disponibile.

- Active IQ Unified Manager è uno strumento gratuito che ti consente di gestire tutto lo storage in tutti i cluster del tuo ambiente.
- System Manager è un'interfaccia utente grafica integrata in ONTAP che consente di gestire manualmente le esigenze di storage a livello di cluster.
- OnCommand Insight offre una singola vista dell'infrastruttura storage e consente di impostare il monitoraggio automatico, gli avvisi e i report quando LUN, volumi e aggregati stanno esaurendo lo spazio di storage.

## Funzionalità e limitazioni delle LUN in transizione

In un ambiente SAN, è necessario un'interruzione del servizio durante la transizione di un volume 7-Mode a ONTAP. Per completare la transizione, è necessario spegnere gli host. Dopo la transizione, è necessario aggiornare le configurazioni host prima di poter iniziare a fornire i dati in ONTAP.

È necessario pianificare una finestra di manutenzione durante la quale è possibile arrestare gli host e completare la transizione.

I LUN che sono stati trasferiti da Data ONTAP in 7-Mode a ONTAP presentano alcune funzionalità e restrizioni che influiscono sul modo in cui è possibile gestire i LUN.

Con i LUN in transizione è possibile effettuare le seguenti operazioni:

- Visualizzare il LUN utilizzando `lun show` comando
- Visualizzare l'inventario delle LUN in transizione dal volume 7-Mode utilizzando `transition 7-mode show` comando
- Ripristinare un volume da una copia Snapshot 7-Mode

Ripristino delle transizioni del volume di tutte le LUN acquisite nella copia Snapshot

- Ripristinare una singola LUN da una copia Snapshot 7-Mode utilizzando `snapshot restore-file` comando
- Creare un clone di un LUN in una copia Snapshot 7-Mode
- Ripristinare una serie di blocchi da un LUN acquisito in una copia Snapshot 7-Mode
- Creare un FlexClone del volume utilizzando una copia Snapshot 7-Mode

Non è possibile eseguire le seguenti operazioni con LUN in transizione:

- Accedere ai cloni LUN Snapshot con copia supportata catturati nel volume

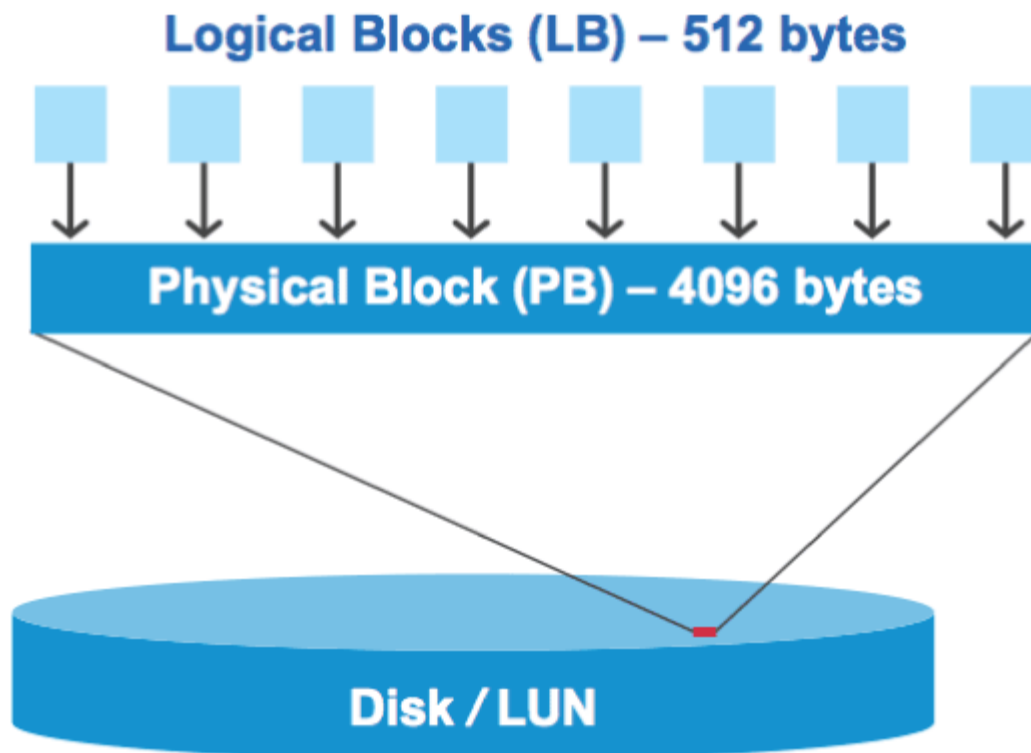
## Informazioni correlate

["Transizione basata sulla copia"](#)

## Panoramica dei disallineamenti i/o sui LUN allineati correttamente

ONTAP potrebbe segnalare disallineamenti i/o su LUN correttamente allineati. In generale, questi avvisi di disallineamento possono essere ignorati se si è certi che il LUN sia correttamente configurato e che la tabella di partizione sia corretta.

I LUN e i dischi rigidi forniscono lo storage come blocchi. Poiché la dimensione del blocco per i dischi sull'host è di 512 byte, i LUN presentano blocchi di tale dimensione all'host, utilizzando blocchi di dimensioni maggiori da 4 KB per memorizzare i dati. Il blocco di dati a 512 byte utilizzato dall'host viene definito blocco logico. Il blocco di dati da 4 KB utilizzato dal LUN per memorizzare i dati viene definito blocco fisico. Ciò significa che ogni blocco fisico da 4 KB contiene otto blocchi logici da 512 byte.



Il sistema operativo host può avviare un'operazione di i/o in lettura o scrittura in qualsiasi blocco logico. Le operazioni di i/o vengono considerate allineate solo quando iniziano dal primo blocco logico del blocco fisico. Se un'operazione di i/o inizia in un blocco logico che non è anche l'inizio di un blocco fisico, l'i/o viene considerato disallineato. ONTAP rileva automaticamente il disallineamento e lo segnala sul LUN. Tuttavia, la presenza di i/o disallineati non significa necessariamente che anche il LUN sia disallineato. È possibile che i/o disallineati vengano segnalati su LUN allineati correttamente.

Per ulteriori indagini, consultare l'articolo della Knowledge base ["Come identificare i/o non allineati sulle LUN?"](#)

Per ulteriori informazioni sugli strumenti per la correzione dei problemi di allineamento, consultare la seguente documentazione: +

- ["Windows Unified host Utilities 7.1"](#)
- ["Guida all'installazione e all'amministrazione di Virtual Storage Console per VMware vSphere"](#)

#### Ottenere l'allineamento i/o utilizzando i tipi di sistema operativo LUN

Per ONTAP 9,7 o versioni precedenti, è necessario utilizzare il LUN ONTAP consigliato `ostype` Valore che si avvicina maggiormente al sistema operativo per ottenere l'allineamento i/o con lo schema di partizionamento del sistema operativo.

Lo schema di partizione utilizzato dal sistema operativo host è un importante fattore che contribuisce ai disallineamenti i/o. Alcune LUN ONTAP `ostype` i valori utilizzano uno speciale offset noto come "prefix" per consentire l'allineamento dello schema di partizione predefinito utilizzato dal sistema operativo host.



In alcuni casi, potrebbe essere necessaria una tabella di partizione personalizzata per ottenere l'allineamento i/o. Tuttavia, per `ostype` valori con un valore "prefix" maggiore di 0, Una partizione personalizzata potrebbe creare un i/o disallineato

Per ulteriori informazioni sui LUN di cui è stato eseguito il provisioning in ONTAP 9,7 o versioni precedenti, consultare l'articolo della Knowledge base ["Come identificare i/o non allineati sui LUN"](#).



Per impostazione predefinita, i nuovi LUN con provisioning in ONTAP 9,8 o versioni successive dispongono di un prefisso e di una dimensione del suffisso pari a zero per tutti i tipi di sistema operativo LUN. Per impostazione predefinita, l'i/o deve essere allineato con il sistema operativo host supportato.

#### Considerazioni speciali sull'allineamento i/o per Linux

Le distribuzioni Linux offrono un'ampia gamma di modi per utilizzare un LUN, tra cui dispositivi raw per database, diversi gestori di volumi e file system. Non è necessario creare partizioni su un LUN se utilizzato come dispositivo raw o come volume fisico in un volume logico.

Per RHEL 5 e versioni precedenti e SLES 10 e versioni precedenti, se il LUN verrà utilizzato senza un gestore di volumi, è necessario partizionare il LUN in modo che una partizione inizi con un offset allineato, ovvero un settore che è anche un multiplo di otto blocchi logici.

#### Considerazioni sull'allineamento i/o speciali per i LUN Solaris

È necessario considerare diversi fattori quando si determina se utilizzare `solaris ostype` o il `solaris_efi` tipo di sistema operativo.

Vedere ["Guida all'installazione e all'amministrazione di Solaris host Utilities"](#) per informazioni dettagliate.

#### Le LUN di avvio ESX riportano un disallineamento

Le LUN utilizzate come LUN di boot ESX vengono in genere segnalate da ONTAP come disallineate. ESX crea più partizioni sul LUN di boot, rendendo molto difficile l'allineamento. Le LUN di boot ESX disallineate non sono generalmente un problema di performance perché la quantità totale di i/o disallineati è ridotta. Presupponendo che il LUN sia stato correttamente configurato con VMware `ostype`, non è necessaria alcuna azione.

#### Informazioni correlate

["Allineamento partizione/disco del file system delle macchine virtuali guest per VMware vSphere, altri ambienti virtuali e sistemi di storage NetApp"](#)

#### Modi per risolvere i problemi quando i LUN passano offline

Quando non è disponibile spazio per le scritture, le LUN passano offline per preservare l'integrità dei dati. Le LUN possono esaurire lo spazio e andare offline per diversi motivi, oltre a diversi modi per risolvere il problema.

Se...	È possibile...
Aggregato pieno	<ul style="list-style-type: none"><li>• Aggiungere altri dischi.</li><li>• Utilizzare <code>volume modify</code> comando per ridurre un volume con spazio disponibile.</li><li>• Se si dispone di volumi con garanzia di spazio che dispongono di spazio disponibile, impostare la garanzia di spazio del volume su <code>none</code> con <code>volume modify</code> comando.</li></ul>

Se...	È possibile...
Il volume è pieno ma c'è spazio disponibile nell'aggregato contenente	<ul style="list-style-type: none"> <li>• Per i volumi di garanzia dello spazio, utilizzare <code>volume modify</code> per aumentare le dimensioni del volume.</li> <li>• Per i volumi con thin provisioning, utilizzare <code>volume modify</code> per aumentare le dimensioni massime del volume.</li> </ul> <p>Se la crescita automatica del volume non è attivata, utilizzare <code>volume modify -autogrow -mode</code> per attivarlo.</p> <ul style="list-style-type: none"> <li>• Eliminare manualmente le copie Snapshot con <code>volume snapshot delete</code> oppure utilizzare il comando <code>volume snapshot autodelete modify</code> Comando per eliminare automaticamente le copie Snapshot.</li> </ul>

#### Informazioni correlate

["Gestione di dischi e Tier locali \(aggregato\)"](#)

["Gestione dello storage logico"](#)

#### Eseguire il troubleshooting dei LUN iSCSI non visibili sull'host

I LUN iSCSI vengono visualizzati come dischi locali per l'host. Se i LUN del sistema di storage non sono disponibili come dischi sull'host, verificare le impostazioni di configurazione.

Impostazione di configurazione	Cosa fare
Cablaggio	Verificare che i cavi tra l'host e il sistema di storage siano collegati correttamente.
Connettività di rete	<p>Verificare che vi sia una connettività TCP/IP tra l'host e il sistema di storage.</p> <ul style="list-style-type: none"> <li>• Dalla riga di comando del sistema storage, eseguire il ping delle interfacce host utilizzate per iSCSI: <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre> </li> <li>• Dalla riga di comando dell'host, eseguire il ping delle interfacce del sistema di storage utilizzate per iSCSI: <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre> </li> </ul>

Impostazione di configurazione	Cosa fare
Requisiti di sistema	Verificare che i componenti della configurazione siano qualificati. Inoltre, verificare di disporre del livello corretto del service pack del sistema operativo host (OS), della versione initiator, della versione di ONTAP e di altri requisiti di sistema. La matrice di interoperabilità contiene i requisiti di sistema più aggiornati.
Frame jumbo	Se si utilizzano frame jumbo nella configurazione, verificare che i frame jumbo siano attivati su tutti i dispositivi nel percorso di rete: La NIC Ethernet host, il sistema di storage e gli switch.
Stato del servizio iSCSI	Verificare che il servizio iSCSI sia concesso in licenza e avviato sul sistema storage.
Accesso initiator	Verificare che l'iniziatore sia connesso al sistema di storage. Se il <code>iscsi initiator show</code> l'output del comando indica che non sono stati registrati iniziatori. controllare la configurazione dell'iniziatore sull'host. Verificare inoltre che il sistema di storage sia configurato come destinazione dell'iniziatore.
Nomi dei nodi iSCSI (IQN)	Verificare di utilizzare i nomi dei nodi iniziatori corretti nella configurazione igroup. Sull'host, è possibile utilizzare i comandi e gli strumenti di initiator per visualizzare il nome del nodo di initiator. I nomi dei nodi iniziatori configurati nell'igroup e sull'host devono corrispondere.
Mappature LUN	Verificare che i LUN siano mappati a un igroup. Nella console del sistema di storage, è possibile utilizzare uno dei seguenti comandi: <ul style="list-style-type: none"> <li><code>lun mapping show</code> Visualizza tutti i LUN e gli igroups a cui sono associati.</li> <li><code>lun mapping show -igroup</code> Visualizza i LUN mappati a un igroup specifico.</li> </ul>
Le LIF iSCSI sono abilitate	Verificare che le interfacce logiche iSCSI siano attivate.

#### Informazioni correlate

["Tool di matrice di interoperabilità NetApp"](#)

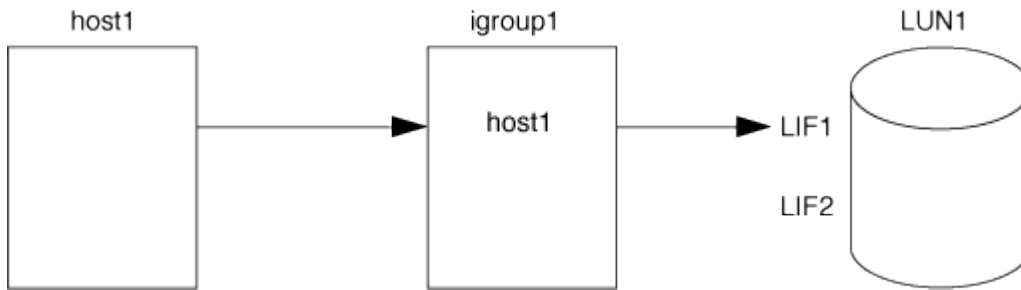
## Gestire igroups e portset

### Metodi per limitare l'accesso LUN con portset e igroups

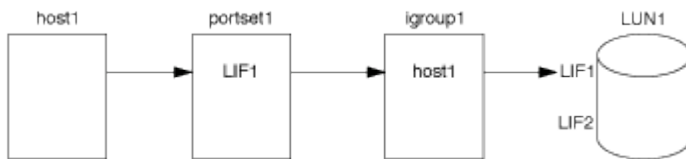
Oltre a utilizzare la mappa LUN selettiva (SLM), è possibile limitare l'accesso ai LUN tramite igroups e portset.

I portset possono essere utilizzati con SLM per limitare ulteriormente l'accesso di determinate destinazioni a determinati iniziatori. Quando si utilizza SLM con i portset, i LUN saranno accessibili sull'insieme di LIF nel portset sul nodo che possiede il LUN e sul partner ha di quel nodo.

Nell'esempio seguente, initiator1 non ha un portset. Senza un portset, l'iniziator1 può accedere a LUN1 tramite LIF e LISF2.



È possibile limitare l'accesso a LUN1 utilizzando un portset. Nell'esempio seguente, l'iniziatore1 può accedere a LUN1 solo tramite LIF. Tuttavia, l'iniziatore1 non può accedere a LUN1 tramite LISF2 perché LISF2 non si trova in portset1.



#### Informazioni correlate

- [Mappa LUN selettiva](#)
- [Creare un portset e associarlo a un igroup](#)

#### Visualizza e gestisci GLI iniziatori SAN e igroups

È possibile utilizzare System Manager per visualizzare e gestire i gruppi di iniziatori (igroups) e gli iniziatori.

##### A proposito di questa attività

- I gruppi di iniziatori identificano gli host in grado di accedere a LUN specifiche sul sistema di storage.
- Una volta creati un gruppo iniziatore e un gruppo iniziatore, è possibile modificarli o eliminarli.
- Per gestire i gruppi di iniziatori SAN e gli iniziatori, è possibile eseguire le seguenti attività:
  - [\[view-manage-san-igroups\]](#)
  - [\[view-manage-san-inits\]](#)

#### Visualizzare e gestire i gruppi SAN Initiator

È possibile utilizzare System Manager per visualizzare un elenco di gruppi di iniziatori (igroups). Dall'elenco, è possibile eseguire operazioni aggiuntive.

#### Fasi

1. In System Manager, fare clic su **Hosts > SAN Initiator Groups** (host > gruppi iniziatori SAN).

Nella pagina viene visualizzato un elenco di gruppi di iniziatori (igroups). Se l'elenco è grande, è possibile visualizzare altre pagine dell'elenco facendo clic sui numeri di pagina nell'angolo inferiore destro della pagina.


Le colonne visualizzano varie informazioni su igroups. A partire da 9.11.1, viene visualizzato anche lo stato

di connessione dell'igroup. Passare il mouse sugli avvisi di stato per visualizzare i dettagli.


2. (Facoltativo): È possibile eseguire le seguenti attività facendo clic sulle icone nell'angolo superiore destro dell'elenco:

- **Ricerca**
- **Scaricare** l'elenco.
- **Mostra o Nascondi** nell'elenco.
- **Filtra** i dati nell'elenco.

3. È possibile eseguire le operazioni dall'elenco:

- Fare clic su  **Add** per aggiungere un igroup.
- Fare clic sul nome dell'igroup per visualizzare la pagina **Overview** che mostra i dettagli relativi all'igroup.

Nella pagina **Panoramica**, è possibile visualizzare i LUN associati all'igroup ed eseguire le operazioni per creare LUN e mappare i LUN. Fare clic su **All SAN Initiator** (tutti gli iniziatori SAN) per tornare all'elenco principale.

- Passare il mouse sull'igroup, quindi fare clic su  accanto a un nome igroup per modificare o eliminare l'igroup.
- Passare il mouse sull'area a sinistra del nome dell'igroup, quindi selezionare la casella di controllo. Facendo clic su **+Aggiungi a gruppo iniziatore**, è possibile aggiungere tale igroup a un altro igroup.
- Nella colonna **Storage VM**, fare clic sul nome di una storage VM per visualizzarne i dettagli.

#### Visualizzare e gestire GLI iniziatori SAN

È possibile utilizzare System Manager per visualizzare un elenco di iniziatori. Dall'elenco, è possibile eseguire operazioni aggiuntive.

#### Fasi

1. In System Manager, fare clic su **Hosts > SAN Initiator Groups** (host > gruppi iniziatori SAN).

Nella pagina viene visualizzato un elenco di gruppi di iniziatori (igroups).

2. Per visualizzare gli iniziatori, attenersi alla seguente procedura:

- Fare clic sulla scheda **iniziatori FC** per visualizzare un elenco di iniziatori FC.
- Fare clic sulla scheda **iSCSI Initiators** per visualizzare un elenco di iniziatori iSCSI.

Le colonne visualizzano varie informazioni sugli iniziatori.

A partire da 9.11.1, viene visualizzato anche lo stato di connessione dell'iniziatore. Passare il mouse sugli avvisi di stato per visualizzare i dettagli.

3. (Facoltativo): È possibile eseguire le seguenti attività facendo clic sulle icone nell'angolo superiore destro dell'elenco:

- **Cerca** l'elenco di iniziatori specifici.
- **Scaricare** l'elenco.
- **Mostra o Nascondi** nell'elenco.



- **Filtra** i dati nell'elenco.

## Creare un igroup nidificato

A partire da ONTAP 9.9.1, è possibile creare un igroup composto da altri igroups esistenti.

1. In System Manager, fare clic su **host > SAN Initiator Groups**, quindi fare clic su **Add**.
2. Inserire i campi igroup **Name** (Nome) e **Description** (Descrizione).

La descrizione funge da alias igroup.

3. Selezionare **Storage VM** e **host Operating System**.



Il tipo di sistema operativo di un igroup nidificato non può essere modificato dopo la creazione dell'igroup.

4. In **Initiator Group Members** selezionare **Existing Initiator group**.

È possibile utilizzare **Search** per trovare e selezionare i gruppi iniziatori che si desidera aggiungere.

## Mappare igroups a più LUN

A partire da ONTAP 9.9.1, è possibile associare igroups a due o più LUN contemporaneamente.

1. In System Manager, fare clic su **Storage > LUN**.
2. Selezionare i LUN che si desidera mappare.
3. Fare clic su **More** (Altro), quindi su **Map to Initiator Groups** (Mappa ai gruppi di iniziatori)



Gli igroups selezionati vengono aggiunti ai LUN selezionati. Le mappature preesistenti non vengono sovrascritte.

## Creare un portset e associarlo a un igroup

Oltre all'utilizzo "**Mappa LUN selettiva (SLM)**", È possibile creare un portset e associare il portset a un igroup per limitare ulteriormente le LIF che possono essere utilizzate da un iniziatore per accedere a un LUN.

Se non si associa un portset a un igroup, tutti gli iniziatori nell'igroup possono accedere alle LUN mappate attraverso tutte le LIF sul nodo che possiede il LUN e il partner ha del nodo proprietario.

### Di cosa hai bisogno

Devi avere almeno un LIF e un igroup.

A meno che non si utilizzino gruppi di interfacce, si consigliano due LIF per la ridondanza sia per iSCSI che per FC. Per i gruppi di interfacce si consiglia un solo LIF.

### A proposito di questa attività

È vantaggioso utilizzare i portset con SLM quando si dispone di più di due LIF su un nodo e si desidera limitare

un determinato iniziatore a un sottoinsieme di LIF. Senza i portset, tutti gli iniziatori avranno accesso al LUN a tutte le destinazioni del nodo tramite il nodo proprietario del LUN e il partner ha del nodo proprietario.


Esempio 11. Fasi

System Manager

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per creare portset e associarli a igroups.

Se è necessario creare un portset e associarlo a un igroup in una release di ONTAP precedente alla 9.10.1, è necessario utilizzare la procedura CLI di ONTAP.

- 1. In System Manager, fare clic su **Network > Overview > Portsets**, quindi fare clic su **Add**.
- 2. Inserire le informazioni relative al nuovo portset e fare clic su **Add** (Aggiungi).
- 3. Fare clic su **host > SAN Initiator Groups** (gruppi iniziatori SAN)
- 4. Per associare il portset a un nuovo igroup, fare clic su **Add** (Aggiungi).

Per associare il portset a un igroup esistente, selezionare il igroup, quindi fare clic su , Quindi fare clic su **Edit Initiator Group** (Modifica gruppo iniziatore).

Informazioni correlate

["Visualizza e gestisci gli iniziatori e gli igroups"](#)

CLI

- 1. Creare un set di porte contenente le LIF appropriate:

```
portset create -vserver vs1 -portset portset_name -protocol
protocol -port-name port_name
```

Se si utilizza FC, specificare protocol parametro as fcp. Se si utilizza iSCSI, specificare protocol parametro as iscsi.

- 2. Collegare l'igroup al set di porte:

```
lun igroup bind -vserver vs1 -igroup igroup_name -portset
portset_name
```

- 3. Verificare che i set di porte e i LIF siano corretti:

```
portset show -vserver vs1
```

Vserver	Portset	Protocol	Port Names	Igroups
vs3	portset0	iscsi	lif0,lif1	igroup1


Gestire i portset

Oltre a ["Mappa LUN selettiva \(SLM\)"](#), È possibile utilizzare i portset per limitare


ulteriormente le LIF che possono essere utilizzate da un iniziatore per accedere a un LUN.

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per modificare le interfacce di rete associate ai portset ed eliminare i portset.

#### Modificare le interfacce di rete associate a un portset

1. In System Manager, selezionare **Network > Overview > Portsets**.
2. Selezionare il set di porte che si desidera modificare , Quindi selezionare **Edit Portset** (Modifica portset).

#### Eliminare un portset

1. In System Manager, fare clic su **Network > Overview > Portsets**.
2. Per eliminare un singolo set di porte, selezionarlo e scegliere  Quindi selezionare **Delete Portsets** (Elimina portset).

Per eliminare più portset, selezionare i portset e fare clic su **Delete** (Elimina).

#### Panoramica della mappa LUN selettiva

La mappa LUN selettiva (SLM) riduce il numero di percorsi dall'host al LUN. Con SLM, quando viene creata una nuova mappa LUN, la LUN è accessibile solo attraverso i percorsi sul nodo che possiede il LUN e il suo partner ha.

SLM consente la gestione di un singolo igroup per host e supporta anche operazioni di spostamento LUN senza interruzioni che non richiedono la manipolazione di portset o il remapping del LUN.

**"Portset"** Può essere utilizzato con SLM per limitare ulteriormente l'accesso di determinati target a determinati iniziatori. Quando si utilizza SLM con i portset, i LUN saranno accessibili sull'insieme di LIF nel portset sul nodo che possiede il LUN e sul partner ha di quel nodo.

SLM è attivato per impostazione predefinita su tutte le nuove mappe LUN.

#### Determinare se SLM è attivato su una mappa LUN

Se l'ambiente in uso dispone di una combinazione di LUN creati in una release di ONTAP 9 e di LUN trasferiti da versioni precedenti, potrebbe essere necessario determinare se la mappa LUN selettiva (SLM) è attivata su un LUN specifico.

È possibile utilizzare le informazioni visualizzate nell'output di `lun mapping show -fields reporting-nodes, node` Per determinare se SLM è attivato sulla mappa LUN. Se SLM non è abilitato, nelle celle sotto la colonna "reporting-nodes" dell'output del comando viene visualizzato "-". Se SLM è attivato, l'elenco dei nodi visualizzato nella colonna "Nodes" viene duplicato nella colonna "reporting-Nodes".

#### Modificare l'elenco dei nodi di reporting SLM

Se si sposta un LUN o un volume contenente LUN in un'altra coppia ad alta disponibilità (ha) all'interno dello stesso cluster, è necessario modificare l'elenco dei nodi di reporting della mappa LUN selettiva (SLM) prima di iniziare lo spostamento per garantire che vengano mantenuti i percorsi LUN attivi e ottimizzati.

#### Fasi

1. Aggiungere il nodo di destinazione e il relativo nodo partner all'elenco dei nodi di reporting dell'aggregato o del volume:

```
lun mapping add-reporting-nodes -vserver _vserver_name_ -path _lun_path_  
-igroup _igroup_name_ [-destination-aggregate _aggregate_name_|-  
destination-volume _volume_name_]
```

Se si dispone di una convenzione di denominazione coerente, è possibile modificare più mappature LUN contemporaneamente utilizzando *igroup\_prefix\** invece di *igroup\_name*.

2. Eseguire nuovamente la scansione dell'host per rilevare i percorsi aggiunti di recente.
3. Se il sistema operativo lo richiede, aggiungere i nuovi percorsi alla configurazione MPIO (Multipath Network i/o).
4. Eseguire il comando per l'operazione di spostamento desiderata e attendere il completamento dell'operazione.
5. Verificare che l'i/o venga gestito tramite il percorso Active/Optimized:

```
lun mapping show -fields reporting-nodes
```

6. Rimuovere il proprietario del LUN precedente e il relativo nodo partner dall'elenco dei nodi di reporting:

```
lun mapping remove-reporting-nodes -vserver _vserver_name_ -path  
_lun_path_ -igroup _igroup_name_ -remote-nodes
```

7. Verificare che il LUN sia stato rimosso dalla mappa LUN esistente:

```
lun mapping show -fields reporting-nodes
```

8. Rimuovere eventuali voci di dispositivi obsolete per il sistema operativo host.
9. Modificare eventuali file di configurazione multipathing, se necessario.
10. Eseguire nuovamente la scansione dell'host per verificare la rimozione dei vecchi percorsi. + consultare la documentazione dell'host per istruzioni specifiche su come eseguire nuovamente la scansione degli host.

## Gestire il protocollo iSCSI

### Configura la tua rete per ottenere le migliori performance

Le reti Ethernet variano notevolmente in termini di performance. È possibile massimizzare le prestazioni della rete utilizzata per iSCSI selezionando valori di configurazione specifici.

#### Fasi

1. Collegare le porte host e storage alla stessa rete.

Si consiglia di collegarsi agli stessi switch. Il routing non deve mai essere utilizzato.

2. Selezionare le porte più veloci disponibili e dedicarle a iSCSI.

Le porte da 10 GbE sono le migliori. Le porte 1 GbE sono il minimo.

3. Disattiva il controllo di flusso Ethernet per tutte le porte.

Dovrebbe essere visualizzato ["Gestione della rete"](#) Per utilizzare la CLI per configurare il controllo di flusso della porta Ethernet.

4. Abilitare i frame jumbo (in genere MTU di 9000).

Tutti i dispositivi nel percorso dati, inclusi iniziatori, destinazioni e switch, devono supportare i frame jumbo. In caso contrario, l'abilitazione dei frame jumbo riduce notevolmente le performance di rete.

### **Configurare una SVM per iSCSI**

Per configurare una macchina virtuale di storage (SVM) per iSCSI, è necessario creare LIF per SVM e assegnare il protocollo iSCSI a tali LIF.


#### **A proposito di questa attività**

È necessario un minimo di un LIF iSCSI per nodo per ogni SVM che fornisce dati con il protocollo iSCSI. Per la ridondanza, è necessario creare almeno due LIF per nodo.

Esempio 12. Fasi

System Manager

Configurazione di una VM di storage per iSCSI con Gestore di sistema di ONTAP (9.7 e versioni successive).

Per configurare iSCSI su una nuova VM di storage	Per configurare iSCSI su una VM di storage esistente
<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VMS</b>, quindi su <b>Add</b>.</li><li>2. Immettere un nome per la VM di storage.</li><li>3. Selezionare <b>iSCSI</b> per il protocollo di accesso*.</li><li>4. Fare clic su <b>Enable iSCSI</b> (attiva iSCSI) e inserire l'indirizzo IP e la subnet mask dell'interfaccia di rete. + ogni nodo deve avere almeno due interfacce di rete.</li><li>5. Fare clic su <b>Save</b> (Salva).</li></ol>	<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VM</b>.</li><li>2. Fare clic sulla VM di storage che si desidera configurare.</li><li>3. Fare clic sulla scheda <b>Impostazioni</b>, quindi su  Accanto al protocollo iSCSI.</li><li>4. Fare clic su <b>Enable iSCSI</b> (attiva iSCSI) e inserire l'indirizzo IP e la subnet mask dell'interfaccia di rete. + ogni nodo deve avere almeno due interfacce di rete.</li><li>5. Fare clic su <b>Save</b> (Salva).</li></ol>

CLI

Configurare una VM di storage per iSCSI con l'interfaccia CLI di ONTAP.

1. Abilitare le SVM per l'ascolto del traffico iSCSI:

```
vserver iscsi create -vserver vserver_name -target-alias vserver_name
```

2. Creare una LIF per le SVM su ciascun nodo da utilizzare per iSCSI:

- Per ONTAP 9.6 e versioni successive:

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol iscsi -service-policy default-data-iscsi -home-node node_name  
-home-port port_name -address ip_address -netmask netmask
```

- Per ONTAP 9.5 e versioni precedenti:

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol iscsi -home-node node_name -home-port port_name -address  
ip_address -netmask netmask
```

3. Verificare di aver configurato correttamente i file LIF:

```
network interface show -vserver vserver_name
```

4. Verificare che iSCSI sia attivo e in esecuzione e che l'IQN di destinazione per la SVM:

```
vserver iscsi show -vserver vserver_name
```

5. Dal tuo host, crea sessioni iSCSI sulle tue LIF.

## Informazioni correlate

["Report tecnico NetApp 4080: Best practice per le SAN moderne"](#)

## Definire un metodo di policy di sicurezza per un iniziatore

È possibile definire un elenco di iniziatori e i relativi metodi di autenticazione. È inoltre possibile modificare il metodo di autenticazione predefinito applicabile agli iniziatori che non dispongono di un metodo di autenticazione definito dall'utente.

### A proposito di questa attività

È possibile generare password univoche utilizzando gli algoritmi dei criteri di protezione del prodotto oppure specificare manualmente le password che si desidera utilizzare.



Non tutti gli iniziatori supportano password CHAP segrete esadecimali.

### Fasi

1. Utilizzare `vserver iscsi security create` per creare un metodo di policy di sicurezza per un iniziatore.

```
vserver iscsi security create -vserver vs2 -initiator iqn.1991-05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name bob2
```

2. Seguire i comandi sullo schermo per aggiungere le password.

Crea un metodo di policy di sicurezza per Initiator iqn.1991-05.com.microsoft:host1 con nomi utente e password CHAP in entrata e in uscita.

## Informazioni correlate

- [Come funziona l'autenticazione iSCSI](#)
- [Autenticazione CHAP](#)

## Eliminare un servizio iSCSI per una SVM

È possibile eliminare un servizio iSCSI per una macchina virtuale di storage (SVM) se non è più necessario.

### Di cosa hai bisogno

Lo stato di amministrazione del servizio iSCSI deve essere "proprio d'" prima di poter eliminare un servizio iSCSI. È possibile spostare lo stato di amministrazione in basso con il ``vserver iscsi modify` comando.

### Fasi

1. Utilizzare `vserver iscsi modify` Per arrestare l'i/o al LUN.

```
vserver iscsi modify -vserver vs1 -status-admin down
```

2. Utilizzare `vserver iscsi delete` Comando per rimuovere il servizio iscsi dalla SVM.

```
vserver iscsi delete -vserver vs_1
```

3. Utilizzare `vserver iscsi show` command Per verificare che il servizio iSCSI sia stato eliminato da SVM.

```
vserver iscsi show -vserver vs1
```

**Per ulteriori informazioni, consultare la sezione relativa ai ripristini degli errori della sessione iSCSI**

L'aumento del livello di ripristino degli errori di sessione iSCSI consente di ricevere informazioni più dettagliate sui ripristini degli errori iSCSI. L'utilizzo di un livello di ripristino degli errori superiore potrebbe causare una riduzione minore delle prestazioni della sessione iSCSI.

#### A proposito di questa attività

Per impostazione predefinita, ONTAP è configurato per utilizzare il livello di ripristino degli errori 0 per le sessioni iSCSI. Se si utilizza un iniziatore qualificato per il livello di ripristino degli errori 1 o 2, è possibile scegliere di aumentare il livello di ripristino degli errori. Il livello di ripristino degli errori di sessione modificato influisce solo sulle sessioni appena create e non sulle sessioni esistenti.

A partire da ONTAP 9.4, la `max-error-recovery-level` l'opzione non è supportata in `iscsi show` e `iscsi modify` comandi.

#### Fasi

1. Accedere alla modalità avanzata:

```
set -privilege advanced
```

2. Verificare l'impostazione corrente utilizzando `iscsi show` comando.

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
-----
vs3      0
```

3. Modificare il livello di ripristino degli errori utilizzando `iscsi modify` comando.

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

#### Registrare la SVM con un server iSNS

È possibile utilizzare `vserver iscsi isns` Comando per configurare la macchina virtuale di storage (SVM) per la registrazione con un server iSNS.

#### A proposito di questa attività

Il `vserver iscsi isns create` Il comando configura la SVM per la registrazione con il server iSNS. SVM non fornisce comandi che consentono di configurare o gestire il server iSNS. Per gestire il server iSNS, è possibile utilizzare gli strumenti di amministrazione del server o l'interfaccia fornita dal fornitore per il server iSNS.



## Fasi

1. Sul server iSNS, assicurarsi che il servizio iSNS sia attivo e disponibile per l'assistenza.
2. Creare la LIF di gestione SVM su una porta dati:

```
network interface create -vserver SVM_name -lif lif_name -role data -data  
-protocol none -home-node home_node_name -home-port home_port -address  
IP_address -netmask network_mask
```

3. Creare un servizio iSCSI sulla SVM se non ne esiste già uno:

```
vserver iscsi create -vserver SVM_name
```

4. Verificare che il servizio iSCSI sia stato creato correttamente:

```
iscsi show -vserver SVM_name
```

5. Verificare che esista un percorso predefinito per SVM:

```
network route show -vserver SVM_name
```

6. Se non esiste un percorso predefinito per SVM, creare un percorso predefinito:

```
network route create -vserver SVM_name -destination destination -gateway  
gateway
```

7. Configurare SVM per la registrazione con il servizio iSNS:

```
vserver iscsi isns create -vserver SVM_name -address IP_address
```

Sono supportate sia le famiglie di indirizzi IPv4 che IPv6. La famiglia di indirizzi del server iSNS deve essere uguale a quella della LIF di gestione SVM.

Ad esempio, non è possibile connettere un LIF di gestione SVM con un indirizzo IPv4 a un server iSNS con un indirizzo IPv6.

8. Verificare che il servizio iSNS sia in esecuzione:

```
vserver iscsi isns show -vserver SVM_name
```

9. Se il servizio iSNS non è in esecuzione, avviarlo:

```
vserver iscsi isns start -vserver SVM_name
```

## Risoluzione dei messaggi di errore iSCSI sul sistema di storage

Sono disponibili diversi messaggi di errore comuni relativi a iSCSI che è possibile visualizzare con `event log show` comando. Devi sapere cosa significano questi messaggi e cosa puoi fare per risolvere i problemi che identificano.

La seguente tabella contiene i messaggi di errore più comuni e le istruzioni per risolverli:

Messaggio	Spiegazione	Cosa fare
ISCSI: network interface identifier disabled for use; incoming connection discarded	Il servizio iSCSI non è abilitato sull'interfaccia.	È possibile utilizzare <code>iscsi interface enable</code> Per attivare il servizio iSCSI sull'interfaccia. Ad esempio:  <code>iscsi interface enable -vserver vs1 -lif lif1</code>
ISCSI: Authentication failed for initiator nodename	CHAP non è configurato correttamente per l'iniziatore specificato.	Controllare le impostazioni CHAP; non è possibile utilizzare lo stesso nome utente e password per le impostazioni in entrata e in uscita sul sistema di storage:  <ul style="list-style-type: none"> <li>• Le credenziali in entrata nel sistema di storage devono corrispondere alle credenziali in uscita sull'iniziatore.</li> <li>• Le credenziali in uscita sul sistema di storage devono corrispondere alle credenziali in entrata sull'iniziatore.</li> </ul>

### Attiva o disattiva il failover automatico della LIF iSCSI

Dopo l'upgrade a ONTAP 9.11.1 o versione successiva, dovresti attivare manualmente il failover LIF automatico su tutte le LIF iSCSI create in ONTAP 9.10.1 o versione precedente.

A partire da ONTAP 9.11.1, puoi abilitare il failover LIF automatico per LIF iSCSI su piattaforme di array SAN all-flash. In caso di failover dello storage, la LIF iSCSI viene automaticamente migrata dal nodo home o dalla porta al nodo partner di ha o alla porta, per poi tornare indietro una volta completato il failover. Oppure, se la porta per LIF iSCSI diventa guasta, la LIF viene migrata automaticamente a una porta funzionante nel suo nodo home corrente e quindi di nuovo alla porta originale una volta che la porta è nuovamente funzionante. Consente ai carichi di lavoro SAN in esecuzione su iSCSI di riprendere più rapidamente il servizio i/o dopo un failover.

In ONTAP 9.11.1 e versioni successive, per impostazione predefinita, le LIF iSCSI appena create vengono attivate per il failover automatico della LIF se si verifica una delle seguenti condizioni:

- Non ci sono LIF iSCSI nell'SVM
- Tutte le LIF iSCSI presenti nella SVM sono abilitate per il failover automatico della LIF

### Attiva il failover automatico della LIF iSCSI

Per impostazione predefinita, le LIF iSCSI create in ONTAP 9.10.1 e versioni precedenti non sono abilitate per il failover automatico della LIF. Se nell'SVM sono presenti LIF iSCSI non abilitate per il failover automatico della LIF, nemmeno le LIF create di recente saranno abilitate per il failover automatico della LIF. Se il failover automatico della LIF non è abilitato e in caso di failover, la LIF iSCSI non migrerà.

Scopri di più ["Failover e sconto della LIF"](#).

## Fase

1. Attivazione del failover automatico per una LIF iSCSI:

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-policy sfo-partner-only -auto-revert true
```

Per aggiornare tutte le LIF iSCSI nella SVM, utilizza `-lif*` invece di `lif`.

## Disattiva il failover automatico della LIF iSCSI

Se in precedenza hai abilitato il failover automatico di una LIF iSCSI creato in ONTAP 9.10.1 o versione precedente, puoi disabilitarlo.

## Fase

1. Disattivare il failover automatico per una LIF iSCSI:

```
network interface modify -vserver SVM_name -lif iscsi_lif -failover-policy disabled -auto-revert false
```

Per aggiornare tutte le LIF iSCSI nella SVM, utilizza `-lif*` invece di `lif`.

## Informazioni correlate

- ["Creare una LIF"](#)
- Manualmente ["Migrazione di una LIF"](#)
- Manualmente ["Ripristina una LIF nella porta home"](#)
- ["Configurare le impostazioni di failover su una LIF"](#)

## Gestire il protocollo FC

### Configurare una SVM per FC

Per configurare una SVM (Storage Virtual Machine) per FC, è necessario creare LIF per SVM e assegnare il protocollo FC a tali LIF.

#### Prima di iniziare

È necessario disporre di una licenza FC (["Incluso con ONTAP One"](#)) e deve essere attivato. Se la licenza FC non è abilitata, le LIF e le SVM sembrano essere in linea, ma lo stato operativo è `down`. Il servizio FC deve essere abilitato affinché i tuoi LIF e SVM siano operativi. Per ospitare gli iniziatori, è necessario utilizzare lo zoning initiator singolo per tutte le LIF FC nella SVM.


#### A proposito di questa attività

NetApp supporta almeno un LIF FC per nodo per ogni SVM che fornisce dati con il protocollo FC. È necessario utilizzare due LIF per nodo e due fabric, con un LIF per nodo collegato. Ciò garantisce la ridondanza a livello di nodo e fabric.

## Esempio 13. Fasi

### System Manager

Configurazione di una VM di storage per iSCSI con Gestore di sistema di ONTAP (9.7 e versioni successive).

Per configurare FC su una nuova VM di storage	Per configurare FC su una VM di storage esistente
<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VMS</b>, quindi su <b>Add</b>.</li><li>2. Immettere un nome per la VM di storage.</li><li>3. Selezionare <b>FC</b> per il protocollo di accesso*.</li><li>4. Fare clic su <b>Enable FC</b> (attiva FC). + le porte FC vengono assegnate automaticamente.</li><li>5. Fare clic su <b>Save</b> (Salva).</li></ol>	<ol style="list-style-type: none"><li>1. In System Manager, fare clic su <b>Storage &gt; Storage VM</b>.</li><li>2. Fare clic sulla VM di storage che si desidera configurare.</li><li>3. Fare clic sulla scheda <b>Impostazioni</b>, quindi su  Accanto al protocollo FC.</li><li>4. Fare clic su <b>Enable FC</b> (attiva FC) e inserire l'indirizzo IP e la subnet mask dell'interfaccia di rete. + le porte FC vengono assegnate automaticamente.</li><li>5. Fare clic su <b>Save</b> (Salva).</li></ol>

### CLI

1. Abilitare il servizio FC sulla SVM:

```
vserver fcp create -vserver vserver_name -status-admin up
```

2. Creare due LIF per le SVM su ciascun nodo che serve FC:

- Per ONTAP 9.6 e versioni successive:

```
network interface create -vserver vserver_name -lif lif_name -data  
-protocol fcp -service-policy default-data-fcp -home-node node_name  
-home-port port_name -address ip_address -netmask netmask -status-admin  
up
```

- Per ONTAP 9.5 e versioni precedenti:

```
network interface create -vserver vserver_name -lif lif_name -role data  
-data-protocol fcp -home-node node_name -home-port port
```

3. Verificare che i file LIF siano stati creati e che il loro stato operativo sia online:

```
network interface show -vserver vserver_name lif_name
```

### Informazioni correlate

["Supporto NetApp"](#)

["Tool di matrice di interoperabilità NetApp"](#)

[Considerazioni per le LIF negli ambienti SAN cluster](#)

## Eliminare un servizio FC per una SVM

È possibile eliminare un servizio FC per una macchina virtuale di storage (SVM) se non è più necessario.

### Di cosa hai bisogno

Lo stato di amministrazione deve essere “dOwn” (proprio) prima di poter eliminare un servizio FC per una SVM. È possibile impostare lo stato di amministrazione su inattivo con `vserver fcp modify` o il `vserver fcp stop` comando.

### Fasi

1. Utilizzare `vserver fcp stop` Per arrestare l'i/o al LUN.

```
vserver fcp stop -vserver vs_1
```

2. Utilizzare `vserver fcp delete` Comando per rimuovere il servizio dalla SVM.

```
vserver fcp delete -vserver vs_1
```

3. Utilizzare `vserver fcp show` Per verificare che il servizio FC sia stato eliminato dalla SVM:

```
vserver fcp show -vserver vs_1
```

## Configurazioni MTU consigliate per jumbo frame FCoE

Per Fibre Channel over Ethernet (FCoE), i frame jumbo per la parte dell'adattatore Ethernet del CNA devono essere configurati a 9000 MTU. I frame jumbo per la parte dell'adattatore FCoE del CNA devono essere configurati a un valore superiore a 1500 MTU. Configurare i frame jumbo solo se gli switch iniziatori, di destinazione e tutti gli switch interventori supportano e sono configurati per i frame jumbo.

## Gestire il protocollo NVMe

### Avviare il servizio NVMe per una SVM

Prima di poter utilizzare il protocollo NVMe sulla macchina virtuale di storage (SVM), è necessario avviare il servizio NVMe sulla SVM.

### Prima di iniziare

NVMe deve essere consentito come protocollo sul sistema.

Sono supportati i seguenti protocolli NVMe:

Protocollo	A partire da ...	Consentito da...
TCP	ONTAP 9.10.1	Predefinito
FCP	ONTAP 9.4	Predefinito

### Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Verificare che NVMe sia consentito come protocollo:

```
vserver nvme show
```

3. Creare il servizio del protocollo NVMe:

```
vserver nvme create
```

4. Avviare il servizio del protocollo NVMe su SVM:

```
vserver nvme modify -status -admin up
```

### **Eliminare il servizio NVMe da una SVM**

Se necessario, è possibile eliminare il servizio NVMe dalla macchina virtuale di storage (SVM).

#### **Fasi**

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Arrestare il servizio NVMe su SVM:

```
vserver nvme modify -status -admin down
```

3. Eliminare il servizio NVMe:


```
vserver nvme delete
```

### **Ridimensionare uno spazio dei nomi**

A partire da ONTAP 9.10.1, è possibile utilizzare l'interfaccia utente di ONTAP per aumentare o ridurre le dimensioni di uno spazio dei nomi NVMe. È possibile utilizzare System Manager per aumentare le dimensioni di uno spazio dei nomi NVMe.

#### **Aumentare le dimensioni di uno spazio dei nomi**

## System Manager

1. Fare clic su **Storage > NVMe Namespaces**.
2. Fai clic per passare il mouse sullo spazio dei nomi che desideri aumentare , Quindi fare clic su **Modifica**.
3. In **CAPACITY**, modificare le dimensioni dello spazio dei nomi.

## CLI

1. Immettere il seguente comando: `vserver nvme namespace modify -vserver SVM_name -path path -size new_size_of_namespace`

## Ridurre le dimensioni di uno spazio dei nomi

È necessario utilizzare l'interfaccia utente di ONTAP per ridurre le dimensioni di uno spazio dei nomi NVMe.

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Ridurre le dimensioni dello spazio dei nomi:

```
vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
```

## Convertire uno spazio dei nomi in un LUN

A partire da ONTAP 9.11.1, puoi utilizzare l'interfaccia a riga di comando di ONTAP per convertire in LUN un namespace NVMe esistente.

### Prima di iniziare

- Lo spazio dei nomi NVMe specificato non deve avere mappe esistenti su un sottosistema.
- Il namespace non deve far parte di una copia Snapshot o sul lato di destinazione della relazione di SnapMirror come namespace di sola lettura.
- Poiché gli spazi dei nomi NVMe sono supportati solo con specifiche piattaforme e schede di rete, questa funzione funziona solo con hardware specifico.

### Fasi

1. Inserisci il seguente comando per convertire un namespace NVMe in una LUN:

```
lun convert-from-namespace -vserver -namespace-path
```

## Configura l'autenticazione in-band su NVMe

A partire da ONTAP 9.12.1 è possibile utilizzare l'interfaccia a riga di comando (CLI) di ONTAP per configurare l'autenticazione in-band (sicura), bidirezionale e unidirezionale tra un host e un controller NVMe sui protocolli NVMe/TCP e NVMe/FC utilizzando l'autenticazione DH-HMAC-CHAP. A partire da ONTAP 9.14.1, l'autenticazione in banda

può essere configurata in Gestione sistema.

Per impostare l'autenticazione in banda, ogni host o controller deve essere associato a una chiave DH-HMAC-CHAP che è una combinazione del NQN dell'host o del controller NVMe e di una password di autenticazione configurata dall'amministratore. Perché un host o un controller NVMe possa autenticare il proprio peer, deve conoscere la chiave associata al peer.

Nell'autenticazione unidirezionale, viene configurata una chiave segreta per l'host, ma non per il controller. Nell'autenticazione bidirezionale, viene configurata una chiave segreta sia per l'host che per il controller.

SHA-256 è la funzione hash predefinita e 2048-bit è il gruppo DH predefinito.



## System Manager

A partire da ONTAP 9.14.1, puoi utilizzare System Manager per configurare l'autenticazione in-band creando o aggiornando un sottosistema NVMe, creando o clonando namespace NVMe o aggiungendo gruppi di coerenza con nuovi namespace NVMe.

### Fasi

1. In System Manager, fare clic su **host > sottosistema NVMe**, quindi su **Aggiungi**.
2. Aggiungere il nome del sottosistema NVMe e selezionare la VM di storage e il sistema operativo host.
3. Immettere l'NQN dell'host.
4. Selezionare **Usa autenticazione in banda** accanto a NQN host.
5. Fornire la password dell'host e la password del controller.

La chiave DH-HMAC-CHAP è una combinazione del NQN dell'host o del controller NVMe e di un segreto di autenticazione configurato dall'amministratore.

6. Selezionare la funzione hash preferita e il gruppo DH per ciascun host.

Se non si seleziona una funzione hash e un gruppo DH, SHA-256 viene assegnato come funzione hash predefinita e 2048 bit come gruppo DH predefinito.

7. In alternativa, fare clic su **Aggiungi** e ripetere la procedura come necessario per aggiungere altri host.
8. Fare clic su **Save** (Salva).
9. Per verificare che l'autenticazione in banda sia attivata, fare clic su **System Manager > Hosts > NVMe Subsystem > Grid > Peek view**.

L'icona di una chiave trasparente accanto al nome host indica che la modalità unidirezionale è attivata. Un tasto opaco accanto al nome host indica che la modalità bidirezionale è attivata.

## CLI

### Fasi

1. Aggiungere l'autenticazione DH-HMAC-CHAP al sottosistema NVMe:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn> -dhchap-host-secret  
<authentication_host_secret> -dhchap-controller-secret  
<authentication_controller_secret> -dhchap-hash-function <sha-  
256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-  
bit|8192-bit>
```

2. Verificare che il protocollo di autenticazione DH-HMAC CHAP sia stato aggiunto all'host:

```
vserver nvme subsystem host show
```

```

[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode

```

3. Verificare che l'autenticazione CHAP DH-HMAC sia stata eseguita durante la creazione del controller NVMe:

```
vserver nvme subsystem controller show
```

```

[ -dhchap-hash-function {sha-256|sha-512} ] Authentication Hash
Function
[ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
Diffie-Hellman
Group
[ -dhchap-mode {none|unidirectional|bidirectional} ]
Authentication Mode

```

## Disattiva l'autenticazione in banda su NVMe

Se è stata configurata l'autenticazione in banda su NVMe utilizzando DH-HMAC-CHAP, è possibile scegliere di disattivarla in qualsiasi momento.

Se si torna da ONTAP 9.12.1 o versione successiva a ONTAP 9.12.0 o versione precedente, è necessario disattivare l'autenticazione in banda prima di eseguire l'ripristino. Se l'autenticazione in banda mediante DH-HMAC-CHAP non è disattivata, l'operazione di revert avrà esito negativo.

### Fasi

1. Rimuovere l'host dal sottosistema per disattivare l'autenticazione DH-HMAC-CHAP:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Verificare che il protocollo di autenticazione DH-HMAC-CHAP sia stato rimosso dall'host:

```
vserver nvme subsystem host show
```

3. Aggiungere nuovamente l'host al sottosistema senza autenticazione:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

### Modifica della priorità dell'host NVMe

A partire da ONTAP 9.14.1, è possibile configurare il sottosistema NVMe per assegnare priorità all'allocazione delle risorse per host specifici. Per impostazione predefinita, quando un host viene aggiunto al sottosistema, viene assegnata una priorità regolare. Agli host assegnati una priorità alta viene assegnato un numero maggiore di code i/o e profondità di coda.

È possibile utilizzare l'interfaccia a riga di comando (CLI) di ONTAP per modificare manualmente la priorità predefinita da normale ad alta. Per modificare la priorità assegnata a un host, è necessario rimuovere l'host dal sottosistema e quindi aggiungerlo nuovamente.

#### Fasi

1. Verificare che la priorità dell'host sia impostata su regolare:

```
vserver nvme show-host-priority
```

2. Rimuovere l'host dal sottosistema:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem  
<subsystem> -host-nqn <host_nqn>
```

3. Verificare che l'host sia stato rimosso dal sottosistema:

```
vserver nvme subsystem host show
```

4. Aggiungere nuovamente l'host al sottosistema con priorità alta:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem  
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>  
-priority high
```

## Gestire il rilevamento automatico degli host dei controller NVMe/TCP

A partire da ONTAP 9.14.1, il rilevamento host dei controller che utilizzano il protocollo NVMe/TCP è automatizzato per impostazione predefinita nei fabric basati su IP.

### Rilevamento automatico dell'host dei controller NVMe/TCP

Se in precedenza è stato disattivato il rilevamento automatico dell'host, ma le esigenze sono state modificate, è possibile riattivarlo.

#### Fasi

1. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

2. Attivare il rilevamento automatico:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled true
```

3. Verificare che il rilevamento automatico dei controller NVMe/TCP sia attivato.

```
vserver nvme show
```

### Disattiva il rilevamento automatico degli host dei controller NVMe/TCP

Se non è necessario che l'host rilevi automaticamente i controller NVMe/TCP e rilevi traffico multicast indesiderato sulla rete, disattivare questa funzionalità.

#### Fasi

1. Accedere alla modalità avanzata dei privilegi:

```
set -privilege advanced
```

2. Disattiva rilevamento automatico:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery  
-enabled false
```

3. Verificare che il rilevamento automatico dei controller NVMe/TCP sia disattivato.

```
vserver nvme show
```

## Disattiva l'identificatore della macchina virtuale dell'host NVMe

A partire da ONTAP 9.14.1, per impostazione predefinita, ONTAP supporta la capacità degli host NVMe/FC di identificare le macchine virtuali mediante un identificatore univoco e per gli host NVMe/FC di monitorare l'utilizzo delle risorse della macchina virtuale. Questo migliora il reporting e il troubleshooting sul lato host.

È possibile utilizzare il bootarg per disattivare questa funzionalità.

### Fase

1. Disattivare l'identificatore della macchina virtuale:

```
bootargs set fct_sli_appid_off <port>, <port>
```

Nell'esempio seguente viene disattivato il VMID sulla porta 0g e sulla porta 0i.

```
bootargs set fct_sli_appid_off 0g,0i  
  
fct_sli_appid_off == 0g,0i
```

## Gestire i sistemi con adattatori FC

### Gestire i sistemi con adattatori FC

Sono disponibili comandi per gestire gli adattatori FC integrati e le schede adattatore FC. Questi comandi possono essere utilizzati per configurare la modalità dell'adattatore, visualizzare le informazioni sull'adattatore e modificare la velocità.

La maggior parte dei sistemi storage dispone di adattatori FC integrati che possono essere configurati come iniziatori o destinazioni. È inoltre possibile utilizzare schede adattatore FC configurate come iniziatori o destinazioni. Gli iniziatori si connettono agli shelf di dischi back-end e possibilmente a storage array esterni (FlexArray). Le destinazioni si connettono solo agli switch FC. Le porte HBA di destinazione FC e la velocità della porta dello switch devono essere impostate sullo stesso valore e non devono essere impostate su auto.

### Informazioni correlate

["Configurazione SAN"](#)

### Comandi per la gestione degli adattatori FC

È possibile utilizzare i comandi FC per gestire gli adattatori di destinazione FC, gli adattatori FC Initiator e gli adattatori FC integrati per lo storage controller. Gli stessi comandi vengono utilizzati per gestire gli adattatori FC per il protocollo FC e il protocollo FC-NVMe.

I comandi FC Initiator Adapter funzionano solo a livello di nodo. È necessario utilizzare `run -node node_name` Prima di poter utilizzare i comandi FC Initiator Adapter.

## Comandi per la gestione degli adattatori di destinazione FC

Se si desidera...	Utilizzare questo comando...
Visualizza le informazioni sulla scheda FC su un nodo	<code>network fcp adapter show</code>
Modificare i parametri dell'adattatore di destinazione FC	<code>network fcp adapter modify</code>
Visualizza le informazioni sul traffico del protocollo FC	<code>run -node <i>node_name</i> sysstat -f</code>
Visualizza per quanto tempo il protocollo FC è in esecuzione	<code>run -node <i>node_name</i> uptime</code>
Visualizzare la configurazione e lo stato dell'adattatore	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	<code>run -node <i>node_name</i> sysconfig -ac</code>
Visualizzare una pagina man per un comando	<code>man <i>command_name</i></code>

## Comandi per la gestione degli adattatori FC Initiator

Se si desidera...	Utilizzare questo comando...
Visualizza le informazioni per tutti gli iniziatori e i relativi adattatori in un nodo	<code>run -node <i>node_name</i> storage show adapter</code>
Visualizzare la configurazione e lo stato dell'adattatore	<code>run -node <i>node_name</i> sysconfig -v <i>adapter</i></code>
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	<code>run -node <i>node_name</i> sysconfig -ac</code>

## Comandi per la gestione degli adattatori FC integrati

Se si desidera...	Utilizzare questo comando...
Visualizza lo stato delle porte FC integrate	<code>run -node <i>node_name</i> system hardware unified-connect show</code>

## Configurare gli adattatori FC

Ogni porta FC integrata può essere configurata singolarmente come iniziatore o destinazione. Le porte di alcuni adattatori FC possono anche essere configurate singolarmente come una porta di destinazione o una porta initiator, proprio come le porte

FC integrate. In è disponibile un elenco di adattatori che è possibile configurare per la modalità di destinazione ["NetApp Hardware Universe"](#).

La modalità di destinazione viene utilizzata per collegare le porte agli iniziatori FC. La modalità Initiator viene utilizzata per collegare le porte a unità a nastro, librerie a nastro o storage di terze parti con la virtualizzazione FlexArray o l'importazione di LUN esterne (FLI).

La stessa procedura viene utilizzata per la configurazione degli adattatori FC per il protocollo FC e il protocollo FC-NVMe. Tuttavia, solo alcuni adattatori FC supportano FC-NVMe. Vedere ["NetApp Hardware Universe"](#) Per un elenco di adattatori che supportano il protocollo FC-NVMe.

### Configurare gli adattatori FC per la modalità di destinazione

#### Fasi

1. Portare l'adattatore offline:

```
node run -node node_name storage disable adapter adapter_name
```

Se l'adattatore non viene scollegato, è anche possibile rimuovere il cavo dalla porta dell'adattatore appropriata sul sistema.

2. Cambiare la scheda di rete da iniziatore a destinazione:

```
system hardware unified-connect modify -t target -node node_name adapter adapter_name
```

3. Riavviare il nodo che ospita l'adattatore modificato.
4. Verificare che la porta di destinazione abbia la configurazione corretta:

```
network fcp adapter show -node node_name
```

5. Porta online il tuo adattatore:

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

### Configurare gli adattatori FC per la modalità Initiator

#### Di cosa hai bisogno

- Le LIF della scheda di rete devono essere rimosse da tutti i set di porte di cui sono membri.
- Tutti i LIF di ogni macchina virtuale di storage (SVM) che utilizza la porta fisica da modificare devono essere migrati o distrutti prima di cambiare la personalità della porta fisica da destinazione a iniziatore.



NVMe/FC supporta la modalità Initiator.

#### Fasi

1. Rimuovere tutti i file LIF dalla scheda:

```
network interface delete -vserver SVM_name -lif LIF_name,LIF_name
```

2. Porta l'adattatore offline:

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin
```

down

Se l'adattatore non viene scollegato, è anche possibile rimuovere il cavo dalla porta dell'adattatore appropriata sul sistema.

3. Cambiare la scheda di rete da destinazione a iniziatore:

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Riavviare il nodo che ospita l'adattatore modificato.
5. Verificare che le porte FC siano configurate nello stato corretto per la configurazione:

```
system hardware unified-connect show
```

6. Riportare l'adattatore online:

```
node run -node node_name storage enable adapter adapter_port
```

## Visualizzare le impostazioni dell'adattatore

È possibile utilizzare comandi specifici per visualizzare informazioni sugli adattatori FC/UTA.

### Adattatore di destinazione FC

#### Fase

1. Utilizzare `network fcp adapter show` comando per visualizzare le informazioni sull'adattatore:  
`network fcp adapter show -instance -node node1 -adapter 0a`

L'output visualizza le informazioni di configurazione del sistema e le informazioni sull'adattatore per ogni slot utilizzato.

### Unified Target Adapter (UTA) X1143A-R6

#### Fasi

1. Avviare il controller senza i cavi collegati.
2. Eseguire `system hardware unified-connect show` per visualizzare la configurazione delle porte e i moduli.
3. Visualizzare le informazioni sulla porta prima di configurare il CNA e le porte.

### Modificare la porta UTA2 dalla modalità CNA alla modalità FC

Modificare la porta UTA2 dalla modalità Converged Network Adapter (CNA) alla modalità Fibre Channel (FC) per supportare la modalità FC Initiator e FC target. È necessario modificare la personalità dalla modalità CNA alla modalità FC quando si desidera modificare il supporto fisico che collega la porta alla rete.

#### Fasi

1. Portare l'adattatore offline:



```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
down
```

## 2. Modificare la modalità della porta:

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

## 3. Riavviare il nodo, quindi portare l'adattatore in linea:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
up
```

## 4. Avvisare l'amministratore o il gestore VIF di eliminare o rimuovere la porta, a seconda dei casi:

- Se la porta viene utilizzata come porta principale di una LIF, fa parte di un gruppo di interfacce (ifgrp) o ospita VLAN, un amministratore deve eseguire le seguenti operazioni:
  - i. Spostare le LIF, rimuovere la porta da ifgrp o eliminare le VLAN, rispettivamente.
  - ii. Eliminare manualmente la porta eseguendo `network port delete` comando.

Se il `network port delete` il comando non riesce, l'amministratore dovrebbe risolvere gli errori ed eseguire di nuovo il comando.

- Se la porta non viene utilizzata come porta home di un LIF, non è membro di un ifgrp e non ospita VLAN, il gestore VIF deve rimuovere la porta dai record al momento del riavvio.

Se il gestore VIF non rimuove la porta, l'amministratore deve rimuoverla manualmente dopo il riavvio utilizzando `network port delete` comando.

```
net-f8040-34::> network port show
```

Node: net-f8040-34-01

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps) Admin/Oper	Health Status
...						
e0i	Default	Default	down	1500	auto/10	-
e0f	Default	Default	down	1500	auto/10	-
...						

```
net-f8040-34::> ucadmin show
```

Admin	Current	Current	Pending	Pending
Node	Adapter	Mode	Type	Type
Status				
net-f8040-34-01	0e	cna	target	-
offline				-

```

net-f8040-34-01 0f cna target - -
offline
...

net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0

net-f8040-34::> network interface show -fields home-port, curr-port

vserver lif home-port curr-port
-----
Cluster net-f8040-34-01_clus1 e0a e0a
Cluster net-f8040-34-01_clus2 e0b e0b
Cluster net-f8040-34-01_clus3 e0c e0c
Cluster net-f8040-34-01_clus4 e0d e0d
net-f8040-34
cluster_mgmt e0M e0M
net-f8040-34
m e0e e0i
net-f8040-34
net-f8040-34-01_mgmt1 e0M e0M
7 entries were displayed.

net-f8040-34::> ucadmin modify local 0e fc

Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
Do you want to continue? {y|n}: y
Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

net-f8040-34::> reboot local
(system node reboot)

Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y

```

##### 5. Verificare di avere installato il modulo SFP+ corretto:

```
network fcp adapter show -instance -node -adapter
```

Per CNA, è necessario utilizzare un SFP Ethernet da 10 GB. Per FC, è necessario utilizzare un SFP da 8 GB o un SFP da 16 GB, prima di modificare la configurazione sul nodo.

## Sostituire i moduli ottici dell'adattatore target CNA/UTA2

È necessario modificare i moduli ottici sull'adattatore di destinazione unificato (CNA/UTA2) per supportare la modalità di personalità selezionata per l'adattatore.

### Fasi

1. Verificare l'SFP+ corrente utilizzato nella scheda. Quindi, sostituire il modulo SFP+ corrente con il modulo SFP+ appropriato per il linguaggio preferito (FC o CNA).
2. Rimuovere i moduli ottici correnti dall'adattatore X1143A-R6.
3. Inserire i moduli corretti per l'ottica della modalità Personality (FC o CNA) preferita.
4. Verificare di avere installato il modulo SFP+ corretto:

```
network fcp adapter show -instance -node -adapter
```

I moduli SFP+ supportati e i cavi in rame (Twinax) di marchio Cisco sono elencati nel *Hardware Universe*.

### Informazioni correlate

["NetApp Hardware Universe"](#)

## Configurazioni delle porte supportate per gli adattatori X1143A-R6

La modalità di destinazione FC è la configurazione predefinita per le porte dell'adattatore X1143A-R6. Tuttavia, le porte di questo adattatore possono essere configurate come porte Ethernet da 10 GB e FCoE o come porte FC da 16 GB.

Se configurati per Ethernet e FCoE, gli adattatori X1143A-R6 supportano il traffico di destinazione simultaneo di NIC e FCoE sulla stessa porta 10-GBE. Se configurata per FC, ciascuna coppia di due porte che condivide lo stesso ASIC può essere configurata singolarmente per la destinazione FC o la modalità iniziatore FC. Ciò significa che un singolo adattatore X1143A-R6 può supportare la modalità di destinazione FC su una coppia a due porte e la modalità iniziatore FC su un'altra coppia a due porte.

### Informazioni correlate

["NetApp Hardware Universe"](#)

["Configurazione SAN"](#)

## Configurare le porte

Per configurare l'adattatore di destinazione unificato (X1143A-R6), è necessario configurare le due porte adiacenti sullo stesso chip nella stessa modalità personality.

### Fasi

1. Configurare le porte in base alle necessità per Fibre Channel (FC) o Converged Network Adapter (CNA) utilizzando `system node hardware unified-connect modify` comando.
2. Collegare i cavi appropriati per FC o Ethernet da 10 GB.
3. Verificare di avere installato il modulo SFP+ corretto:

```
network fcp adapter show -instance -node -adapter
```

Per CNA, è necessario utilizzare un SFP Ethernet da 10 GB. Per FC, è necessario utilizzare un SFP da 8 GB o un SFP da 16 GB, in base al fabric FC a cui è collegato.

## **Evitare la perdita di connettività quando si utilizza l'adattatore X1133A-R6**

È possibile evitare la perdita di connettività durante un errore di porta configurando il sistema con percorsi ridondanti per separare gli HBA X1133A-R6.

X1133A-R6 HBA è un adattatore FC da 16 GB a 4 porte composto da due coppie di 2 porte. L'adattatore X1133A-R6 può essere configurato come modalità di destinazione o Initiator. Ogni coppia di 2 porte è supportata da un singolo ASIC (ad esempio, porta 1 e porta 2 su ASIC 1 e porta 3 e porta 4 su ASIC 2). Entrambe le porte di un singolo ASIC devono essere configurate per funzionare nella stessa modalità, sia in modalità di destinazione che in modalità iniziatore. Se si verifica un errore con ASIC che supporta una coppia, entrambe le porte della coppia passano offline.

Per evitare questa perdita di connettività, configurare il sistema con percorsi ridondanti per separare gli HBA X1133A-R6 o con percorsi ridondanti alle porte supportate da diversi ASIC sull'HBA.

## **Gestire le LIF per tutti i protocolli SAN**

### **Gestire le LIF per tutti i protocolli SAN**

Gli initiator devono utilizzare multipath i/o (MPIO) e Asymmetric Logical Unit Access (ALUA) per la funzionalità di failover dei cluster in un ambiente SAN. In caso di guasto di un nodo, i file LIF non migrano né assumono gli indirizzi IP del nodo partner guasto. Il software MPIO, che utilizza ALUA sull'host, è invece responsabile della selezione dei percorsi appropriati per l'accesso LUN tramite LIF.

È necessario creare uno o più percorsi iSCSI da ciascun nodo di una coppia ha, utilizzando le interfacce logiche (LIF) per consentire l'accesso alle LUN servite dalla coppia ha. È necessario configurare una LIF di gestione per ogni macchina virtuale di storage (SVM) che supporti LA SAN.

La connessione diretta o l'utilizzo di switch Ethernet sono supportati per la connettività. Devi creare LIF per entrambi i tipi di connettività.

- È necessario configurare una LIF di gestione per ogni macchina virtuale di storage (SVM) che supporti LA SAN.  
È possibile configurare due LIF per nodo, uno per ciascun fabric utilizzato con FC e per separare le reti Ethernet per iSCSI.

Una volta create, le LIF possono essere rimosse dai set di porte, spostate in nodi diversi di una Storage Virtual Machine (SVM) ed eliminate.

### **Informazioni correlate**

- ["Configurare LIF overveiw"](#)
- ["Creare una LIF"](#)

## **Configurare una LIF NVMe**

Quando si configurano le LIF NVMe, è necessario soddisfare alcuni requisiti.

### **Prima di iniziare**

NVMe deve essere supportato dall'adattatore FC su cui si crea la LIF. Gli adattatori supportati sono elencati nella ["Hardware Universe"](#).

### A proposito di questa attività

A partire da ONTAP 9.12.1 e versioni successive, puoi configurare due LIF NVMe per nodo con un massimo di 12 nodi. In ONTAP 9.11.1 e versioni precedenti, è possibile configurare due LIF NVMe per nodo su un massimo di due nodi.

Quando si crea una LIF NVMe si applicano le seguenti regole:

- NVMe può essere l'unico protocollo dati sulle LIF dei dati.
- È necessario configurare una LIF di gestione per ogni SVM che supporta LA SAN.
- Per ONTAP 9,5 e versioni successive, devi configurare una LIF NVMe sul nodo che contiene il namespace e sul partner ha del nodo.
- Solo per ONTAP 9.4:
  - Le LIF e gli spazi dei nomi NVMe devono essere ospitati sullo stesso nodo.
  - È possibile configurare un solo LIF dati NVMe per SVM.

### Fasi

#### 1. Crea la LIF:

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role  
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>  
-home-port <home_port>
```



NVME/TCP è disponibile a partire da ONTAP 9.10.1 e versioni successive.

#### 2. Verificare che la LIF sia stata creata:

```
network interface show -vserver <SVM_name>
```

Dopo la creazione, le LIF NVMe/TCP sono in attesa del rilevamento sulla porta 8009.

### Cosa fare prima di spostare UNA SAN LIF

È necessario eseguire uno spostamento LIF solo se si modifica il contenuto del cluster, ad esempio aggiungendo nodi al cluster o eliminando nodi dal cluster. Se si esegue un movimento LIF, non è necessario ridefinire la zona del fabric FC o creare nuove sessioni iSCSI tra gli host collegati del cluster e la nuova interfaccia di destinazione.

Non è possibile spostare UN LIF SAN utilizzando `network interface move` comando. Lo spostamento DELLA SAN LIF deve essere eseguito portando la LIF offline, spostando la LIF su un nodo o una porta home differente e quindi riportandola online nella nuova posizione. ALUA (Asymmetric Logical Unit Access) offre percorsi ridondanti e selezione automatica del percorso come parte di qualsiasi soluzione SAN ONTAP. Pertanto, non si verifica alcuna interruzione i/o quando la LIF viene portata offline per il movimento. L'host semplicemente riprova e sposta i/o in un altro LIF.

Grazie al movimento LIF, puoi effettuare le seguenti operazioni senza interruzioni:

- Sostituire una coppia ha di un cluster con una coppia ha aggiornata in modo trasparente per gli host che accedono ai dati LUN
- Aggiornare una scheda di interfaccia di destinazione
- Spostare le risorse di una macchina virtuale di storage (SVM) da un set di nodi in un cluster a un altro set di nodi nel cluster

### **Rimuovere una LIF SAN da un set di porte**

Se la LIF che si desidera eliminare o spostare si trova in un set di porte, è necessario rimuovere la LIF dal set di porte prima di poter eliminare o spostare la LIF.

#### **A proposito di questa attività**

È necessario eseguire il passaggio 1 della procedura seguente solo se una porta LIF è impostata. Non è possibile rimuovere l'ultimo LIF in un set di porte se il set di porte è associato a un gruppo di iniziatori. In caso contrario, è possibile iniziare con la fase 2 se sono presenti più LIF nella porta impostata.

#### **Fasi**

1. Se nella porta impostata è presente un solo LIF, utilizzare `lun igroup unbind` comando per disassociare il set di porte dal gruppo di iniziatori.



Quando si dislega un gruppo di iniziatori da un set di porte, tutti gli iniziatori del gruppo di iniziatori hanno accesso a tutte le LUN di destinazione mappate al gruppo di iniziatori su tutte le interfacce di rete.

```
cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
```

2. Utilizzare `lun portset remove` Comando per rimuovere LIF dal set di porte.

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

### **Spostare UNA LIF SAN**

Se un nodo deve essere portato offline, è possibile spostare un LIF SAN per conservare le informazioni di configurazione, ad esempio WWPN, ed evitare di eseguire il zoning dello switch fabric. Poiché un LIF SAN deve essere portato offline prima di essere spostato, il traffico host deve fare affidamento sul software di multipathing host per fornire un accesso senza interruzioni al LUN. È possibile spostare LE LIF SAN in qualsiasi nodo di un cluster, ma non è possibile spostare LE LIF SAN tra le macchine virtuali di storage (SVM).

#### **Di cosa hai bisogno**

Se la LIF è membro di un set di porte, la LIF deve essere stata rimossa dalla porta impostata prima di poter spostare la LIF in un nodo diverso.

#### **A proposito di questa attività**

Il nodo di destinazione e la porta fisica di un LIF che si desidera spostare devono trovarsi sullo stesso fabric FC o sulla stessa rete Ethernet. Se si sposta un LIF in un fabric diverso che non è stato correttamente zonato

o si sposta un LIF in una rete Ethernet che non dispone di connettività tra iSCSI Initiator e destinazione, il LUN non sarà accessibile quando viene riportato online.

## Fasi

1. Visualizzare lo stato amministrativo e operativo della LIF:

```
network interface show -vserver vserver_name
```

2. Modificare lo stato del LIF in down (offline):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin  
down
```

3. Assegnare alla LIF un nuovo nodo e una nuova porta:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node  
node_name -home-port port_name
```

4. Modificare lo stato del LIF in up (online):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

5. Verificare le modifiche:

```
network interface show -vserver vserver_name
```

## Eliminare una LIF in un ambiente SAN

Prima di eliminare una LIF, assicurarsi che l'host connesso alla LIF possa accedere alle LUN attraverso un altro percorso.


### Di cosa hai bisogno

Se il LIF che si desidera eliminare è membro di un set di porte, è necessario prima rimuovere il LIF dal set di porte prima di poter eliminare il LIF.

## System Manager

Eliminazione di una LIF con Gestione di sistema di ONTAP (9.7 e versioni successive).

### Fasi

1. In System Manager, fare clic su **rete > Panoramica**, quindi selezionare **interfacce di rete**.
2. Selezionare la VM di storage da cui si desidera eliminare la LIF.
3. Fare clic su  E selezionare **Delete** (Elimina).

### CLI

Eliminare un LIF con l'interfaccia utente di ONTAP.

### Fasi

1. Verificare il nome della LIF e la porta corrente da eliminare:

```
network interface show -vserver vs1
```

2. Eliminare la LIF:

```
network interface delete
```

```
network interface delete -vserver vs1 -lif lif1
```

3. Verificare di aver eliminato la LIF:

```
network interface show
```

```
network interface show -vserver vs1
```

Logical Status	Network	Current	Current Is
Vserver Interface	Admin/Oper	Address/Mask	Node Port
Home			
-----	-----	-----	-----
vs1			
lif2	up/up	192.168.2.72/24	node-01 e0b
true			
lif3	up/up	192.168.2.73/24	node-01 e0b
true			

## Requisiti LIF SAN per l'aggiunta di nodi a un cluster

Quando si aggiungono nodi a un cluster, è necessario tenere presente alcune considerazioni.

- Prima di creare LUN sui nuovi nodi, è necessario creare i file LIF appropriati.



- È necessario rilevare tali LIF dagli host in base alle specifiche dello stack host e del protocollo.
- È necessario creare LIF sui nuovi nodi in modo che i movimenti di LUN e volume siano possibili senza utilizzare la rete di interconnessione del cluster.

### Configurare le LIF iSCSI in modo che restituisca FQDN per ospitare l'operazione di rilevamento di iSCSI SendTargets

A partire da ONTAP 9, è possibile configurare le LIF iSCSI in modo che restituisca un nome di dominio completo (FQDN) quando un sistema operativo host invia un'operazione di rilevamento di iSCSI SendTargets. La restituzione di un FQDN è utile quando è presente un dispositivo NAT (Network Address Translation) tra il sistema operativo host e il servizio di storage.

#### A proposito di questa attività

Gli indirizzi IP su un lato del dispositivo NAT non hanno alcun significato dall'altro lato, ma gli FQDN possono avere un significato su entrambi i lati.



Il limite di interoperabilità del valore FQDN è di 128 caratteri su tutti i sistemi operativi host.

#### Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Configurare le LIF iSCSI per restituire FQDN:

```
vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name  
-sendtargets_fqdn FQDN
```

Nell'esempio seguente, le LIF iSCSI sono configurate per restituire storagehost-005.example.com come FQDN.

```
vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn  
storagehost-005.example.com
```

3. Verificare che sendtargets sia l'FQDN:

```
vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
```

In questo esempio, storagehost-005.example.com viene visualizzato nel campo di output sendtargets-fqdn.

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields  
sendtargets-fqdn  
vserver lif          sendtargets-fqdn  
-----  
vs1      vs1_iscsi1  storagehost-005.example.com  
vs1      vs1_iscsi2  storagehost-006.example.com
```

#### Informazioni correlate

## Combinazioni di configurazione di volume e file o LUN consigliate

### Panoramica delle combinazioni di configurazione di volume e file o LUN consigliate

Esistono combinazioni specifiche di configurazioni di volume e file o LUN FlexVol che è possibile utilizzare, a seconda dei requisiti di amministrazione e dell'applicazione. La comprensione dei vantaggi e dei costi di queste combinazioni può aiutarti a determinare la combinazione di configurazione del volume e del LUN più adatta al tuo ambiente.

Si consiglia di utilizzare le seguenti combinazioni di configurazione del volume e del LUN:

- File o LUN con spazio riservato con provisioning di volumi thick
- File o LUN non riservati in termini di spazio con provisioning di volumi thin
- File o LUN con spazio riservato con provisioning di volumi semi-spessi

È possibile utilizzare il thin provisioning SCSI sui LUN in combinazione con una qualsiasi di queste combinazioni di configurazione.

#### File o LUN con spazio riservato con provisioning di volumi thick

##### Benefici:

- Tutte le operazioni di scrittura all'interno dei file con spazio riservato sono garantite; non si verificheranno errori a causa dello spazio insufficiente.
- Non esistono limitazioni all'efficienza dello storage e alle tecnologie di protezione dei dati sul volume.

##### Costi e limitazioni:

- È necessario disporre di spazio sufficiente per l'aggregato in primo piano per supportare il volume con provisioning spesso.
- Lo spazio pari al doppio delle dimensioni del LUN viene allocato dal volume al momento della creazione del LUN.

#### File o LUN non riservati in termini di spazio con provisioning di volumi thin

##### Benefici:

- Non esistono limitazioni all'efficienza dello storage e alle tecnologie di protezione dei dati sul volume.
- Lo spazio viene allocato solo quando viene utilizzato.

##### Costi e restrizioni:

- Le operazioni di scrittura non sono garantite; possono fallire se il volume esaurisce lo spazio libero.
- È necessario gestire lo spazio libero nell'aggregato in modo efficace per evitare che l'aggregato esaurisca lo spazio libero.

#### File o LUN con spazio riservato con provisioning di volumi semi-spessi

##### Benefici:

Meno spazio viene riservato in anticipo rispetto al provisioning di volumi spessi e viene comunque fornita una garanzia di scrittura con il massimo sforzo.

#### **Costi e restrizioni:**

- Con questa opzione, le operazioni di scrittura possono non riuscire.

È possibile ridurre questo rischio bilanciando correttamente lo spazio libero nel volume rispetto alla volatilità dei dati.

- Non è possibile fare affidamento sulla conservazione di oggetti di protezione dei dati come copie Snapshot e file FlexClone e LUN.
- Non è possibile utilizzare le funzionalità di efficienza dello storage per la condivisione di blocchi di ONTAP che non possono essere eliminate automaticamente, tra cui deduplica, compressione e offload ODX/copia.

#### **Determinare la combinazione di configurazione del volume e del LUN corretta per l'ambiente in uso**

Rispondendo ad alcune domande di base sull'ambiente in uso, è possibile determinare la migliore configurazione del volume FlexVol e del LUN per l'ambiente in uso.

#### **A proposito di questa attività**

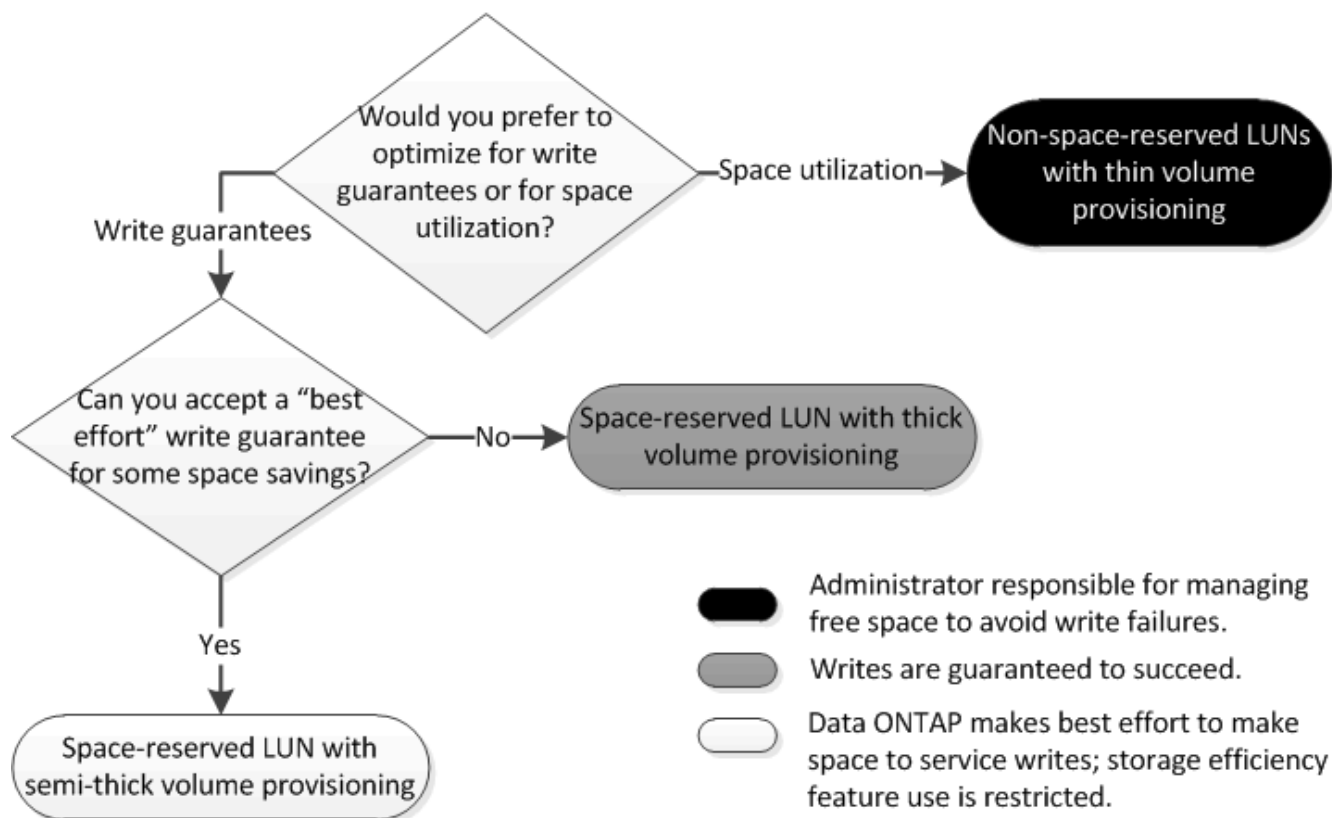
È possibile ottimizzare le configurazioni di LUN e volumi per il massimo utilizzo dello storage o per la sicurezza delle garanzie di scrittura. In base ai requisiti di utilizzo dello storage e alla capacità di monitorare e riempire rapidamente lo spazio libero, è necessario determinare il volume FlexVol e i volumi LUN appropriati per l'installazione.



Non è necessario un volume separato per ogni LUN.

#### **Fase**

1. Utilizzare la seguente struttura decisionale per determinare la combinazione di configurazione del volume e del LUN migliore per l'ambiente in uso:



### Calcola il tasso di crescita dei dati per le LUN

È necessario conoscere il tasso di crescita dei dati LUN nel tempo per determinare se è necessario utilizzare LUN con spazio riservato o LUN senza spazio riservato.

#### A proposito di questa attività

Se hai un tasso di crescita dei dati costantemente elevato, le LUN riservate allo spazio potrebbero essere un'opzione migliore per te. Se si ha un basso tasso di crescita dei dati, è necessario prendere in considerazione LUN non riservate allo spazio.

Puoi utilizzare strumenti come OnCommand Insight per calcolare il tasso di crescita dei dati oppure puoi calcolarlo manualmente. I seguenti passaggi sono per il calcolo manuale.

#### Fasi

1. Impostare un LUN con spazio riservato.
2. Monitorare i dati sul LUN per un determinato periodo di tempo, ad esempio una settimana.

Assicurarsi che il periodo di monitoraggio sia sufficientemente lungo da formare un campione rappresentativo degli aumenti della crescita dei dati che si verificano regolarmente. Ad esempio, alla fine di ogni mese si potrebbe avere una notevole crescita dei dati.

3. Ogni giorno, registra in GB la crescita dei tuoi dati.
4. Al termine del periodo di monitoraggio, sommare i totali di ogni giorno, quindi dividere per il numero di giorni del periodo di monitoraggio.

Questo calcolo consente di ottenere il tasso medio di crescita.

## Esempio

In questo esempio, è necessario un LUN da 200 GB. Si decide di monitorare il LUN per una settimana e di registrare le seguenti modifiche giornaliere dei dati:

- Domenica: 20 GB
- Lunedì: 18 GB
- Martedì: 17 GB
- Mercoledì: 20 GB
- Giovedì: 20 GB
- Venerdì: 23 GB
- Sabato: 22 GB

In questo esempio, il tasso di crescita è  $(20+18+17+20+20+23+22) / 7 = 20$  GB al giorno.

## Impostazioni di configurazione per file o LUN con spazio riservato con volumi con thick provisioning

Questa combinazione di configurazione di file e volumi FlexVol o LUN offre la possibilità di utilizzare le tecnologie di efficienza dello storage e non richiede il monitoraggio attivo dello spazio libero, in quanto viene allocato spazio sufficiente in anticipo.

Le seguenti impostazioni sono necessarie per configurare un file o LUN con spazio riservato in un volume utilizzando il thick provisioning:

Impostazione del volume	Valore
Garanzia	Volume
Riserva frazionaria	100
Riserva di Snapshot	Qualsiasi
Eliminazione automatica di Snapshot	Opzionale
Crescita automatica	Facoltativo; se attivato, lo spazio libero aggregato deve essere monitorato attivamente.

Impostazione del file o del LUN	Valore
Prenotazione di spazio	Attivato

## Impostazioni di configurazione per file non riservati allo spazio o LUN con volumi con thin provisioning

Questa combinazione di configurazione di file e volumi FlexVol o LUN richiede la minima quantità di storage da allocare in anticipo, ma richiede la gestione dello spazio libero attivo per evitare errori dovuti alla mancanza di spazio.

Le seguenti impostazioni sono necessarie per configurare un LUN o file non riservati allo spazio in un volume

con thin provisioning:

Impostazione del volume	Valore
Garanzia	Nessuno
Riserva frazionaria	0
Riserva di Snapshot	Qualsiasi
Eliminazione automatica di Snapshot	Opzionale
Crescita automatica	Opzionale

Impostazione del file o del LUN	Valore
Prenotazione di spazio	Disattivato

#### Considerazioni aggiuntive

Quando il volume o l'aggregato esaurisce lo spazio, le operazioni di scrittura sul file o sul LUN possono avere esito negativo.

Se non si desidera monitorare attivamente lo spazio libero per il volume e l'aggregato, attivare la crescita automatica per il volume e impostare la dimensione massima del volume in base alle dimensioni dell'aggregato. In questa configurazione, è necessario monitorare attivamente lo spazio libero aggregato, ma non è necessario monitorare lo spazio libero nel volume.

#### Impostazioni di configurazione per file o LUN con spazio riservato con provisioning di volumi semi-spessi

Questa combinazione di configurazione di file e volumi FlexVol o LUN richiede una quantità inferiore di storage da allocare in anticipo rispetto alla combinazione con provisioning completo, ma pone restrizioni sulle tecnologie di efficienza che è possibile utilizzare per il volume. Le sovrascritture vengono eseguite con il massimo sforzo per questa combinazione di configurazione.

Le seguenti impostazioni sono necessarie per configurare un LUN con spazio riservato in un volume utilizzando il provisioning semi-spessi:

Impostazione del volume	Valore
Garanzia	Volume
Riserva frazionaria	0
Riserva di Snapshot	0

Impostazione del volume	Valore
Eliminazione automatica di Snapshot	On, con un livello di impegno di Destroy, un elenco Destroy che include tutti gli oggetti, il trigger impostato sul volume e tutti i LUN FlexClone e i file FlexClone abilitati per l'eliminazione automatica.
Crescita automatica	Facoltativo; se attivato, lo spazio libero aggregato deve essere monitorato attivamente.

Impostazione del file o del LUN	Valore
Prenotazione di spazio	Attivato

### Restrizioni tecnologiche

Non è possibile utilizzare le seguenti tecnologie per l'efficienza dello storage dei volumi per questa combinazione di configurazione:

- Compressione
- Deduplica
- Offload delle copie di ODX e FlexClone
- LUN FlexClone e file FlexClone non contrassegnati per l'eliminazione automatica (cloni attivi)
- File secondari FlexClone
- Offload ODX/copia

### Considerazioni aggiuntive

Quando si utilizza questa combinazione di configurazione, è necessario considerare i seguenti fatti:

- Quando il volume che supporta tale LUN occupa poco spazio, i dati di protezione (LUN e file FlexClone, copie Snapshot) vengono distrutti.
- Le operazioni di scrittura possono scadere e fallire quando il volume esaurisce lo spazio libero.

La compressione è attivata per impostazione predefinita per le piattaforme AFF. È necessario disattivare esplicitamente la compressione per qualsiasi volume per il quale si desidera utilizzare il provisioning semi-thick su una piattaforma AFF.

## Protezione dei dati SAN

### Panoramica dei metodi di protezione dei dati negli ambienti SAN

È possibile proteggere i dati creando copie di questi in modo che siano disponibili per il ripristino in caso di eliminazione accidentale, crash delle applicazioni, danneggiamento dei dati o disastro. A seconda delle esigenze di backup e protezione dei dati, ONTAP offre una vasta gamma di metodi che consentono di proteggere i dati.

## **Continuità aziendale SnapMirror (SM-BC)**

A partire dalla disponibilità generale in ONTAP 9.9.1, fornisce l'obiettivo di tempo di ripristino zero (RTO zero) o il failover trasparente delle applicazioni (TAF) per consentire il failover automatico delle applicazioni business-critical negli ambienti SAN. SM-BC richiede l'installazione di ONTAP Mediator 1,2 in una configurazione con due cluster AFF o due cluster ASA (All-Flash SAN Array).

["Documentazione NetApp: SnapMirror Business Continuity"](#)

## **Copia Snapshot**

Consente di creare, pianificare e gestire manualmente o automaticamente più backup delle LUN. Le copie Snapshot utilizzano solo una quantità minima di spazio aggiuntivo sul volume e non hanno un costo di performance. Se i dati LUN vengono modificati o cancellati accidentalmente, è possibile ripristinarli facilmente e rapidamente da una delle copie Snapshot più recenti.

## **LUN FlexClone (richiesta licenza FlexClone)**

Fornisce copie point-in-time e scrivibili di un altro LUN in un volume attivo o in una copia Snapshot. Un clone e il suo padre possono essere modificati indipendentemente senza influire l'uno sull'altro.

## **SnapRestore (licenza richiesta)**

Consente di eseguire un ripristino dei dati rapido, efficiente in termini di spazio e on-request da copie Snapshot su un intero volume. È possibile utilizzare SnapRestore per ripristinare un LUN a uno stato precedentemente conservato senza riavviare il sistema di storage.

## **Copie mirrorate per la protezione dei dati (licenza SnapMirror richiesta)**

Fornisce il disaster recovery asincrono, consentendo di creare periodicamente copie Snapshot dei dati sul volume, copiare tali copie Snapshot su una rete locale o wide-area su un volume partner, di solito su un altro cluster, e conservare tali copie Snapshot. La copia mirror sul volume partner fornisce una rapida disponibilità e ripristino dei dati a partire dall'ultima copia Snapshot, se i dati sul volume di origine sono danneggiati o persi.

## **Backup SnapVault (licenza SnapMirror richiesta)**

Offre storage efficiente e conservazione a lungo termine dei backup. Le relazioni SnapVault consentono di eseguire il backup di copie Snapshot selezionate dei volumi in un volume di destinazione e di conservare i backup.

Se si eseguono backup su nastro e operazioni di archiviazione, è possibile eseguirli sui dati di cui è già stato eseguito il backup sul volume secondario SnapVault.

## **SnapDrive per Windows o UNIX (licenza SnapDrive richiesta)**

Configura l'accesso alle LUN, gestisce le LUN e gestisce le copie Snapshot del sistema di storage direttamente da host Windows o UNIX.

## **Backup e ripristino su nastro nativo**

Il supporto per la maggior parte delle unità a nastro esistenti è incluso in ONTAP, oltre a un metodo per i vendor di nastri per aggiungere dinamicamente il supporto per i nuovi dispositivi. ONTAP supporta anche il protocollo RMT (Remote Magnetic Tape), che consente il backup e il ripristino su qualsiasi sistema compatibile.



## Informazioni correlate

["Documentazione NetApp: SnapDrive per UNIX"](#)

["Documentazione NetApp: SnapDrive per Windows \(release correnti\)"](#)

["Protezione dei dati mediante backup su nastro"](#)

## Effetto dello spostamento o della copia di un LUN sulle copie Snapshot

### Effetto dello spostamento o della copia di un LUN sulle copie Snapshot

Le copie Snapshot vengono create a livello di volume. Se si copia o si sposta un LUN in un volume diverso, il criterio di copia Snapshot del volume di destinazione viene applicato al volume copiato o spostato. Se le copie Snapshot non sono stabilite per il volume di destinazione, le copie Snapshot non verranno create per il LUN spostato o copiato.

### Ripristinare una singola LUN da una copia Snapshot

È possibile ripristinare una singola LUN da una copia Snapshot senza ripristinare l'intero volume che contiene la singola LUN. È possibile ripristinare il LUN in posizione o in un nuovo percorso nel volume. L'operazione ripristina solo la singola LUN senza influire su altri file o LUN nel volume. È anche possibile ripristinare i file con i flussi.

### Di cosa hai bisogno

- È necessario disporre di spazio sufficiente sul volume per completare l'operazione di ripristino:
  - Se si sta ripristinando una LUN riservata allo spazio in cui la riserva frazionaria è pari a 0%, è necessario avere una dimensione pari a una volta quella della LUN ripristinata.
  - Se si sta ripristinando una LUN riservata allo spazio in cui la riserva frazionaria è del 100%, sono necessarie due volte le dimensioni della LUN ripristinata.
  - Se si sta ripristinando una LUN non riservata allo spazio, è necessario solo lo spazio effettivo utilizzato per la LUN ripristinata.
- È necessario creare una copia Snapshot del LUN di destinazione.

Se l'operazione di ripristino non riesce, il LUN di destinazione potrebbe essere troncato. In questi casi, è possibile utilizzare la copia Snapshot per evitare la perdita di dati.

- È necessario creare una copia Snapshot del LUN di origine.

In rari casi, il ripristino del LUN potrebbe non riuscire, lasciando inutilizzabile il LUN di origine. In questo caso, è possibile utilizzare la copia Snapshot per riportare il LUN allo stato precedente al tentativo di ripristino.

- Il LUN di destinazione e il LUN di origine devono avere lo stesso tipo di sistema operativo.

Se il LUN di destinazione ha un tipo di sistema operativo diverso dal LUN di origine, l'host potrebbe perdere l'accesso ai dati al LUN di destinazione dopo l'operazione di ripristino.

### Fasi

1. Interrompere tutti gli accessi host al LUN dall'host.

2. Smontare il LUN sul proprio host in modo che l'host non possa accedere al LUN.

3. Dismappare il LUN:

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Determinare la copia Snapshot in cui si desidera ripristinare il LUN:

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Creare una copia Snapshot del LUN prima di ripristinare il LUN:

```
volume snapshot create -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

6. Ripristinare il LUN specificato in un volume:

```
volume snapshot restore-file -vserver vserver_name -volume volume_name  
-snapshot snapshot_name -path lun_path
```

7. Seguire le istruzioni visualizzate.

8. Se necessario, portare il LUN online:

```
lun modify -vserver vserver_name -path lun_path -state online
```

9. Se necessario, rimappare il LUN:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

10. Dall'host, rimontare il LUN.

11. Riavviare l'accesso al LUN dall'host.

### **Ripristinare tutte le LUN di un volume da una copia Snapshot**

È possibile utilizzare `volume snapshot restore` Comando per ripristinare tutte le LUN di un volume specificato da una copia Snapshot.

#### **Fasi**

1. Interrompere tutti gli accessi host alle LUN dall'host.

L'utilizzo di SnapRestore senza interrompere tutti gli accessi host alle LUN nel volume può causare la corruzione dei dati e gli errori di sistema.

2. Smontare i LUN su tale host in modo che l'host non possa accedere ai LUN.

3. Dismappare le LUN:

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Determinare la copia Snapshot in cui si desidera ripristinare il volume:

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

6. Ripristinare i dati:

```
volume snapshot restore -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

7. Seguire le istruzioni visualizzate.

8. Rimappare le LUN:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

9. Verificare che i LUN siano online:

```
lun show -vserver vserver_name -path lun_path -fields state
```

10. Se le LUN non sono online, portarle online:

```
lun modify -vserver vserver_name -path lun_path -state online
```

11. Impostare i privilegi su admin:

```
set -privilege admin
```

12. Dall'host, rimontare i LUN.

13. Dall'host, riavviare l'accesso ai LUN.

### **Eliminare una o più copie Snapshot esistenti da un volume**

È possibile eliminare manualmente una o più copie Snapshot esistenti dal volume. Questa operazione potrebbe essere utile se è necessario più spazio sul volume.

#### **Fasi**

1. Utilizzare `volume snapshot show` Per verificare quali copie Snapshot si desidera eliminare.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3
```

Vserver	Volume	Snapshot	Size	---Blocks---	
				Total%	Used%
vs3	vol3				
		snap1.2013-05-01_0015	100KB	0%	38%
		snap1.2013-05-08_0015	76KB	0%	32%
		snap2.2013-05-09_0010	76KB	0%	32%
		snap2.2013-05-10_0010	76KB	0%	32%
		snap3.2013-05-10_1005	72KB	0%	31%
		snap3.2013-05-10_1105	72KB	0%	31%
		snap3.2013-05-10_1205	72KB	0%	31%
		snap3.2013-05-10_1305	72KB	0%	31%
		snap3.2013-05-10_1405	72KB	0%	31%
		snap3.2013-05-10_1505	72KB	0%	31%

10 entries were displayed.

## 2. Utilizzare volume snapshot delete Comando per eliminare le copie Snapshot.

Se si desidera...	Immettere questo comando...
Eliminare una singola copia Snapshot	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name</code>
Eliminare più copie Snapshot	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name1[, snapshot_name2,...]</code>
Elimina tutte le copie Snapshot	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot *</code>

Nell'esempio seguente vengono eliminate tutte le copie Snapshot del volume vol3.

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *
```

10 entries were acted on.

## Utilizza le LUN FlexClone per proteggere i tuoi dati

### Utilizza le LUN FlexClone per proteggere la tua panoramica dei dati

Un LUN FlexClone è una copia point-in-time e scrivibile di un altro LUN in un volume

attivo o in una copia Snapshot. Il clone e il suo padre possono essere modificati indipendentemente senza influire l'uno sull'altro.

Un LUN FlexClone condivide inizialmente lo spazio con il LUN di origine. Per impostazione predefinita, il LUN FlexClone eredita l'attributo spazio-riservato del LUN padre. Ad esempio, se il LUN principale non è riservato allo spazio, anche il LUN FlexClone non è riservato per impostazione predefinita. Tuttavia, è possibile creare un LUN FlexClone non riservato allo spazio da un LUN padre che è riservato allo spazio.

Quando si clona un LUN, la condivisione dei blocchi avviene in background e non è possibile creare una copia Snapshot del volume fino al termine della condivisione dei blocchi.

È necessario configurare il volume per attivare la funzione di eliminazione automatica del LUN FlexClone con `volume snapshot autodelete modify` comando. In caso contrario, se si desidera eliminare automaticamente i LUN FlexClone ma il volume non è configurato per l'eliminazione automatica di FlexClone, non viene eliminata alcuna LUN FlexClone.

Quando si crea un LUN FlexClone, la funzione di eliminazione automatica del LUN FlexClone viene disattivata per impostazione predefinita. È necessario abilitarlo manualmente su ogni LUN FlexClone prima che il LUN FlexClone possa essere cancellato automaticamente. Se si utilizza il provisioning di volumi semi-spessi e si desidera la garanzia di scrittura "Best effort" fornita da questa opzione, è necessario rendere disponibili *tutti* i LUN FlexClone per l'eliminazione automatica.



Quando si crea un LUN FlexClone da una copia Snapshot, il LUN viene automaticamente suddiviso dalla copia Snapshot utilizzando un processo in background efficiente in termini di spazio, in modo che il LUN non continui a dipendere dalla copia Snapshot o non occupi spazio aggiuntivo. Se la suddivisione in background non è stata completata e la copia Snapshot viene eliminata automaticamente, il LUN FlexClone viene cancellato anche se la funzione di eliminazione automatica di FlexClone per il LUN FlexClone è stata disattivata. Una volta completata la suddivisione in background, il LUN FlexClone non viene cancellato anche se tale copia Snapshot viene eliminata.

#### Informazioni correlate

["Gestione dello storage logico"](#)

#### Motivi per utilizzare le LUN FlexClone

È possibile utilizzare LUN FlexClone per creare più copie di lettura/scrittura di un LUN.

Questa operazione potrebbe essere utile per i seguenti motivi:

- È necessario creare una copia temporanea di un LUN a scopo di test.
- È necessario rendere disponibile una copia dei dati a utenti aggiuntivi senza fornire loro l'accesso ai dati di produzione.
- Si desidera creare un clone di un database per le operazioni di manipolazione e proiezione, conservando al contempo i dati originali in una forma inalterata.
- Si desidera accedere a un sottoinsieme specifico dei dati di un LUN (un volume logico o un file system specifico in un gruppo di volumi, O un file o un set di file specifico in un file system) e copiarlo nel LUN originale, senza ripristinare il resto dei dati nel LUN originale. Funziona su sistemi operativi che supportano contemporaneamente il montaggio di un LUN e di un clone del LUN. SnapDrive per UNIX supporta questa funzionalità con `snap connect` comando.
- Sono necessari più host DI boot SAN con lo stesso sistema operativo.

## Come un volume FlexVol può recuperare spazio libero con l'impostazione di eliminazione automatica

È possibile attivare l'impostazione di eliminazione automatica di un volume FlexVol per eliminare automaticamente i file FlexClone e i LUN FlexClone. Attivando l'eliminazione automatica, è possibile recuperare una quantità di spazio libero di destinazione nel volume quando un volume è quasi pieno.

È possibile configurare un volume in modo che avvii automaticamente l'eliminazione dei file FlexClone e dei LUN FlexClone quando lo spazio libero nel volume scende al di sotto di un determinato valore di soglia e interrompa automaticamente l'eliminazione dei cloni quando viene recuperata una quantità di spazio libero di destinazione nel volume. Sebbene non sia possibile specificare il valore di soglia che avvia l'eliminazione automatica dei cloni, è possibile specificare se un clone è idoneo per l'eliminazione ed è possibile specificare la quantità di spazio libero di destinazione per un volume.

Un volume elimina automaticamente i file FlexClone e i LUN FlexClone quando lo spazio libero nel volume scende al di sotto di una determinata soglia e quando vengono soddisfatti i seguenti requisiti:

- La funzione di eliminazione automatica è attivata per il volume che contiene i file FlexClone e i LUN FlexClone.

È possibile attivare la funzione di eliminazione automatica per un volume FlexVol utilizzando `volume snapshot autodelete modify` comando. È necessario impostare `-trigger` parametro a `volume` oppure `snap_reserve` Per eliminare automaticamente i file FlexClone e le LUN FlexClone di un volume.

- La funzione di eliminazione automatica è abilitata per i file FlexClone e le LUN FlexClone.

È possibile attivare l'eliminazione automatica per un file FlexClone o un LUN FlexClone utilizzando `file clone create` con il `-autodelete` parametro. Di conseguenza, è possibile conservare alcuni file FlexClone e LUN FlexClone disattivando l'eliminazione automatica per i cloni e garantendo che altre impostazioni del volume non sovrascrivano l'impostazione del clone.

## Configurare un volume FlexVol per eliminare automaticamente i file FlexClone e i LUN FlexClone

È possibile abilitare un volume FlexVol per eliminare automaticamente i file FlexClone e i LUN FlexClone con l'eliminazione automatica attivata quando lo spazio libero nel volume scende al di sotto di una determinata soglia.

### Di cosa hai bisogno

- Il volume FlexVol deve contenere file FlexClone e LUN FlexClone ed essere online.
- Il volume FlexVol non deve essere un volume di sola lettura.

### Fasi

1. Attivare l'eliminazione automatica dei file FlexClone e dei LUN FlexClone nel volume FlexVol utilizzando `volume snapshot autodelete modify` comando.
  - Per `-trigger` è possibile specificare `volume` oppure `snap_reserve`.
  - Per `-destroy-list` è necessario specificare sempre `lun_clone`, `file_clone` indipendentemente dal fatto che si desideri eliminare un solo tipo di clone. L'esempio seguente mostra come attivare il volume vol1 per l'eliminazione automatica dei file FlexClone e dei LUN FlexClone per la rigenerazione dello spazio fino a quando il 25% del volume non è costituito da spazio libero:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume  
vol1 -enabled true -commitment disrupt -trigger volume -target-free  
-space 25 -destroy-list lun_clone,file_clone
```

```
Volume modify successful on volume:vol1
```



Durante l'attivazione dell'eliminazione automatica dei volumi FlexVol, se si imposta il valore di `-commitment` parametro a. `destroy`, Tutti i file FlexClone e le LUN FlexClone con `-autodelete` parametro impostato su `true` potrebbe essere cancellato quando lo spazio libero nel volume scende al di sotto del valore di soglia specificato. Tuttavia, FlexClone Files e FlexClone LUN con `-autodelete` parametro impostato su `false` non verrà eliminato.

2. Verificare che l'eliminazione automatica dei file FlexClone e dei LUN FlexClone sia attivata nel volume FlexVol utilizzando `volume snapshot autodelete show` comando.

L'esempio seguente mostra che il volume `vol1` è abilitato per l'eliminazione automatica di file FlexClone e LUN FlexClone:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1
```

```
Vserver Name: vs1  
Volume Name: vol1  
Enabled: true  
Commitment: disrupt  
Defer Delete: user_created  
Delete Order: oldest_first  
Defer Delete Prefix: (not specified)*  
Target Free Space: 25%  
Trigger: volume  
Destroy List: lun_clone,file_clone  
Is Constituent Volume: false
```

3. Assicurarsi che l'eliminazione automatica sia attivata per i file FlexClone e le LUN FlexClone nel volume che si desidera eliminare, procedendo come segue:

- a. Attivare l'eliminazione automatica di un file FlexClone o di un LUN FlexClone specifico utilizzando `volume file clone autodelete` comando.

È possibile forzare l'eliminazione automatica di un file FlexClone o di un LUN FlexClone specifico utilizzando `volume file clone autodelete` con il `-force` parametro.

L'esempio seguente mostra che è attivata l'eliminazione automatica del LUN `Lun1_clone` FlexClone contenuto nel volume `vol1`:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path  
/vol/vol1/lun1_clone -enabled true
```

È possibile attivare l'eliminazione automatica quando si creano file FlexClone e LUN FlexClone.

- b. Verificare che il file FlexClone o il LUN FlexClone sia abilitato per l'eliminazione automatica utilizzando `volume file clone show-autodelete` comando.

L'esempio seguente mostra che il LUN `lun 1_clone` FlexClone è abilitato per l'eliminazione automatica:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone  
-path vol/vol1/lun1_clone  
  
Name: vs1  
Path: vol/vol1/lun1_clone  
  
**Autodelete Enabled: true**
```

Per ulteriori informazioni sull'utilizzo dei comandi, vedere le rispettive pagine man.

## Clonare i LUN da un volume attivo

È possibile creare copie dei LUN clonando i LUN nel volume attivo. Queste LUN FlexClone sono copie leggibili e scrivibili delle LUN originali nel volume attivo.

### Di cosa hai bisogno

È necessario installare una licenza FlexClone. Questa licenza è inclusa con **"ONTAP uno"**.

### A proposito di questa attività

Un LUN FlexClone riservato allo spazio richiede tanto spazio quanto il LUN padre riservato allo spazio. Se il LUN FlexClone non è riservato allo spazio, è necessario assicurarsi che il volume disponga di spazio sufficiente per accogliere le modifiche apportate al LUN FlexClone.

### Fasi

1. Prima di creare il clone, è necessario aver verificato che le LUN non siano mappate su un igroup o siano scritte su di esso.
2. Utilizzare `lun show` Per verificare l'esistenza del LUN.

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1	online	unmapped	windows	47.07MB



### 3. Utilizzare `volume file clone create` Per creare il LUN FlexClone.

```
volume file clone create -vserver vs1 -volume vol1 -source-path lun1
-destination-path/lun1_clone
```

Se è necessario che il LUN FlexClone sia disponibile per l'eliminazione automatica, è possibile includere `-autodelete true`. Se si crea questo LUN FlexClone in un volume utilizzando il provisioning semi-thick, è necessario attivare l'eliminazione automatica per tutti i LUN FlexClone.

### 4. Utilizzare `lun show` Per verificare che sia stata creata una LUN.

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/volX/lun1	online	unmapped	windows	47.07MB
vs1	/vol/volX/lun1_clone	online	unmapped	windows	47.07MB

## Creare LUN FlexClone da una copia Snapshot in un volume

È possibile utilizzare una copia Snapshot nel volume per creare copie FlexClone delle LUN. Le copie FlexClone delle LUN sono sia leggibili che scrivibili.

### Di cosa hai bisogno

È necessario installare una licenza FlexClone. Questa licenza è inclusa con ["ONTAP uno"](#).

### A proposito di questa attività

Il LUN FlexClone eredita l'attributo `space reservations` del LUN padre. Un LUN FlexClone riservato allo spazio richiede tanto spazio quanto il LUN padre riservato allo spazio. Se il LUN FlexClone non è riservato allo spazio, il volume deve disporre di spazio sufficiente per consentire le modifiche apportate al clone.

### Fasi

1. Verificare che il LUN non sia mappato o in cui sia in corso la scrittura.
2. Creare una copia Snapshot del volume contenente i LUN:

```
volume snapshot create -vserver vserver_name -volume volume_name -snapshot
snapshot_name
```

È necessario creare una copia Snapshot (la copia Snapshot di backup) del LUN che si desidera clonare.

3. Creare il LUN FlexClone dalla copia Snapshot:

```
file clone create -vserver vserver_name -volume volume_name -source-path
source_path -snapshot-name snapshot_name -destination-path destination_path
```

Se è necessario che il LUN FlexClone sia disponibile per l'eliminazione automatica, è possibile includere `-autodelete true`. Se si crea questo LUN FlexClone in un volume utilizzando il provisioning semi-thick, è necessario attivare l'eliminazione automatica per tutti i LUN FlexClone.

#### 4. Verificare che il LUN FlexClone sia corretto:

```
lun show -vserver vs1 -volume vol1 -lun lun1_clone
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1_clone	online	unmapped	windows	47.07MB
vs1	/vol/vol1/lun1_snap_clone	online	unmapped	windows	47.07MB

#### Impedire l'eliminazione automatica di un file FlexClone o di un LUN FlexClone specifico

Se si configura un volume FlexVol per eliminare automaticamente i file FlexClone e le LUN FlexClone, qualsiasi clone che soddisfa i criteri specificati potrebbe essere cancellato. Se si desidera conservare file FlexClone o LUN FlexClone specifici, è possibile escluderli dal processo di eliminazione automatica di FlexClone.

##### Di cosa hai bisogno

È necessario installare una licenza FlexClone. Questa licenza è inclusa con "ONTAP uno".

##### A proposito di questa attività

Quando si crea un file FlexClone o un LUN FlexClone, per impostazione predefinita l'eliminazione automatica del clone viene disattivata. I file FlexClone e i LUN FlexClone con eliminazione automatica disattivata vengono conservati quando si configura un volume FlexVol per eliminare automaticamente i cloni per recuperare spazio sul volume.



Se si imposta `commitment` sul volume a `try` oppure `disrupt`, È possibile conservare file FlexClone specifici o LUN FlexClone disabilitando l'eliminazione automatica per tali cloni. Tuttavia, se si imposta `commitment` sul volume a `destroy` e le liste `destroy` includono `lun_clone`, `file_clone`, L'impostazione del volume sovrascrive l'impostazione del clone e tutti i file FlexClone e i LUN FlexClone possono essere cancellati indipendentemente dall'impostazione di eliminazione automatica per i cloni.

#### Fasi

1. Impedire l'eliminazione automatica di un file FlexClone o di un LUN FlexClone specifico utilizzando `volume file clone autodelete` comando.

Nell'esempio seguente viene illustrato come disattivare l'eliminazione automatica per FlexClone LUN `lun1_clone` contenuto in `vol1`:

```
cluster1::> volume file clone autodelete -vserver vs1 -volume vol1  
-clone-path lun1_clone -enable false
```

Un file FlexClone o un LUN FlexClone con eliminazione automatica disattivata non può essere cancellato automaticamente per recuperare spazio sul volume.

2. Verificare che l'eliminazione automatica sia disattivata per il file FlexClone o per il LUN FlexClone utilizzando `volume file clone show-autodelete` comando.

L'esempio seguente mostra che l'eliminazione automatica è falsa per il LUN lun 1\_clone FlexClone:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path  
vol/vol1/lun1_clone
```

	Vserver
Name: vs1	
	Clone Path:
vol/vol1/lun1_clone	
	Autodelete
Enabled: false	

## Configurare e utilizzare i backup SnapVault in un ambiente SAN

### Configurare e utilizzare i backup SnapVault in una panoramica dell'ambiente SAN

La configurazione e l'utilizzo di SnapVault in un ambiente SAN sono molto simili alla configurazione e all'utilizzo in un ambiente NAS, ma il ripristino delle LUN in un ambiente SAN richiede alcune procedure speciali.

I backup di SnapVault contengono un set di copie di sola lettura di un volume di origine. In un ambiente SAN è sempre possibile eseguire il backup di interi volumi nel volume secondario SnapVault, non di singole LUN.

La procedura per la creazione e l'inizializzazione della relazione SnapVault tra un volume primario contenente LUN e un volume secondario che funge da backup SnapVault è identica alla procedura utilizzata con i volumi FlexVol utilizzati per i protocolli di file. Questa procedura è descritta in dettaglio in ["Protezione dei dati"](#).

Prima di creare e copiare le copie Snapshot nel volume secondario SnapVault, è importante assicurarsi che le LUN di cui viene eseguito il backup siano in uno stato coerente. L'automazione della creazione delle copie Snapshot con SnapCenter garantisce che le LUN di backup siano complete e utilizzabili dall'applicazione originale.

Esistono tre opzioni di base per il ripristino delle LUN da un volume secondario SnapVault:

- È possibile mappare un LUN direttamente dal volume secondario SnapVault e connettere un host al LUN per accedere al contenuto del LUN.

Il LUN è di sola lettura ed è possibile eseguire il mapping solo dalla copia Snapshot più recente nel backup di SnapVault. Le prenotazioni persistenti e altri metadati LUN vengono persi. Se lo si desidera, è possibile utilizzare un programma di copia sull'host per copiare nuovamente il contenuto del LUN nel LUN originale, se ancora accessibile.

Il numero di serie del LUN è diverso da quello del LUN di origine.

- È possibile clonare qualsiasi copia Snapshot nel volume secondario SnapVault in un nuovo volume di lettura/scrittura.

È quindi possibile mappare qualsiasi LUN del volume e connettere un host al LUN per accedere al contenuto del LUN. Se lo si desidera, è possibile utilizzare un programma di copia sull'host per copiare nuovamente il contenuto del LUN nel LUN originale, se ancora accessibile.

- È possibile ripristinare l'intero volume contenente il LUN da qualsiasi copia Snapshot nel volume secondario SnapVault.

Il ripristino dell'intero volume sostituisce tutte le LUN e tutti i file presenti nel volume. Tutti i nuovi LUN creati dopo la creazione della copia Snapshot andranno persi.

Le LUN mantengono la mappatura, i numeri di serie, gli UUID e le riserve persistenti.

### **Accedere a una copia LUN di sola lettura da un backup di SnapVault**

È possibile accedere a una copia di sola lettura di un LUN dall'ultima copia Snapshot in un backup SnapVault. L'ID LUN, il percorso e il numero di serie sono diversi dal LUN di origine e devono essere prima mappati. Le prenotazioni persistenti, le mappature LUN e gli igroups non vengono replicati nel volume secondario SnapVault.

#### **Di cosa hai bisogno**

- La relazione SnapVault deve essere inizializzata e l'ultima copia Snapshot nel volume secondario SnapVault deve contenere il LUN desiderato.
- La macchina virtuale di storage (SVM) contenente il backup SnapVault deve disporre di una o più LIF con il protocollo SAN desiderato accessibile dall'host utilizzato per accedere alla copia del LUN.
- Se si prevede di accedere alle copie LUN direttamente dal volume secondario SnapVault, è necessario creare in anticipo i propri igroups sulla SVM SnapVault.

È possibile accedere a un LUN direttamente dal volume secondario SnapVault senza dover prima ripristinare o clonare il volume contenente il LUN.

#### **A proposito di questa attività**

Se una nuova copia Snapshot viene aggiunta al volume secondario SnapVault mentre si dispone di un LUN mappato da una copia Snapshot precedente, il contenuto del LUN mappato cambia. Il LUN viene ancora mappato con gli stessi identificatori, ma i dati vengono estratti dalla nuova copia Snapshot. Se le dimensioni del LUN cambiano, alcuni host rilevano automaticamente la modifica delle dimensioni; gli host Windows richiedono una nuova scansione del disco per rilevare qualsiasi modifica delle dimensioni.

#### **Fasi**

1. Eseguire `lun show` Per elencare i LUN disponibili nel volume secondario SnapVault.

In questo esempio, è possibile visualizzare i LUN originali nel volume primario `srcvolA` e le copie nel volume secondario SnapVault `dstvolB`:

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

```
6 entries were displayed.
```

2. Se l'igroup per l'host desiderato non esiste già sulla SVM contenente il volume secondario SnapVault, eseguire `igroup create` per creare un igroup.

Questo comando crea un igroup per un host Windows che utilizza il protocollo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup  
-protocol iscsi -ostype windows  
-initiator iqn.1991-05.com.microsoft:hostA
```

3. Eseguire `lun mapping create` Per mappare la copia LUN desiderata sull'igroup.

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A  
-igroup temp_igroup
```

4. Collegare l'host al LUN e accedere al contenuto del LUN come desiderato.

### Ripristinare una singola LUN da un backup SnapVault

È possibile ripristinare una singola LUN in una nuova posizione o nella posizione originale. È possibile eseguire il ripristino da qualsiasi copia Snapshot nel volume secondario SnapVault. Per ripristinare il LUN nella posizione originale, ripristinarlo in una nuova posizione, quindi copiarlo.

#### Di cosa hai bisogno

- La relazione SnapVault deve essere inizializzata e il volume secondario SnapVault deve contenere una copia Snapshot appropriata per il ripristino.
- La macchina virtuale di storage (SVM) contenente il volume secondario SnapVault deve disporre di una o più LIF con il protocollo SAN desiderato, accessibili dall'host utilizzato per accedere alla copia LUN.
- gli igroups devono già esistere sulla SVM SnapVault.

#### A proposito di questa attività

Il processo include la creazione di un clone di un volume in lettura/scrittura da una copia Snapshot nel volume secondario SnapVault. È possibile utilizzare il LUN direttamente dal clone oppure, facoltativamente, copiare di nuovo il contenuto del LUN nella posizione originale del LUN.

Il LUN nel clone ha un percorso e un numero di serie diversi dal LUN originale. Le prenotazioni persistenti non vengono conservate.

## Fasi

1. Eseguire `snapmirror show` Per verificare il volume secondario che contiene il backup di SnapVault.

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored	Idle	-	true	-

2. Eseguire `volume snapshot show` Per identificare la copia Snapshot da cui si desidera ripristinare il LUN.

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB	snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

3. Eseguire `volume clone create` Per creare un clone di lettura/scrittura dalla copia Snapshot desiderata.

Il clone del volume viene creato nello stesso aggregato del backup di SnapVault. Lo spazio nell'aggregato deve essere sufficiente per memorizzare il clone.

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Eseguire `lun show` Per elencare i LUN nel clone del volume.

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone
```

Vserver	Path	State	Mapped	Type
vserverB	/vol/dstvolB_clone/lun_A	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_B	online	unmapped	windows
vserverB	/vol/dstvolB_clone/lun_C	online	unmapped	windows

```
3 entries were displayed.
```

5. Se l'igroup per l'host desiderato non esiste già sulla SVM contenente il backup SnapVault, eseguire `igroup create` per creare un igroup.

Questo esempio crea un igroup per un host Windows che utilizza il protocollo iSCSI:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
               -protocol iscsi -ostype windows
               -initiator iqn.1991-05.com.microsoft:hostA
```

6. Eseguire `lun mapping create` Per mappare la copia LUN desiderata sull'igroup.

```
cluster::> lun mapping create -vserver vserverB
               -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. Collegare l'host al LUN e accedere al contenuto del LUN, come desiderato.

Il LUN è di lettura/scrittura e può essere utilizzato al posto del LUN originale. Poiché il numero di serie del LUN è diverso, l'host lo interpreta come un LUN diverso dall'originale.

8. Utilizzare un programma di copia sull'host per copiare nuovamente il contenuto del LUN nel LUN originale.

## Ripristinare tutte le LUN di un volume da un backup SnapVault

Se è necessario ripristinare una o più LUN di un volume da un backup SnapVault, è possibile ripristinare l'intero volume. Il ripristino del volume influisce su tutti i LUN del volume.

### Di cosa hai bisogno

La relazione SnapVault deve essere inizializzata e il volume secondario SnapVault deve contenere una copia Snapshot appropriata per il ripristino.

### A proposito di questa attività

Il ripristino di un intero volume riporta il volume allo stato in cui si trovava quando è stata eseguita la copia Snapshot. Se un LUN è stato aggiunto al volume dopo la copia Snapshot, tale LUN viene rimosso durante il processo di ripristino.

Dopo il ripristino del volume, i LUN rimangono mappati agli igroups a cui sono stati mappati poco prima del ripristino. La mappatura LUN potrebbe essere diversa dalla mappatura al momento della copia Snapshot. Le riserve persistenti sulle LUN dei cluster host vengono mantenute.

## Fasi

1. Arrestare i/o su tutti i LUN del volume.
2. Eseguire `snapmirror show` Per verificare il volume secondario che contiene il volume secondario SnapVault.

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored	Idle	-	true	-

3. Eseguire `volume snapshot show` Per identificare la copia Snapshot da cui si desidera eseguire il ripristino.

```
cluster::> volume snapshot show
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vserverB	dstvolB	snap2.2013-02-10_0010	valid	124KB	0%	0%
		snap1.2013-02-10_0015	valid	112KB	0%	0%
		snap2.2013-02-11_0010	valid	164KB	0%	0%

4. Eseguire `snapmirror restore` e specificare `-source-snapshot` Opzione per specificare la copia Snapshot da utilizzare.

La destinazione specificata per il ripristino è il volume originale su cui si sta eseguendo il ripristino.



```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
        -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Se si condividono LUN in un cluster host, ripristinare le riserve persistenti sulle LUN dagli host interessati.

#### **Ripristino di un volume da un backup SnapVault**

Nell'esempio seguente, il LUN denominato lun\_D è stato aggiunto al volume dopo la creazione della copia Snapshot. Dopo aver ripristinato l'intero volume dalla copia Snapshot, lun\_D non viene più visualizzato.

In `lun show` Output dei comandi, è possibile visualizzare i LUN nel volume primario srcvolA e le copie di sola lettura di tali LUN nel volume secondario SnapVault dstvolB. Nessuna copia di lun\_D nel backup di SnapVault.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_D	online	mapped	windows	250.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

7 entries were displayed.

```
cluster::>snapmirror restore -destination-path vserverA:srcvolA
-source-path vserverB:dstvolB
-source-snapshot daily.2013-02-10_0010
```

Warning: All data newer than Snapshot copy hourly.2013-02-11\_1205 on volume vserverA:src\_volA will be deleted.

Do you want to continue? {y|n}: y

[Job 98] Job is queued: snapmirror restore from source "vserverB:dstvolB" for the snapshot daily.2013-02-10\_0010.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

6 entries were displayed.

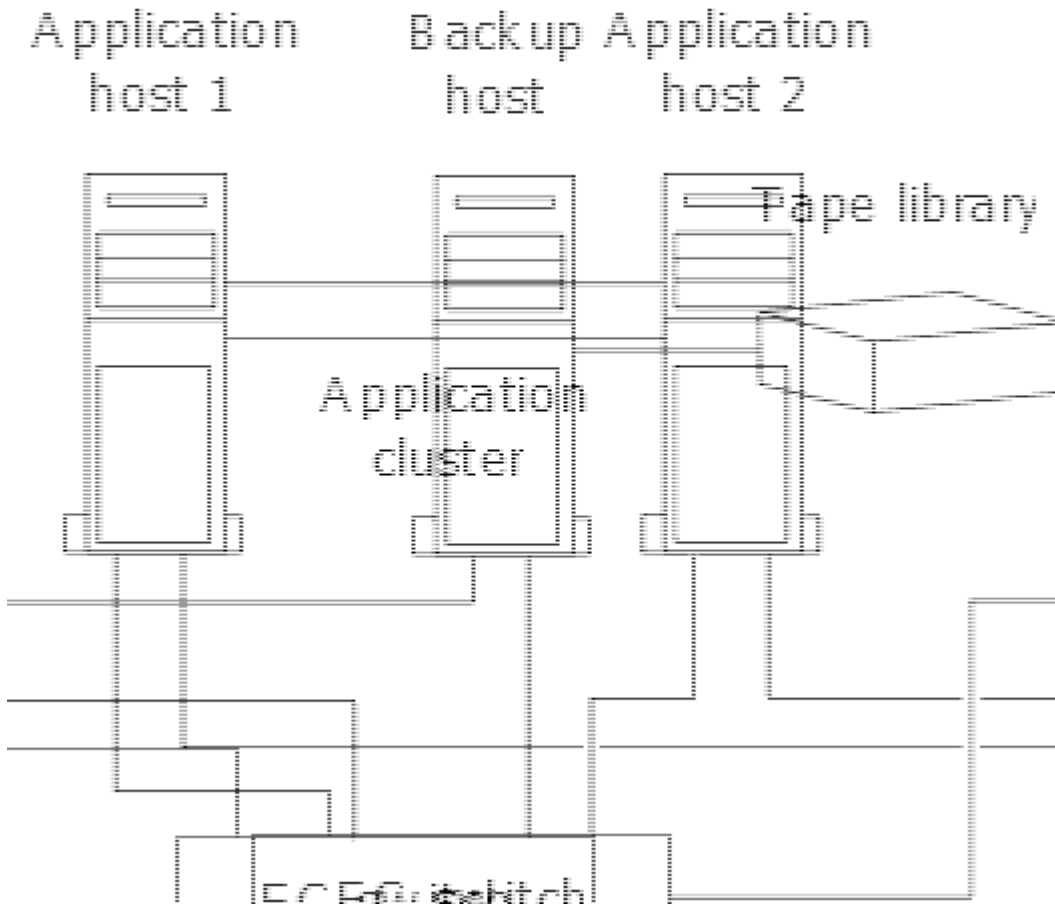
Una volta ripristinato il volume dal volume secondario SnapVault, il volume di origine non contiene più lun\_D. Non è necessario rimappare le LUN nel volume di origine dopo il ripristino, perché sono ancora mappate.

## Come collegare un sistema di backup host al sistema di storage primario

È possibile eseguire il backup dei sistemi SAN su nastro attraverso un host di backup separato per evitare il peggioramento delle performance sull'host dell'applicazione.

È fondamentale che i dati SAN e NAS siano separati a scopo di backup. La figura seguente mostra la configurazione fisica consigliata per un sistema di backup host sul sistema di storage primario. È necessario configurare i volumi solo COME SAN. Le LUN possono essere limitate a un singolo volume oppure possono

essere distribuite su più volumi o sistemi storage.



I volumi su un host possono essere costituiti da un singolo LUN mappato dal sistema di storage o da più LUN utilizzando un gestore di volumi, ad esempio VxVM sui sistemi HP-UX.

## Eseguire il backup di un LUN tramite un sistema di backup host

È possibile utilizzare un LUN clonato da una copia Snapshot come dati di origine per il sistema di backup host.

### Di cosa hai bisogno

Un LUN di produzione deve esistere ed essere mappato a un igroup che includa il nome del nodo WWPN o Initiator del server applicazioni. Anche il LUN deve essere formattato e accessibile all'host

### Fasi

1. Salvare su disco il contenuto dei buffer del file system host.

È possibile utilizzare il comando fornito dal sistema operativo host oppure SnapDrive per Windows o SnapDrive per UNIX. Puoi anche scegliere di includere questo passo nello script di pre-elaborazione del backup SAN.

2. Utilizzare `volume snapshot create` Per creare una copia Snapshot del LUN di produzione.

```
volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot  
-comment "Single snapshot" -foreground false
```

3. Utilizzare `volume file clone create` Per creare un clone del LUN di produzione.

```
volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot  
-name snap_vol3 -destination-path lun1_backup
```

4. Utilizzare `lun igroup create` Per creare un igroup che includa il WWPN del server di backup.

```
lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows  
-initiator 10:00:00:00:c9:73:5b:91
```

5. Utilizzare `lun mapping create` Per mappare il clone LUN creato al punto 3 all'host di backup.

```
lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
```

È possibile scegliere di inserire questo passo nello script di post-elaborazione dell'applicazione DI backup SAN.

6. Individuare il nuovo LUN dall'host e rendere il file system disponibile all'host.

È possibile scegliere di inserire questo passo nello script di post-elaborazione dell'applicazione DI backup SAN.

7. Eseguire il backup dei dati nel clone LUN dall'host di backup su nastro utilizzando l'applicazione DI backup SAN.

8. Utilizzare `lun modify` Comando per portare offline il clone del LUN.

```
lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
```

9. Utilizzare `lun delete` Per rimuovere il clone del LUN.

```
lun delete -vserver vs3 -volume vol3 -lun lun1_backup
```

10. Utilizzare `volume snapshot delete` Comando per rimuovere la copia Snapshot.

```
volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
```

## Riferimento alla configurazione SAN

### Panoramica della configurazione SAN

Una rete SAN è costituita da una soluzione storage connessa agli host tramite un protocollo di trasporto SAN come iSCSI o FC. È possibile configurare la RETE SAN in modo che la soluzione di storage si colleghi agli host tramite uno o più switch. Se si utilizza iSCSI, è anche possibile configurare la SAN in modo che la soluzione di storage si colleghi direttamente all'host senza utilizzare uno switch.

In una SAN, più host, utilizzando sistemi operativi diversi, come Windows, Linux o UNIX, possono accedere alla soluzione di storage contemporaneamente. È possibile utilizzare ["Mappatura selettiva delle LUN"](#) e ["portset"](#) per limitare l'accesso ai dati tra gli host e lo storage.

Per iSCSI, la topologia di rete tra la soluzione di storage e gli host viene definita rete. Per FC, FC/NVMe e FCoE la topologia della rete tra la soluzione di storage e gli host è indicata come fabric. Per creare la ridondanza, che protegge dai rischi di perdita dell'accesso ai dati, è necessario impostare la SAN con coppie ha in una configurazione multi-network o multi-fabric. Le configurazioni che utilizzano nodi singoli o reti/fabric singoli non sono completamente ridondanti, quindi non sono consigliate.

Una volta configurato il SAN, è possibile ["Provisioning dello storage per iSCSI o FC"](#) oppure è possibile ["Eseguire il provisioning dello storage per FC/NVMe"](#). Quindi, è possibile connettersi agli host per iniziare la manutenzione dei dati.

Il supporto del protocollo SAN varia in base alla versione di ONTAP in uso, alla piattaforma e alla configurazione in uso. Per ulteriori informazioni sulla configurazione specifica, consultare la ["Tool di matrice di interoperabilità NetApp"](#).

#### Informazioni correlate

- ["Panoramica dell'amministrazione SAN"](#)
- ["Configurazione, supporto e limitazioni NVMe"](#)

## Configurazioni iSCSI

### Metodi di configurazione degli host SAN iSCSI

È necessario configurare la configurazione iSCSI con coppie ha (High Availability) che si collegano direttamente agli host SAN iSCSI o che si connettono agli host tramite uno o più switch IP.

["Coppie HA"](#) Sono definiti come nodi di reporting per i percorsi Active/Optimized e Active/UnOptimized che verranno utilizzati dagli host per accedere alle LUN. Più host, utilizzando sistemi operativi diversi, come Windows, Linux o UNIX, possono accedere allo storage contemporaneamente. Gli host richiedono che sia installata e configurata una soluzione multipathing supportata che supporti ALUA. I sistemi operativi supportati e le soluzioni multipathing possono essere verificati sul ["Tool di matrice di interoperabilità NetApp"](#).

In una configurazione multi-network, esistono due o più switch che collegano gli host al sistema di storage. Le configurazioni multi-rete sono consigliate perché sono completamente ridondanti. In una configurazione a singola rete, è presente uno switch che connette gli host al sistema di storage. Le configurazioni di rete singola non sono completamente ridondanti.



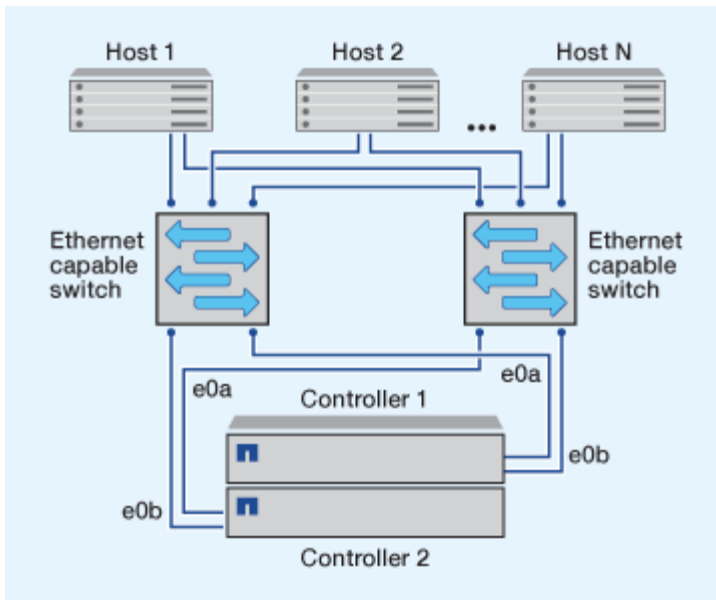
["Configurazioni a nodo singolo"](#) sono sconsigliati perché non forniscono la ridondanza necessaria per supportare la tolleranza agli errori e le operazioni senza interruzioni.

#### Informazioni correlate

- Scopri come ["Mappatura selettiva delle LUN \(SLM\)"](#) Limita i percorsi utilizzati per accedere alle LUN di proprietà di una coppia ha.
- Scopri di più ["LIF SAN"](#).
- Ulteriori informazioni su ["Vantaggi delle VLAN in iSCSI"](#).

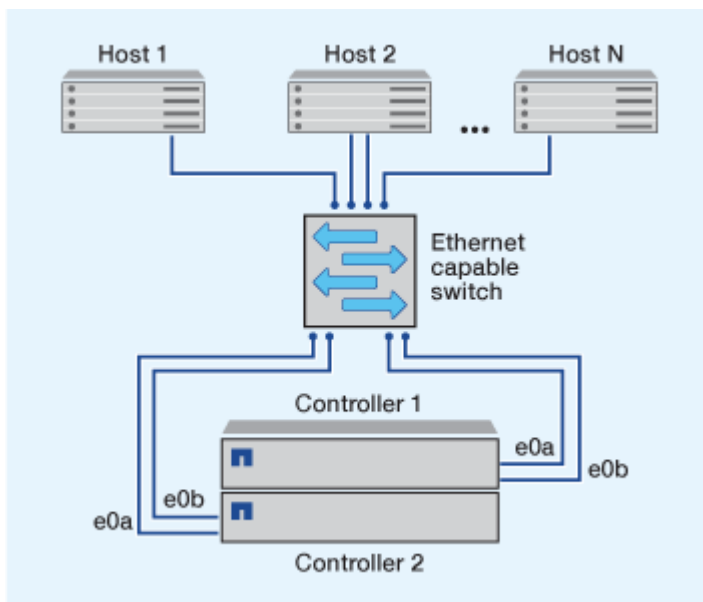
### Configurazioni iSCSI multi-rete

Nelle configurazioni di coppia ha multi-rete, due o più switch connettono la coppia ha a uno o più host. Poiché esistono più switch, questa configurazione è completamente ridondante.



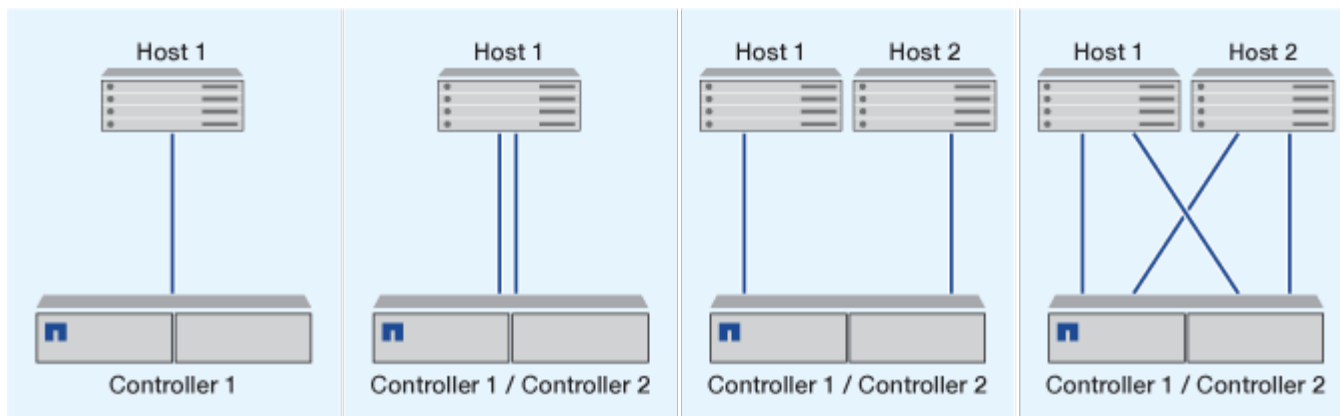
### Configurazioni iSCSI a rete singola

Nelle configurazioni a coppia ha a rete singola, uno switch connette la coppia ha a uno o più host. Poiché esiste un singolo switch, questa configurazione non è completamente ridondante.



### Configurazione iSCSI a collegamento diretto

In una configurazione direct-attached, uno o più host sono collegati direttamente ai controller.



### Vantaggi dell'utilizzo delle VLAN nelle configurazioni iSCSI

Una VLAN è costituita da un gruppo di porte dello switch raggruppate in un dominio di broadcast. Una VLAN può essere su un singolo switch o può abbracciare più chassis switch. Le VLAN statiche e dinamiche consentono di aumentare la sicurezza, isolare i problemi e limitare i percorsi disponibili all'interno dell'infrastruttura di rete IP.

Quando si implementano VLAN in infrastrutture di rete IP di grandi dimensioni, si ottengono i seguenti vantaggi:

- Maggiore sicurezza.

Le VLAN consentono di sfruttare l'infrastruttura esistente pur garantendo una maggiore sicurezza in quanto limitano l'accesso tra diversi nodi di una rete Ethernet o di una SAN IP.

- Maggiore affidabilità della rete Ethernet e della SAN IP grazie all'isolamento dei problemi.
- Riduzione dei tempi di risoluzione dei problemi limitando lo spazio dei problemi.
- Riduzione del numero di percorsi disponibili per una determinata porta di destinazione iSCSI.
- Riduzione del numero massimo di percorsi utilizzati da un host.

La presenza di troppi percorsi rallenta i tempi di riconnessione. Se un host non dispone di una soluzione multipathing, è possibile utilizzare le VLAN per consentire un solo percorso.

### VLAN dinamiche

Le VLAN dinamiche sono basate sull'indirizzo MAC. È possibile definire una VLAN specificando l'indirizzo MAC dei membri che si desidera includere.

Le VLAN dinamiche offrono flessibilità e non richiedono il mapping alle porte fisiche in cui il dispositivo è fisicamente collegato allo switch. È possibile spostare un cavo da una porta all'altra senza riconfigurare la VLAN.

### VLAN statiche

Le VLAN statiche sono basate su porta. Lo switch e la porta dello switch vengono utilizzati per definire la VLAN e i relativi membri.

Le VLAN statiche offrono una maggiore sicurezza perché non è possibile violare le VLAN utilizzando lo spoofing MAC (Media Access Control). Tuttavia, se qualcuno ha accesso fisico allo switch, la sostituzione di un

cavo e la riconfigurazione dell'indirizzo di rete possono consentire l'accesso.

In alcuni ambienti, è più semplice creare e gestire VLAN statiche rispetto alle VLAN dinamiche. Questo perché le VLAN statiche richiedono solo la specifica dello switch e dell'identificatore della porta, invece dell'indirizzo MAC a 48 bit. Inoltre, è possibile etichettare gli intervalli di porte dello switch con l'identificatore VLAN.

## Configurazioni FC

### Modalità di configurazione degli host SAN FC & FC-NVMe

Si consiglia di configurare gli host SAN FC e FC-NVMe utilizzando coppie ha e un minimo di due switch. Questo garantisce ridondanza a livello di fabric e di sistema storage per supportare la tolleranza agli errori e le operazioni senza interruzioni. Non è possibile collegare direttamente host FC o FC-NVMe SAN a coppie ha senza utilizzare uno switch.

Cascade, Partial Mesh, full mesh, core-edge e director fabric sono tutti metodi standard di settore per collegare switch FC a un fabric e sono tutti supportati. L'utilizzo di fabric switch FC eterogenei non è supportato, tranne nel caso di switch blade integrati. Le eccezioni specifiche sono elencate nella ["Tool di matrice di interoperabilità"](#). Un fabric può essere costituito da uno o più switch e i controller di storage possono essere collegati a più switch.

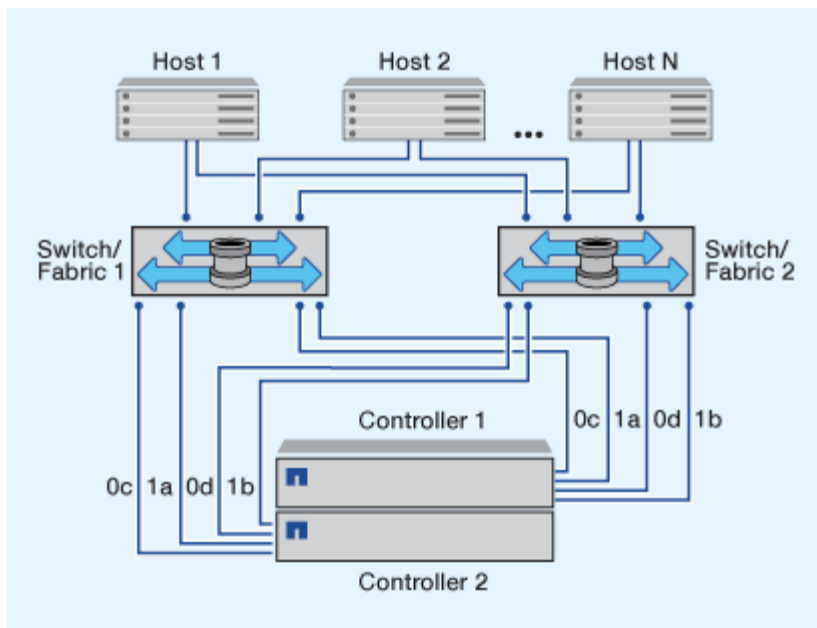
Più host, utilizzando sistemi operativi diversi, come Windows, Linux o UNIX, possono accedere contemporaneamente ai controller di storage. Gli host richiedono l'installazione e la configurazione di una soluzione multipathing supportata. È possibile verificare i sistemi operativi e le soluzioni multipathing supportate tramite Interoperability Matrix Tool.

### Configurazioni FC e FC-NVMe multi-fabric

Nelle configurazioni ha Pair multi-fabric, sono presenti due o più switch che collegano coppie ha a uno o più host. Per semplicità, la seguente figura di coppia ha multi-fabric mostra solo due fabric, ma puoi avere due o più fabric in qualsiasi configurazione multi-fabric.

I numeri delle porte di destinazione FC (0C, 0d, 1a, 1b) nelle illustrazioni sono esempi. I numeri di porta effettivi variano a seconda del modello del nodo di storage e dell'utilizzo di adattatori di espansione.



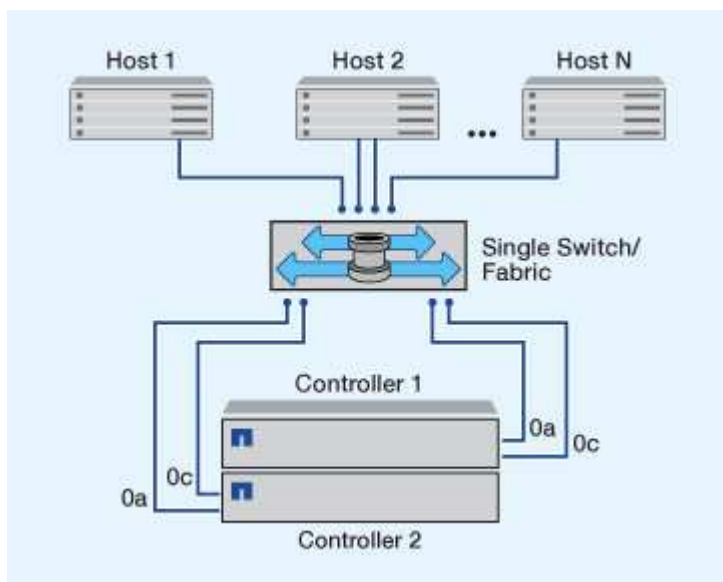


### Configurazioni FC e FC-NVMe single-fabric

Nelle configurazioni a coppia ha a fabric singolo, esiste un fabric che collega entrambi i controller della coppia ha a uno o più host. Poiché gli host e i controller sono connessi tramite un singolo switch, le configurazioni ha Pair single-fabric non sono completamente ridondanti.

I numeri delle porte di destinazione FC (0A, 0C) nelle illustrazioni sono esempi. I numeri di porta effettivi variano a seconda del modello del nodo di storage e dell'utilizzo di adattatori di espansione.

Tutte le piattaforme che supportano le configurazioni FC supportano le configurazioni ha Pair single-fabric.



"Configurazioni a nodo singolo" sono sconsigliati perché non forniscono la ridondanza necessaria per supportare la tolleranza agli errori e le operazioni senza interruzioni.

### Informazioni correlate

- Scopri come "[Mappatura selettiva delle LUN \(SLM\)](#)" Limita i percorsi utilizzati per accedere alle LUN di proprietà di una coppia ha.

- Scopri di più ["LIF SAN"](#).

## Best practice per la configurazione dello switch FC

Per ottenere prestazioni ottimali, è necessario prendere in considerazione alcune Best practice durante la configurazione dello switch FC.

Un'impostazione della velocità di collegamento fissa è la procedura migliore per le configurazioni degli switch FC, in particolare per i fabric di grandi dimensioni, in quanto offre le migliori prestazioni per le ricostruzioni del fabric e può risparmiare significativamente tempo. Sebbene la negoziazione automatica offra la massima flessibilità, la configurazione dello switch FC non sempre funziona come previsto e aggiunge tempo alla sequenza generale di fabric-build.

Tutti gli switch collegati al fabric devono supportare la virtualizzazione NPIV (N\_Port ID Virtualization) e attivare NPIV. ONTAP utilizza NPIV per presentare i target FC a un fabric.

Per ulteriori informazioni sugli ambienti supportati, vedere ["Tool di matrice di interoperabilità NetApp"](#).

Per informazioni sulle Best practice FC e iSCSI, vedere ["Report tecnico NetApp 4080: Best practice per le SAN moderne"](#).

## Numero supportato di conteggi FC hop

Il numero massimo di hop FC supportato tra un host e un sistema storage dipende dal fornitore dello switch e dal supporto del sistema storage per le configurazioni FC.

Il numero di hop viene definito come il numero di switch nel percorso tra l'iniziatore (host) e la destinazione (sistema di storage). Cisco fa anche riferimento a questo valore come *diametro del fabric SAN*.

Cambiare fornitore	Numero di hop supportato
Brocade	7 GB per FC, 5 GB per FCoE
Cisco	7 per FC, fino a 3 switch possono essere FCoE.

## Informazioni correlate

["Download NetApp: Documenti matrice di scalabilità Brocade"](#)

["Download NetApp: Documenti Cisco Scalability Matrix"](#)

## Velocità supportate dalla porta di destinazione FC

Le porte di destinazione FC possono essere configurate per funzionare a velocità diverse. Impostare la velocità della porta di destinazione in modo che corrisponda alla velocità del dispositivo a cui si connette. Tutte le porte di destinazione utilizzate da un determinato host devono essere impostate alla stessa velocità.

Le porte di destinazione FC possono essere utilizzate per le configurazioni FC-NVMe esattamente come per le configurazioni FC.

È necessario impostare la velocità della porta di destinazione in modo che corrisponda alla velocità del

dispositivo a cui si connette invece di utilizzare la negoziazione automatica. Una porta impostata per la negoziazione automatica può richiedere più tempo per riconnettersi dopo un takeover/giveback o un'altra interruzione.

È possibile configurare le porte integrate e gli adattatori di espansione in modo che funzionino alle seguenti velocità. Ogni porta del controller e dell'adattatore di espansione può essere configurata singolarmente per diverse velocità in base alle esigenze.

Porte da 4 GB	Porte da 8 GB	Porte da 16 GB	Porte da 32 GB
<ul style="list-style-type: none"><li>• 4 GB</li><li>• 2 GB</li><li>• 1 GB</li></ul>	<ul style="list-style-type: none"><li>• 8 GB</li><li>• 4 GB</li><li>• 2 GB</li></ul>	<ul style="list-style-type: none"><li>• 16 GB</li><li>• 8 GB</li><li>• 4 GB</li></ul>	<ul style="list-style-type: none"><li>• 32 GB</li><li>• 16 GB</li><li>• 8 GB</li></ul>



Le porte UTA2 possono utilizzare un adattatore SFP+ da 8 GB per supportare velocità da 8, 4 e 2 GB, se necessario.

Consigli per la configurazione della porta di destinazione FC

Per ottenere le migliori prestazioni e la massima disponibilità, è necessario utilizzare la configurazione della porta di destinazione FC consigliata.

La seguente tabella mostra l'ordine di utilizzo delle porte preferito per le porte di destinazione FC e FC-NVMe integrate. Per gli adattatori di espansione, le porte FC devono essere distribuite in modo che non utilizzino lo stesso ASIC per la connettività. L'ordine degli slot preferiti è riportato nella "NetApp Hardware Universe" Per la versione del software ONTAP utilizzata dal controller.

FC-NVMe è supportato sui seguenti modelli:

- AFF A300



Le porte integrate AFF A300 non supportano FC-NVMe.

- AFF A700
- AFF A700
- AFF A800



I sistemi FAS2520 non hanno porte FC integrate e non supportano adattatori aggiuntivi.

Controller	Coppie di porte con ASIC condiviso	Numero di porte di destinazione: Porte preferite
FAS9000, AFF A700, AFF A700 e AFF A800	Nessuno	Tutte le porte dati si trovano sugli adattatori di espansione. Vedere "NetApp Hardware Universe" per ulteriori informazioni.

Controller	Coppie di porte con ASIC condiviso	Numero di porte di destinazione: Porte preferite
8080, 8060 e 8040	0e+0f  0g+0h	1: 0e  2: 0e, 0g  3: 0e, 0g, 0h  4: 0e, 0g, 0f, 0h
FAS8200 e AFF A300	0g+0h	1: 0 g.  2: 0 g, 0 ore
8020	0c+0d	1: 0c  2: 0c, 0d
62xx	0a+0b  0c+0d	1: 0a  2: 0a, 0c  3: 0a, 0c, 0b  4: 0a, 0c, 0b, 0d
32xx	0c+0d	1: 0c  2: 0c, 0d
FAS2554, FAS2552, FAS2600, FAS2720, FAS2750, AFF A200 e AFF A220	0c+0d  0e+0f	1: 0c  2: 0c, 0e  3: 0c, 0e, 0d  4: 0c, 0e, 0d, 0f

## Gestire i sistemi con adattatori FC

### Panoramica sulla gestione dei sistemi con adattatori FC

Sono disponibili comandi per gestire gli adattatori FC integrati e le schede adattatore FC. Questi comandi possono essere utilizzati per configurare la modalità dell'adattatore, visualizzare le informazioni sull'adattatore e modificare la velocità.

La maggior parte dei sistemi storage dispone di adattatori FC integrati che possono essere configurati come iniziatori o destinazioni. È inoltre possibile utilizzare schede adattatore FC configurate come iniziatori o destinazioni. Gli iniziatori si connettono agli shelf di dischi back-end e possibilmente a storage array esterni (FlexArray). Le destinazioni si connettono solo agli switch FC. Le porte HBA di destinazione FC e la velocità della porta dello switch devono essere impostate sullo stesso valore e non devono essere impostate su auto.

## Comandi per la gestione degli adattatori FC

È possibile utilizzare i comandi FC per gestire gli adattatori di destinazione FC, gli adattatori FC Initiator e gli adattatori FC integrati per lo storage controller. Gli stessi comandi vengono utilizzati per gestire gli adattatori FC per il protocollo FC e il protocollo FC-NVMe.

I comandi FC Initiator Adapter funzionano solo a livello di nodo. È necessario utilizzare `run -node node_name` Prima di poter utilizzare i comandi FC Initiator Adapter.

## Comandi per la gestione degli adattatori di destinazione FC

Se si desidera...	Utilizzare questo comando...
Visualizza le informazioni sulla scheda FC su un nodo	<code>network fcp adapter show</code>
Modificare i parametri dell'adattatore di destinazione FC	<code>network fcp adapter modify</code>
Visualizza le informazioni sul traffico del protocollo FC	<code>run -node node_name sysstat -f</code>
Visualizza per quanto tempo il protocollo FC è in esecuzione	<code>run -node node_name uptime</code>
Visualizzare la configurazione e lo stato dell'adattatore	<code>run -node node_name sysconfig -v adapter</code>
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	<code>run -node node_name sysconfig -ac</code>
Visualizzare una pagina man per un comando	<code>man command_name</code>

## Comandi per la gestione degli adattatori FC Initiator

Se si desidera...	Utilizzare questo comando...
Visualizza le informazioni per tutti gli iniziatori e i relativi adattatori in un nodo	<code>run -node node_name storage show adapter</code>
Visualizzare la configurazione e lo stato dell'adattatore	<code>run -node node_name sysconfig -v adapter</code>
Verificare quali schede di espansione sono installate e se sono presenti errori di configurazione	<code>run -node node_name sysconfig -ac</code>

## Comandi per la gestione degli adattatori FC integrati

Se si desidera...	Utilizzare questo comando...
Visualizza lo stato delle porte FC integrate	<code>system node hardware unified-connect show</code>

### Configurare gli adattatori FC per la modalità Initiator

È possibile configurare singole porte FC di adattatori integrati e alcune schede FC per la modalità Initiator. La modalità Initiator viene utilizzata per collegare le porte a unità a nastro, librerie a nastro o storage di terze parti con la virtualizzazione FlexArray o l'importazione di LUN esterne (FLI).

#### Di cosa hai bisogno

- Le LIF della scheda di rete devono essere rimosse da tutti i set di porte di cui sono membri.
- Tutti i LIF di ogni macchina virtuale di storage (SVM) che utilizza la porta fisica da modificare devono essere migrati o distrutti prima di cambiare la personalità della porta fisica da destinazione a iniziatore.

#### A proposito di questa attività

Ogni porta FC integrata può essere configurata singolarmente come iniziatore o destinazione. Le porte di alcuni adattatori FC possono anche essere configurate singolarmente come una porta di destinazione o una porta initiator, proprio come le porte FC integrate. In è disponibile un elenco di adattatori che è possibile configurare per la modalità di destinazione "[NetApp Hardware Universe](#)".



NVMe/FC supporta la modalità Initiator.

#### Fasi

1. Rimuovere tutti i file LIF dalla scheda:

```
network interface delete -vserver SVM_name -lif lif_name,lif_name
```

2. Porta l'adattatore offline:

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin down
```

Se l'adattatore non viene scollegato, è anche possibile rimuovere il cavo dalla porta dell'adattatore appropriata sul sistema.

3. Cambiare la scheda di rete da destinazione a iniziatore:

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Riavviare il nodo che ospita l'adattatore modificato.

5. Verificare che le porte FC siano configurate nello stato corretto per la configurazione:

```
system hardware unified-connect show
```

6. Riportare l'adattatore online:

```
node run -node node_name storage enable adapter adapter_port
```

### Configurare gli adattatori FC per la modalità di destinazione

È possibile configurare singole porte FC di adattatori integrati e alcune schede adattatore FC per la modalità di destinazione. La modalità di destinazione viene utilizzata per collegare le porte agli iniziatori FC.

#### A proposito di questa attività

Ogni porta FC integrata può essere configurata singolarmente come iniziatore o destinazione. Le porte di alcuni adattatori FC possono anche essere configurate singolarmente come una porta di destinazione o una porta initiator, proprio come le porte FC integrate. In è disponibile un elenco di adattatori che è possibile configurare per la modalità di destinazione ["NetApp Hardware Universe"](#).

La stessa procedura viene utilizzata per la configurazione degli adattatori FC per il protocollo FC e il protocollo FC-NVMe. Tuttavia, solo alcuni adattatori FC supportano FC-NVMe. Vedere ["NetApp Hardware Universe"](#) Per un elenco di adattatori che supportano il protocollo FC-NVMe.

#### Fasi

1. Portare l'adattatore offline:

```
node run -node node_name storage disable adapter adapter_name
```

Se l'adattatore non viene scollegato, è anche possibile rimuovere il cavo dalla porta dell'adattatore appropriata sul sistema.

2. Cambiare la scheda di rete da iniziatore a destinazione:

```
system node hardware unified-connect modify -t target -node node_name adapter adapter_name
```

3. Riavviare il nodo che ospita l'adattatore modificato.
4. Verificare che la porta di destinazione abbia la configurazione corretta:

```
network fcp adapter show -node node_name
```

5. Porta online il tuo adattatore:

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

### Visualizza informazioni su un adattatore di destinazione FC

È possibile utilizzare `network fcp adapter show` Per visualizzare le informazioni relative alla configurazione del sistema e all'adattatore FC del sistema.

#### Fase

1. Consente di visualizzare le informazioni sull'adattatore FC utilizzando `network fcp adapter show` comando.

L'output visualizza le informazioni di configurazione del sistema e le informazioni sull'adattatore per ogni slot utilizzato.

```
network fcp adapter show -instance -node nodel -adapter 0a
```

### Modificare la velocità dell'adattatore FC

È necessario impostare la velocità della porta di destinazione dell'adattatore in modo che corrisponda alla velocità del dispositivo a cui si connette, invece di utilizzare la negoziazione automatica. Una porta impostata per la negoziazione automatica può richiedere più tempo per riconnettersi dopo un takeover/giveback o un'altra interruzione.

### Di cosa hai bisogno

Tutte le LIF che utilizzano questo adattatore come porta home devono essere offline.

### A proposito di questa attività

Poiché questa attività comprende tutte le macchine virtuali di storage (SVM) e tutte le LIF in un cluster, è necessario utilizzare `-home-port` e `-home-lif` parametri per limitare l'ambito di questa operazione. Se non si utilizzano questi parametri, l'operazione si applica a tutte le LIF del cluster, cosa che potrebbe non essere auspicabile.

### Fasi

1. Porta tutti i LIF su questo adattatore offline:

```
network interface modify -vserver * -lif * { -home-node nodel -home-port 0c }  
-status-admin down
```

2. Portare l'adattatore offline:

```
network fcp adapter modify -node nodel -adapter 0c -state down
```

Se l'adattatore non viene scollegato, è anche possibile rimuovere il cavo dalla porta dell'adattatore appropriata sul sistema.

3. Determinare la velocità massima per l'adattatore porta:

```
fcp adapter show -instance
```

Non è possibile modificare la velocità della scheda oltre la velocità massima.

4. Modificare la velocità dell'adattatore:

```
network fcp adapter modify -node nodel -adapter 0c -speed 16
```

5. Portare l'adattatore online:

```
network fcp adapter modify -node nodel -adapter 0c -state up
```

6. Portare online tutti i file LIF della scheda di rete:

```
network interface modify -vserver * -lif * { -home-node nodel -home-port 0c }  
-status-admin up
```



## Porte FC supportate

Il numero di porte FC integrate e di porte CNA/UTA2 configurate per FC varia in base al modello del controller. Le porte FC sono disponibili anche tramite adattatori di espansione FC target supportati o schede UTA2 aggiuntive configurate con adattatori FC SFP+.

## Porte FC, UTA e UTA2 integrate

- Le porte onboard possono essere configurate singolarmente come porte FC di destinazione o iniziatore.
- Il numero di porte FC integrate varia a seconda del modello di controller.

Il ["NetApp Hardware Universe"](#) Contiene un elenco completo delle porte FC integrate su ciascun modello di controller.

- I sistemi FAS2520 non supportano FC.

## Porte FC dell'adattatore di espansione di destinazione

- Gli adattatori di espansione di destinazione disponibili variano a seconda del modello di controller.

Il ["NetApp Hardware Universe"](#) contiene un elenco completo degli adattatori di espansione di destinazione per ciascun modello di controller.

- Le porte di alcuni adattatori di espansione FC sono configurate in fabbrica come iniziatori o destinazioni e non possono essere modificate.

Altre porte possono essere configurate singolarmente come porte FC di destinazione o iniziatore, proprio come le porte FC integrate. Un elenco completo è disponibile in ["NetApp Hardware Universe"](#).

## Evitare la perdita di connettività quando si utilizza l'adattatore X1133A-R6

È possibile evitare la perdita di connettività durante un errore di porta configurando il sistema con percorsi ridondanti per separare gli HBA X1133A-R6.

X1133A-R6 HBA è un adattatore FC da 16 GB a 4 porte composto da due coppie di 2 porte. L'adattatore X1133A-R6 può essere configurato come modalità di destinazione o Initiator. Ogni coppia di 2 porte è supportata da un singolo ASIC (ad esempio, porta 1 e porta 2 su ASIC 1 e porta 3 e porta 4 su ASIC 2). Entrambe le porte di un singolo ASIC devono essere configurate per funzionare nella stessa modalità, sia in modalità di destinazione che in modalità iniziatore. Se si verifica un errore con ASIC che supporta una coppia, entrambe le porte della coppia passano offline.

Per evitare questa perdita di connettività, configurare il sistema con percorsi ridondanti per separare gli HBA X1133A-R6 o con percorsi ridondanti alle porte supportate da diversi ASIC sull'HBA.

## Gestire gli adattatori X1143A-R6

### Panoramica delle configurazioni delle porte supportate per gli adattatori X1143A-R6

Per impostazione predefinita, l'adattatore X1143A-R6 è configurato in modalità di destinazione FC, ma è possibile configurarne le porte come porte Ethernet da 10 GB e FCoE (CNA) o come porte FC Initiator o di destinazione da 16 GB. Questo richiede diversi adattatori SFP+.

Se configurati per Ethernet e FCoE, gli adattatori X1143A-R6 supportano il traffico di destinazione simultaneo di NIC e FCoE sulla stessa porta 10-GBE. Se configurata per FC, ciascuna coppia di due porte che condivide lo stesso ASIC può essere configurata singolarmente per la destinazione FC o la modalità iniziatore FC. Ciò significa che un singolo adattatore X1143A-R6 può supportare la modalità di destinazione FC su una coppia a due porte e la modalità iniziatore FC su un'altra coppia a due porte. Le coppie di porte collegate allo stesso ASIC devono essere configurate nella stessa modalità.

In modalità FC, l'adattatore X1143A-R6 si comporta come qualsiasi dispositivo FC esistente con velocità fino a 16 Gbps. In modalità CNA, è possibile utilizzare l'adattatore X1143A-R6 per la condivisione simultanea del traffico NIC e FCoE sulla stessa porta 10 GbE. La modalità CNA supporta solo la modalità di destinazione FC per la funzione FCoE.

## Configurare le porte

Per configurare l'adattatore di destinazione unificato (X1143A-R6), è necessario configurare le due porte adiacenti sullo stesso chip nella stessa modalità personality.

### Fasi

1. Configurare le porte in base alle necessità per Fibre Channel (FC) o Converged Network Adapter (CNA) utilizzando `system node hardware unified-connect modify` comando.
2. Collegare i cavi appropriati per FC o Ethernet da 10 GB.
3. Verificare di avere installato il modulo SFP+ corretto:

```
network fcp adapter show -instance -node -adapter
```

Per CNA, è necessario utilizzare un SFP Ethernet da 10 GB. Per FC, è necessario utilizzare un SFP da 8 GB o un SFP da 16 GB, in base al fabric FC a cui è collegato.

## Modificare la porta UTA2 dalla modalità CNA alla modalità FC

Modificare la porta UTA2 dalla modalità Converged Network Adapter (CNA) alla modalità Fibre Channel (FC) per supportare la modalità FC Initiator e FC target. È necessario modificare la personalità dalla modalità CNA alla modalità FC quando si desidera modificare il supporto fisico che collega la porta alla rete.

### Fasi

1. Portare l'adattatore offline:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin down
```

2. Modificare la modalità della porta:

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. Riavviare il nodo, quindi portare l'adattatore in linea:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin up
```

4. Avvisare l'amministratore o il gestore VIF di eliminare o rimuovere la porta, a seconda dei casi:

- Se la porta viene utilizzata come porta principale di una LIF, fa parte di un gruppo di interfacce (ifgrp) o ospita VLAN, un amministratore deve eseguire le seguenti operazioni:
  - i. Spostare le LIF, rimuovere la porta da ifgrp o eliminare le VLAN, rispettivamente.
  - ii. Eliminare manualmente la porta eseguendo `network port delete` comando.

Se il `network port delete` il comando non riesce, l'amministratore dovrebbe risolvere gli errori ed eseguire di nuovo il comando.

- Se la porta non viene utilizzata come porta home di un LIF, non è membro di un ifgrp e non ospita VLAN, il gestore VIF deve rimuovere la porta dai record al momento del riavvio.

Se il gestore VIF non rimuove la porta, l'amministratore deve rimuoverla manualmente dopo il riavvio utilizzando `network port delete` comando.

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

Port	IPspace	Broadcast Domain	Link	MTU	Speed(Mbps)	Health
					Admin/Oper	Status
-----	-----	-----	----	----	-----	
...						
e0i	Default	Default	down	1500	auto/10	-
e0f	Default	Default	down	1500	auto/10	-
...						

```
net-f8040-34::> ucadmin show
```

Node	Adapter	Current	Current	Pending	Pending	Admin
		Mode	Type	Mode	Type	
Status						
-----	-----	-----	-----	-----	-----	
net-f8040-34-01						
	0e	cna	target	-	-	
offline						
net-f8040-34-01						
	0f	cna	target	-	-	
offline						
...						

```
net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0
```

```
net-f8040-34::> network interface show -fields home-port, curr-port
```

```

vserver lif                               home-port curr-port
-----
Cluster net-f8040-34-01_clus1 e0a         e0a
Cluster net-f8040-34-01_clus2 e0b         e0b
Cluster net-f8040-34-01_clus3 e0c         e0c
Cluster net-f8040-34-01_clus4 e0d         e0d
net-f8040-34
      cluster_mgmt          e0M         e0M
net-f8040-34
      m                     e0e         e0i
net-f8040-34
      net-f8040-34-01_mgmt1 e0M         e0M
7 entries were displayed.

```

```
net-f8040-34::> ucaadmin modify local 0e fc
```

Warning: Mode on adapter 0e and also adapter 0f will be changed to fc.

```
Do you want to continue? {y|n}: y
```

Any changes will take effect after rebooting the system. Use the "system node reboot" command to reboot.

```
net-f8040-34::> reboot local
(system node reboot)
```

```
Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y
```

##### 5. Verificare di avere installato il modulo SFP+ corretto:

```
network fcp adapter show -instance -node -adapter
```

Per CNA, è necessario utilizzare un SFP Ethernet da 10 GB. Per FC, è necessario utilizzare un SFP da 8 GB o un SFP da 16 GB, prima di modificare la configurazione sul nodo.

### Sostituire i moduli ottici dell'adattatore target CNA/UTA2

È necessario modificare i moduli ottici sull'adattatore di destinazione unificato (CNA/UTA2) per supportare la modalità di personalità selezionata per l'adattatore.

#### Fasi

1. Verificare l'SFP+ corrente utilizzato nella scheda. Quindi, sostituire il modulo SFP+ corrente con il modulo SFP+ appropriato per il linguaggio preferito (FC o CNA).
2. Rimuovere i moduli ottici correnti dall'adattatore X1143A-R6.
3. Inserire i moduli corretti per l'ottica della modalità Personality (FC o CNA) preferita.

4. Verificare di avere installato il modulo SFP+ corretto:

```
network fcp adapter show -instance -node -adapter
```

I moduli SFP+ supportati e i cavi in rame (Twinax) con marchio Cisco sono elencati nella ["NetApp Hardware Universe"](#).

## Visualizzare le impostazioni dell'adattatore

Per visualizzare le impostazioni dell'adattatore di destinazione unificato (X1143A-R6), è necessario eseguire `system hardware unified-connect show` comando per visualizzare tutti i moduli sul controller.

### Fasi

1. Avviare il controller senza i cavi collegati.
2. Eseguire `system hardware unified-connect show` per visualizzare la configurazione delle porte e i moduli.
3. Visualizzare le informazioni sulla porta prima di configurare il CNA e le porte.

## Configurazioni FCoE

### Panoramica su come configurare FCoE

FCoE può essere configurato in vari modi utilizzando gli switch FCoE. Le configurazioni `direct-attached` non sono supportate in FCoE.

Tutte le configurazioni FCoE sono `dual-fabric`, completamente ridondanti e richiedono software di multipathing lato host. In tutte le configurazioni FCoE, è possibile disporre di più switch FCoE e FC nel percorso tra l'iniziatore e la destinazione, fino al limite massimo del numero di hop. Per collegare gli switch tra loro, è necessario che gli switch eseguano una versione del firmware che supporti gli ISL Ethernet. Ogni host in qualsiasi configurazione FCoE può essere configurato con un sistema operativo diverso.

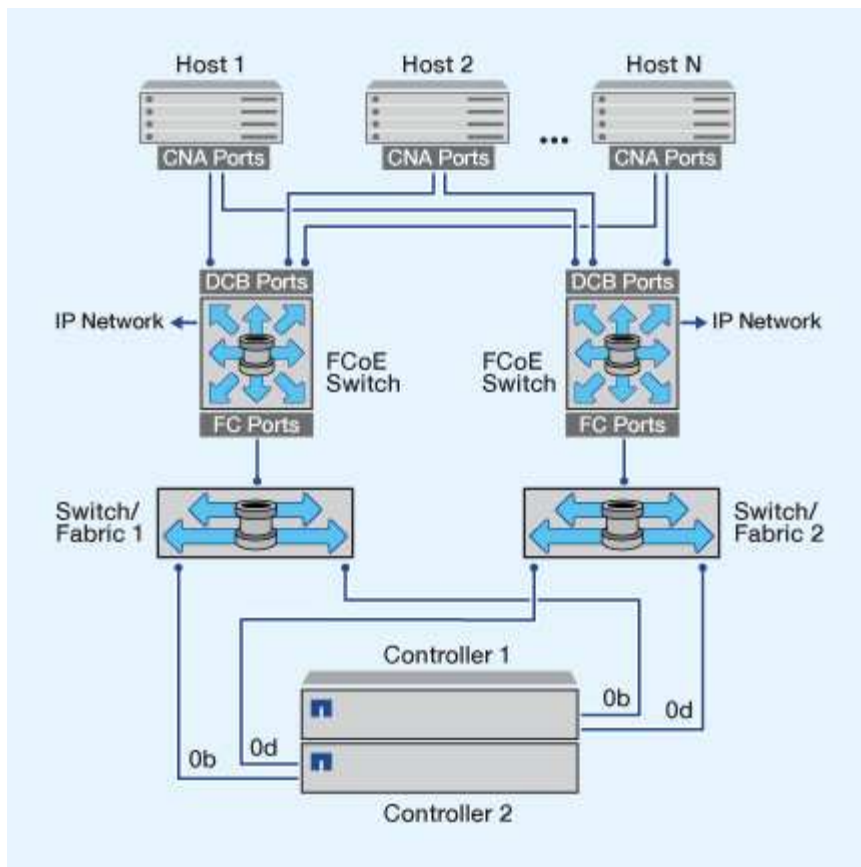
Le configurazioni FCoE richiedono switch Ethernet che supportano esplicitamente le funzionalità FCoE. Le configurazioni FCoE vengono validate attraverso lo stesso processo di interoperabilità e di garanzia della qualità degli switch FC. Le configurazioni supportate sono elencate nella matrice di interoperabilità. Alcuni dei parametri inclusi in queste configurazioni supportate sono il modello di switch, il numero di switch implementabili in un singolo fabric e la versione del firmware dello switch supportata.

I numeri delle porte dell'adattatore di espansione FC target nelle illustrazioni sono esempi. I numeri effettivi delle porte possono variare a seconda degli slot di espansione in cui sono installati gli adattatori di espansione di destinazione FCoE.

### Iniziatore FCoE su destinazione FC

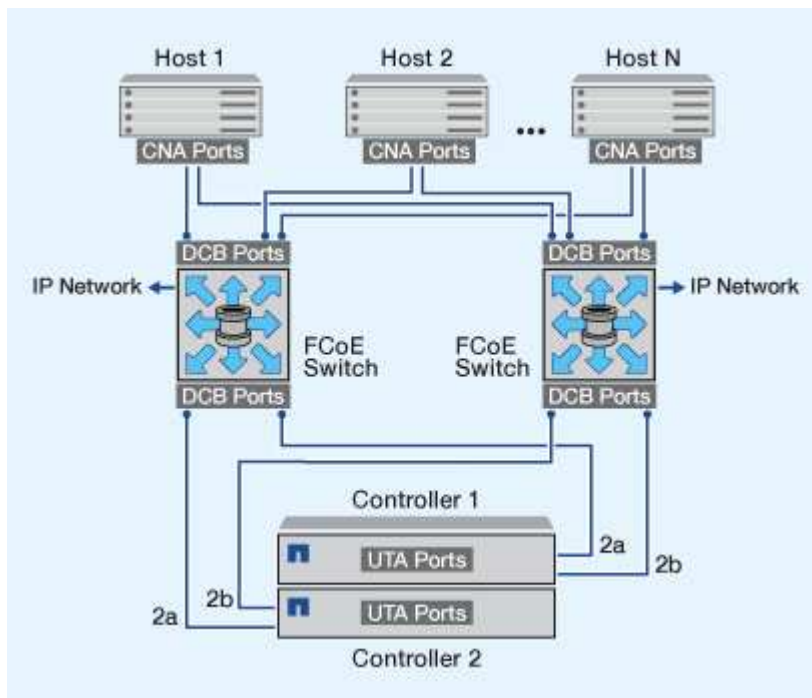
Utilizzando gli iniziatori FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha attraverso gli switch FCoE alle porte di destinazione FC. Lo switch FCoE deve anche disporre di porte FC. L'iniziatore FCoE host si connette sempre allo switch FCoE. Lo switch FCoE può connettersi direttamente alla destinazione FC o alla destinazione FC tramite switch FC.

La figura seguente mostra i CNA host che si collegano a uno switch FCoE e quindi a uno switch FC prima di connettersi alla coppia ha:



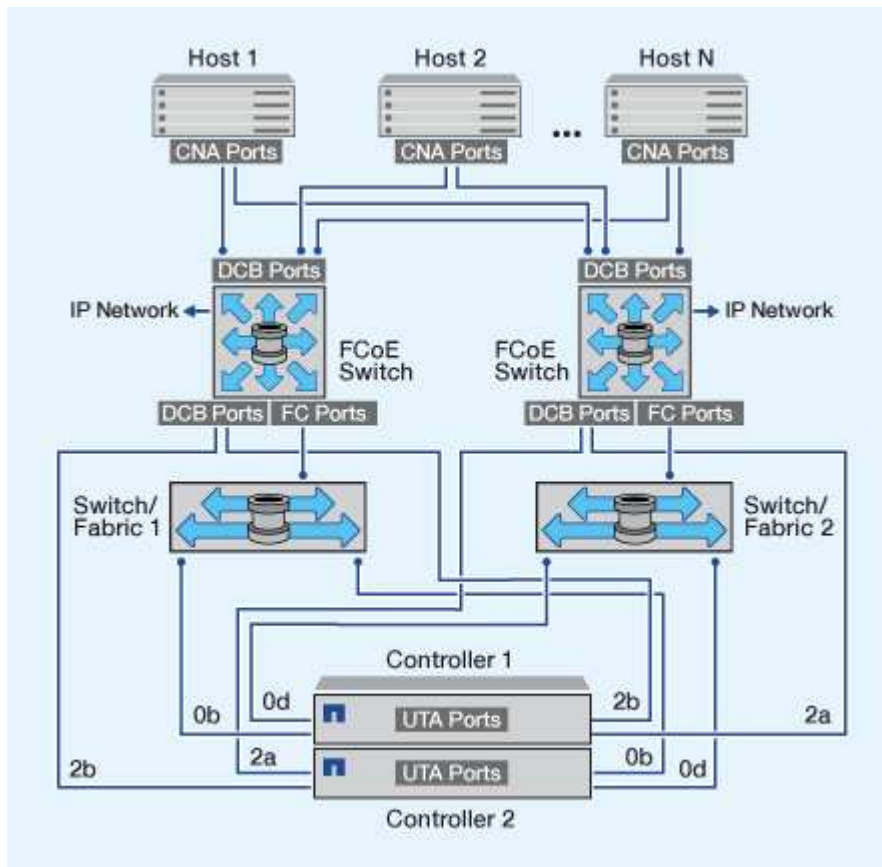
#### Iniziatore FCoE alla destinazione FCoE

Utilizzando gli iniziatori host FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha alle porte di destinazione FCoE (chiamate anche UTAS o UTA2s) attraverso gli switch FCoE.



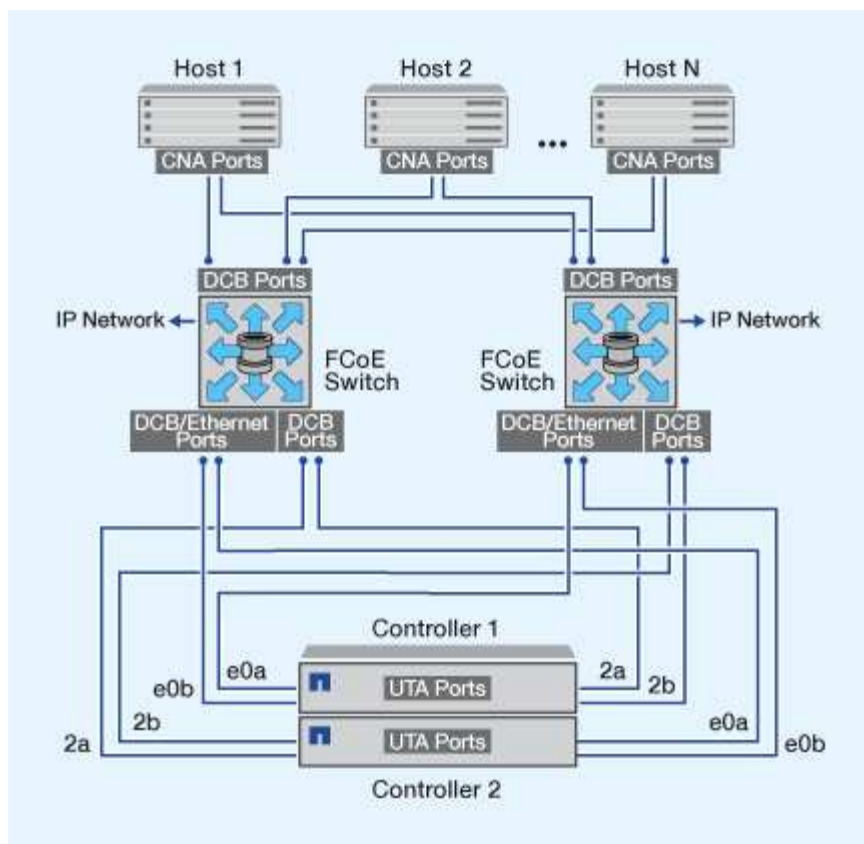
### Iniziatore FCoE per destinazioni FCoE e FC

Utilizzando gli iniziatori host FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha alle porte di destinazione FCoE e FC (chiamate anche UTAS o UTA2s) attraverso gli switch FCoE.



### FCoE combinato con i protocolli di storage IP

Utilizzando gli iniziatori host FCoE (CNA), è possibile collegare gli host a entrambi i controller in una coppia ha alle porte di destinazione FCoE (chiamate anche UTAS o UTA2s) attraverso gli switch FCoE. Le porte FCoE non possono utilizzare l'aggregazione di collegamenti tradizionale per un singolo switch. Gli switch Cisco supportano un tipo speciale di aggregazione di collegamenti (Virtual Port Channel) che supporta FCoE. Un Virtual Port Channel aggrega i singoli collegamenti a due switch. È inoltre possibile utilizzare Virtual Port Channels per altri tipi di traffico Ethernet. Le porte utilizzate per il traffico diverso da FCoE, tra cui NFS, SMB, iSCSI e altro traffico Ethernet, possono utilizzare le normali porte Ethernet degli switch FCoE.



## FCoE Initiator e combinazioni di destinazione

Sono supportate alcune combinazioni di FCoE e iniziatori e target FC tradizionali.

### Iniziatori FCoE

È possibile utilizzare gli iniziatori FCoE nei computer host con destinazioni FCoE e FC tradizionali nei controller di storage. L'iniziatore FCoE host deve connettersi a uno switch FCoE DCB (data center bridging); la connessione diretta a una destinazione non è supportata.

La tabella seguente elenca le combinazioni supportate:

Iniziatore	Destinazione	Supportato?
FC	FC	Sì
FC	FCoE	Sì
FCoE	FC	Sì
FCoE	FCoE	Sì

### Obiettivi FCoE

È possibile combinare porte di destinazione FCoE con porte FC da 4 GB, 8 GB o 16 GB sul controller di storage, indipendentemente dal fatto che le porte FC siano adattatori di destinazione aggiuntivi o porte integrate. È possibile avere sia FCoE che FC Target Adapter nello stesso controller di storage.





Le regole per la combinazione delle porte FC integrate e di espansione sono ancora valide.

## Numero di hop supportati da FCoE

Il numero massimo di hop Fibre Channel over Ethernet (FCoE) supportati tra un host e un sistema storage dipende dal fornitore dello switch e dal supporto del sistema storage per le configurazioni FCoE.

Il numero di hop viene definito come il numero di switch nel percorso tra l'iniziatore (host) e la destinazione (sistema di storage). La documentazione di Cisco Systems fa anche riferimento a questo valore come *diametro del fabric SAN*.

Per FCoE, è possibile collegare gli switch FCoE agli switch FC.

Per le connessioni FCoE end-to-end, gli switch FCoE devono eseguire una versione del firmware che supporti i collegamenti Ethernet tra switch (ISL).

La tabella seguente elenca i conteggi massimi di hop supportati:

Cambiare fornitore	Numero di hop supportato
Brocade	7 per FC 5 per FCoE
Cisco	7 Fino a 3 switch possono essere switch FCoE.

## Zoning FCoE e Fibre Channel

### Panoramica dello zoning FCoE e Fibre Channel

Una zona FC, FC-NVMe o FCoE è un raggruppamento logico di una o più porte all'interno di un fabric. Affinché i dispositivi possano vederti, connettersi, creare sessioni e comunicare tra loro, entrambe le porte devono avere un'appartenenza di zona comune. Si consiglia di utilizzare lo zoning Single Initiator.

### Motivi per lo zoning

- Lo zoning riduce o elimina *crosstalk* tra gli HBA iniziatori.

Ciò si verifica anche in ambienti di piccole dimensioni ed è uno degli argomenti migliori per l'implementazione dello zoning. I sottoinsiemi di fabric logici creati con lo zoning eliminano i problemi di crosstalk.

- Lo zoning riduce il numero di percorsi disponibili per una determinata porta FC, FC-NVMe o FCoE e riduce il numero di percorsi tra un host e una particolare LUN visibili.

Ad esempio, alcune soluzioni di multipathing del sistema operativo host hanno un limite al numero di percorsi che possono gestire. Lo zoning può ridurre il numero di percorsi che un driver multipathing del

sistema operativo vede. Se un host non dispone di una soluzione multipathing installata, è necessario verificare che sia visibile un solo percorso a un LUN utilizzando lo zoning nel fabric o una combinazione di mappatura LUN selettiva (SLM) e portset in SVM.

- Lo zoning aumenta la sicurezza limitando l'accesso e la connettività agli end-point che condividono una zona comune.

Le porte che non hanno zone in comune non possono comunicare tra loro.

- Lo zoning migliora l'affidabilità DELLA SAN isolando i problemi che si verificano e aiuta a ridurre i tempi di risoluzione dei problemi limitando lo spazio dei problemi.

### Consigli per lo zoning

- È necessario implementare lo zoning in qualsiasi momento, se quattro o più host sono connessi a una SAN o se SLM non è implementato sui nodi di una SAN.
- Sebbene sia possibile utilizzare lo zoning dei nomi dei nodi in tutto il mondo con alcuni fornitori di switch, è necessario utilizzare lo zoning dei nomi delle porte in tutto il mondo per definire correttamente una porta specifica e utilizzare NPIV in modo efficace.
- È necessario limitare le dimensioni della zona mantenendo la gestibilità.

È possibile sovrapporre più zone per limitare le dimensioni. Idealmente, viene definita una zona per ciascun host o cluster di host.

- Utilizzare lo zoning a singolo iniziatore per eliminare il crosstalk tra gli HBA iniziatori.

### Zoning basato sul nome

La suddivisione in zone in base al nome globale (WWN) specifica il numero WWN dei membri da includere nella zona. Quando si esegue lo zoning in ONTAP, è necessario utilizzare la zoning del nome della porta universale (WWPN).

Lo zoning WWPN offre flessibilità perché l'accesso non è determinato dalla posizione in cui il dispositivo è fisicamente collegato al fabric. È possibile spostare un cavo da una porta all'altra senza riconfigurare le zone.

Per i percorsi Fibre Channel verso i controller di storage che eseguono ONTAP, assicurarsi che gli switch FC siano dotati di zone utilizzando le WWPN delle interfacce logiche di destinazione (LIF), non le WWPN delle porte fisiche sul nodo. Per ulteriori informazioni sulle schede LIF, consulta la *Guida alla gestione della rete ONTAP*.

### "Gestione della rete"

#### Singole zone

Nella configurazione di zoning consigliata, esiste un iniziatore host per zona. La zona è costituita dalla porta dell'iniziatore host e da una o più LIF di destinazione sui nodi di storage che forniscono l'accesso alle LUN fino al numero desiderato di percorsi per destinazione. Ciò significa che gli host che accedono agli stessi nodi non possono vedere le porte dell'altro, ma ogni iniziatore può accedere a qualsiasi nodo.

È necessario aggiungere tutti i LIF dalla macchina virtuale di storage (SVM) nella zona con l'iniziatore host. Ciò consente di spostare volumi o LUN senza modificare le zone esistenti o creare nuove zone.

Per i percorsi Fibre Channel ai nodi che eseguono ONTAP, assicurarsi che gli switch FC siano dotati di zone utilizzando le WWPN delle interfacce logiche di destinazione (LIF), non le WWPN delle porte fisiche sul nodo. Le WWPN delle porte fisiche iniziano con “50” e le WWPN delle LIF iniziano con “20”.

### Zoning a fabric singolo

In una configurazione a fabric singolo, è comunque possibile connettere ciascun iniziatore host a ciascun nodo di storage. Per gestire percorsi multipli, è necessario un software multipathing sull'host. Ogni host deve disporre di due iniziatori per il multipathing per fornire resilienza nella soluzione.

Ciascun iniziatore deve disporre di almeno una LIF da ciascun nodo a cui l'iniziatore può accedere. Lo zoning deve consentire almeno un percorso dall'iniziatore host alla coppia di nodi nel cluster per fornire un percorso per la connettività LUN. Ciò significa che ogni iniziatore sull'host potrebbe avere un solo LIF di destinazione per nodo nella configurazione di zona. Se è necessario eseguire il multipath sullo stesso nodo o su più nodi del cluster, ciascun nodo avrà più LIF per nodo nella configurazione della zona. In questo modo, l'host può comunque accedere ai propri LUN in caso di guasto di un nodo o di spostamento di un volume contenente il LUN in un nodo diverso. Ciò richiede inoltre che i nodi di reporting siano impostati in modo appropriato.

Le configurazioni a singolo fabric sono supportate, ma non sono considerate altamente disponibili. Il guasto di un singolo componente può causare la perdita di accesso ai dati.

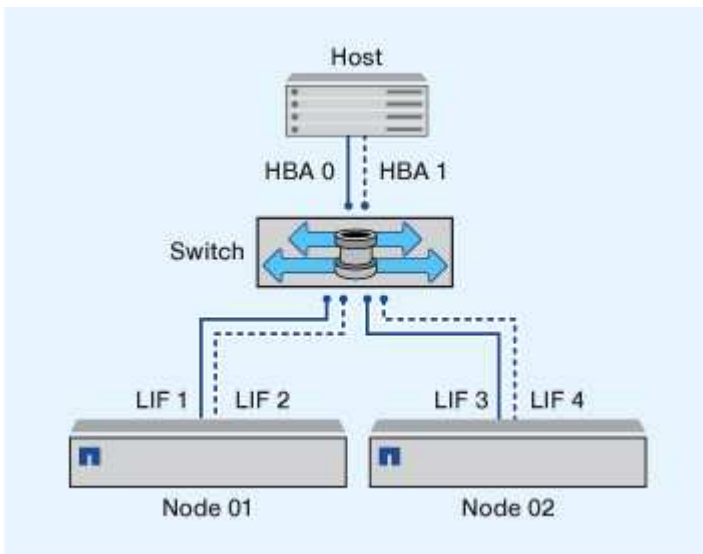
Nella figura seguente, l'host dispone di due iniziatori e sta eseguendo un software multipathing. Esistono due zone:



La convenzione di naming utilizzata in questa figura è solo una raccomandazione di una possibile convenzione di naming che è possibile scegliere di utilizzare per la soluzione ONTAP.

- Zona 1: HBA 0, LIF\_1 e LIF\_3
- Zona 2: HBA 1, LIF\_2 e LIF\_4

Se la configurazione includeva più nodi, le LIF per i nodi aggiuntivi sarebbero incluse in queste zone.



In questo esempio, è possibile avere tutte e quattro le LIF in ciascuna zona. In tal caso, le zone saranno le seguenti:

- Zona 1: HBA 0, LIF\_1, LIF\_2, LIF\_3 e LIF\_4
- Zona 2: HBA 1, LIF\_1, LIF\_2, LIF\_3 e LIF\_4



Il sistema operativo host e il software di multipathing devono supportare il numero di percorsi supportati utilizzati per accedere alle LUN sui nodi. Per determinare il numero di percorsi utilizzati per accedere alle LUN sui nodi, vedere la sezione limiti della configurazione SAN.

## Informazioni correlate

["NetApp Hardware Universe"](#)

## Zoning di coppia ha dual-fabric

Nelle configurazioni a doppio fabric, è possibile collegare ciascun iniziatore host a ciascun nodo del cluster. Ciascun iniziatore host utilizza uno switch diverso per accedere ai nodi del cluster. Per gestire percorsi multipli, è necessario un software multipathing sull'host.

Le configurazioni dual-fabric sono considerate ad alta disponibilità perché l'accesso ai dati viene mantenuto in caso di guasto di un singolo componente.

Nella figura seguente, l'host dispone di due iniziatori e sta eseguendo un software multipathing. Esistono due zone. SLM è configurato in modo che tutti i nodi siano considerati come nodi di reporting.



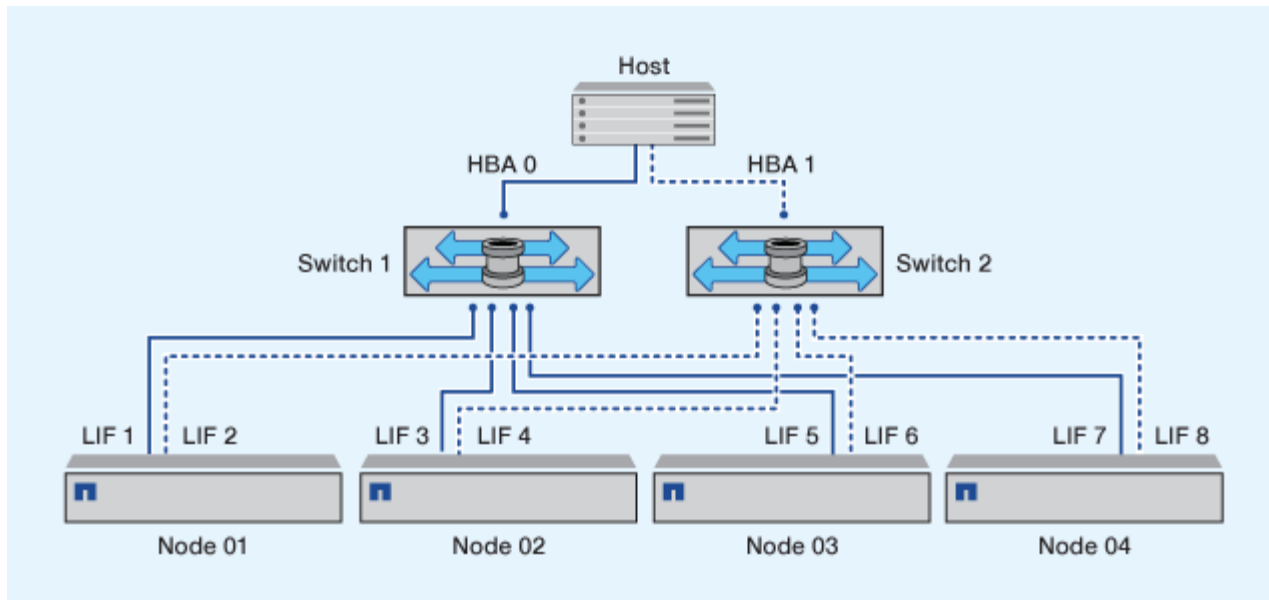
La convenzione di naming utilizzata in questa figura è solo una raccomandazione di una possibile convenzione di naming che è possibile scegliere di utilizzare per la soluzione ONTAP.

- Zona 1: HBA 0, LIF\_1, LIF\_3, LIF\_5 e LIF\_7
- Zona 2: HBA 1, LIF\_2, LIF\_4, LIF\_6 e LIF\_8

Ogni iniziatore host viene associato a zone attraverso uno switch differente. L'accesso alla zona 1 avviene tramite l'interruttore 1. L'accesso alla zona 2 avviene tramite l'interruttore 2.

Ciascun iniziatore può accedere a una LIF su ogni nodo. In questo modo, l'host può continuare ad accedere ai propri LUN in caso di guasto di un nodo. Le SVM hanno accesso a tutte le LIF iSCSI e FC su ogni nodo di una soluzione in cluster in base all'impostazione della mappa LUN selettiva (SLM) e alla configurazione del nodo di reporting. È possibile utilizzare lo zoning di SLM, portset o switch FC per ridurre il numero di percorsi da una SVM all'host e il numero di percorsi da una SVM a una LUN.

Se la configurazione includeva più nodi, le LIF per i nodi aggiuntivi sarebbero incluse in queste zone.



Il sistema operativo host e il software di multipathing devono supportare il numero di percorsi utilizzati per accedere alle LUN sui nodi.

#### Informazioni correlate

["NetApp Hardware Universe"](#)

#### Restrizioni di zoning per switch Cisco FC e FCoE

Quando si utilizzano switch Cisco FC e FCoE, una singola zona fabric non deve contenere più LIF di destinazione per la stessa porta fisica. Se più LIF sulla stessa porta si trovano nella stessa zona, le porte LIF potrebbero non riuscire a ripristinarsi a causa di una perdita di connessione.

I normali switch FC vengono utilizzati per il protocollo FC-NVMe esattamente come per il protocollo FC.

- Più LIF per i protocolli FC e FCoE possono condividere porte fisiche su un nodo purché si trovino in zone diverse.
- FC-NVMe e FCoE non possono condividere la stessa porta fisica.
- FC e FC-NVMe possono condividere la stessa porta fisica da 32 GB.
- Gli switch Cisco FC e FCoE richiedono che ogni LIF su una determinata porta si trova in una zona separata dalle altre LIF su tale porta.
- Una singola zona può avere LIF FC e FCoE. Una zona può contenere una LIF da ogni porta di destinazione nel cluster, ma fare attenzione a non superare i limiti di percorso dell'host e verificare la configurazione SLM.
- Le LIF su diverse porte fisiche possono trovarsi nella stessa zona.
- Gli switch Cisco richiedono la separazione delle LIF.

Sebbene non sia necessario, si consiglia di separare i LIF per tutti gli switch

## Requisiti per le configurazioni SAN condivise

Le configurazioni SAN condivise sono definite come host collegati sia ai sistemi storage ONTAP che ai sistemi storage di altri vendor. L'accesso ai sistemi storage ONTAP e ai sistemi storage di altri vendor da un singolo host è supportato purché vengano soddisfatti diversi requisiti.

Per tutti i sistemi operativi host, è consigliabile utilizzare adattatori separati per connettersi ai sistemi storage di ciascun vendor. L'utilizzo di adattatori separati riduce la possibilità di conflitti tra driver e impostazioni. Per le connessioni a un sistema storage ONTAP, il modello di adattatore, il BIOS, il firmware e il driver devono essere elencati come supportati nel tool matrice di interoperabilità NetApp.

È necessario impostare i valori di timeout richiesti o consigliati e altri parametri di storage per l'host. È sempre necessario installare il software NetApp o applicare le impostazioni NetApp per ultime.

- Per AIX, è necessario applicare i valori della versione delle utility host AIX elencata nello strumento matrice di interoperabilità per la configurazione.
- Per ESX, è necessario applicare le impostazioni host utilizzando Virtual Storage Console per VMware vSphere.
- Per HP-UX, utilizzare le impostazioni di storage predefinite di HP-UX.
- Per Linux, è necessario applicare i valori della versione di Linux host Utilities elencata nello strumento Interoperability Matrix per la configurazione.
- Per Solaris, è necessario applicare i valori della versione di Solaris host Utilities elencata nel tool Interoperability Matrix per la propria configurazione.
- Per Windows, è necessario installare la versione di Windows host Utilities elencata nello strumento Interoperability Matrix per la configurazione in uso.

### Informazioni correlate

["Tool di matrice di interoperabilità NetApp"](#)

## Configurazioni SAN in un ambiente MetroCluster

### Configurazioni SAN in un ambiente MetroCluster

Quando si utilizzano le configurazioni SAN in un ambiente MetroCluster, è necessario tenere presente alcune considerazioni.

- Le configurazioni MetroCluster non supportano le configurazioni vSAN del fabric FC front-end "Routed".
- A partire da ONTAP 9.12.1, le configurazioni IP MetroCluster a quattro nodi sono supportate su NVMe/FC. Le configurazioni MetroCluster non sono supportate su NVMe/TCP. Le configurazioni MetroCluster non sono supportate per NVMe precedenti a ONTAP 9.12.1.
- Altri protocolli SAN come iSCSI, FC e FCoE sono supportati nelle configurazioni MetroCluster.
- Quando si utilizzano configurazioni client SAN, è necessario verificare se eventuali considerazioni speciali per le configurazioni MetroCluster sono incluse nelle note fornite in ["Tool di matrice di interoperabilità NetApp"](#) (IMT).
- I sistemi operativi e le applicazioni devono fornire una resilienza i/o di 120 secondi per supportare lo switchover automatico non pianificato di MetroCluster e lo switchover con interruttore a leva o avviato da un mediatore.

- MetroCluster utilizza le stesse WWPN su entrambi i lati DELLA SAN front-end.

#### Informazioni correlate

- ["Comprensione della protezione dei dati e del disaster recovery di MetroCluster"](#)
- ["Articolo della Knowledge base: Quali sono le considerazioni sul supporto dell'host AIX in una configurazione MetroCluster?"](#)
- ["Articolo della Knowledge base: Considerazioni sul supporto degli host Solaris in una configurazione MetroCluster"](#)

#### Impedire la sovrapposizione delle porte tra switchover e switchback

In un ambiente SAN, è possibile configurare gli switch front-end in modo da evitare sovrapposizioni quando la vecchia porta passa offline e la nuova porta entra in linea.

Durante lo switchover, la porta FC del sito sopravvissuto potrebbe accedere al fabric prima che il fabric abbia rilevato che la porta FC del sito di emergenza non è in linea e abbia rimosso questa porta dai servizi di nome e directory.

Se la porta FC del disastro non viene ancora rimossa, il tentativo di accesso fabric della porta FC nel sito sopravvissuto potrebbe essere rifiutato a causa di un WWPN duplicato. Questo comportamento degli switch FC può essere modificato per rispettare l'accesso del dispositivo precedente e non quello esistente. Verificare gli effetti di questo comportamento su altri dispositivi fabric. Per ulteriori informazioni, contattare il fornitore dello switch.

Scegliere la procedura corretta in base al tipo di switch.

## Esempio 14. Fasi

### Switch Cisco

1. Connettersi allo switch ed effettuare l'accesso.
2. Accedere alla modalità di configurazione:

```
switch# config t  
switch(config)#
```

3. Sovrascrivere la prima voce di dispositivo nel database del server dei nomi con la nuova periferica:

```
switch(config)# no fcns reject-duplicate-pwvn vsan 1
```

4. Negli switch che eseguono NX-OS 8.x, verificare che il timeout di quiesce flogi sia impostato su zero:

- a. Visualizzare il timer di quiesce:

```
switch(config)# show flogi interval info \ i quiesce
```

```
Stats:  fs flogi quiesce timerval:  0
```

- b. Se l'output del passo precedente non indica che il timerval è zero, impostarlo su zero:

```
switch(config)# flogi scale enable
```

```
switch(config)$ flogi quiesce timeout 0
```

### Switch Brocade

1. Connettersi allo switch ed effettuare l'accesso.
2. Inserire il switchDisable comando.
3. Inserire il configure e premere y quando richiesto.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Scegliere l'impostazione 1:

```
- 0: First login take precedence over the second login (default)  
- 1: Second login overrides first login.  
- 2: the port type determines the behavior  
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Rispondere alle richieste rimanenti oppure premere **Ctrl + D**.



6. Inserire il `switchEnable` comando.

#### Informazioni correlate

["Esecuzione di uno switchover per test o manutenzione"](#)

## Supporto host per multipathing

### Panoramica sul supporto host per multipathing

ONTAP utilizza sempre ALUA (Asymmetric Logical Unit Access) per i percorsi FC e iSCSI. Assicurarsi di utilizzare configurazioni host che supportino ALUA per i protocolli FC e iSCSI.

A partire da ONTAP 9.5 multipath ha Pair failover/giveback è supportato per le configurazioni NVMe che utilizzano l'accesso asincrono allo spazio dei nomi (ANA). In ONTAP 9.4, NVMe supporta un solo percorso da host a destinazione. L'host dell'applicazione deve gestire il failover del percorso verso il proprio partner ad alta disponibilità (ha).

Per informazioni su quali configurazioni host specifiche supportano ALUA o ANA, consultare ["Tool di matrice di interoperabilità NetApp"](#) e ["Configurazione host SAN ONTAP"](#) per il sistema operativo host.

### Quando è richiesto un software host multipathing

Se è presente più di un percorso tra le interfacce logiche (LIF) delle macchine virtuali di storage e il fabric, è necessario un software di multipathing. Il software multipathing è necessario sull'host ogni volta che l'host può accedere a un LUN attraverso più di un percorso.

Il software di multipathing presenta un singolo disco al sistema operativo per tutti i percorsi verso una LUN. Senza un software di multipathing, il sistema operativo potrebbe trattare ciascun percorso come un disco separato, con conseguente danneggiamento dei dati.

La soluzione è considerata avere più percorsi se si dispone di uno dei seguenti elementi:

- Una singola porta iniziatore nell'host che si collega a più LIF SAN nella SVM
- Più porte initiator collegate a una singola LIF SAN nella SVM
- Più porte initiator collegate a più LIF SAN nella SVM

Il software multipathing è consigliato nelle configurazioni ha. Oltre alla mappatura LUN selettiva, si consiglia di utilizzare lo zoning o i portset dello switch FC per limitare i percorsi utilizzati per accedere alle LUN.

Il software multipathing è noto anche come software MPIO (multipath i/o).

### Numero consigliato di percorsi da host a nodi nel cluster

Non superare più di otto percorsi dall'host a ciascun nodo del cluster, prestando attenzione al numero totale di percorsi che è possibile supportare per il sistema operativo host e al multipathing utilizzato sull'host.

È necessario disporre di almeno due percorsi per LUN che si connettono a ciascun nodo di reporting tramite la

mappa LUN selettiva (SLM) utilizzata dalla macchina virtuale di storage (SVM) nel cluster. In questo modo si eliminano i singoli punti di errore e si consente al sistema di sopravvivere ai guasti dei componenti.

Se nel cluster sono presenti quattro o più nodi o più di quattro porte di destinazione utilizzate dalle SVM in uno dei nodi, È possibile utilizzare i seguenti metodi per limitare il numero di percorsi che è possibile utilizzare per accedere alle LUN sui nodi in modo da non superare il numero massimo consigliato di otto percorsi.

- SLM

SLM riduce il numero di percorsi dall'host al LUN solo nei percorsi sul nodo proprietario del LUN e del partner ha del nodo proprietario. SLM è attivato per impostazione predefinita.

- Portset per iSCSI
- Mappature FC igroup dall'host
- Zoning dello switch FC

#### Informazioni correlate

["Amministrazione SAN"](#)

## Limiti di configurazione

### Determinare il numero di nodi supportati per le configurazioni SAN

Il numero di nodi per cluster supportati da ONTAP varia a seconda della versione di ONTAP, dei modelli di controller di storage nel cluster e del protocollo dei nodi del cluster.

#### A proposito di questa attività

Se un nodo del cluster è configurato per FC, FC-NVMe, FCoE o iSCSI, tale cluster è limitato ai limiti dei nodi SAN. I limiti dei nodi in base ai controller del cluster sono elencati nel *Hardware Universe*.

#### Fasi

1. Passare a ["NetApp Hardware Universe"](#).
2. Fare clic su **Platforms** in alto a sinistra (accanto al pulsante **Home**) e selezionare il tipo di piattaforma.
3. Selezionare la casella di controllo accanto alla versione di ONTAP in uso.

Viene visualizzata una nuova colonna per la scelta delle piattaforme.

4. Selezionare le caselle di controllo accanto alle piattaforme utilizzate nella soluzione.
5. Deselezionare la casella di controllo **Seleziona tutto** nella colonna **Scegli specifiche**.
6. Selezionare la casella di controllo **Max Nodes per Cluster (NAS/SAN)**.
7. Fare clic su **Mostra risultati**.

#### Informazioni correlate

["NetApp Hardware Universe"](#)

### Determinare il numero di host supportati per cluster nelle configurazioni FC e FC-NVMe

Il numero massimo di host SAN che possono essere connessi a un cluster varia notevolmente in base alla combinazione specifica di più attributi del cluster, ad esempio il

numero di host connessi a ciascun nodo del cluster, gli iniziatori per host, le sessioni per host e i nodi nel cluster.

#### **A proposito di questa attività**

Per le configurazioni FC e FC-NVMe, è necessario utilizzare il numero di ITN (Initiator-Target Nexuses) nel sistema per determinare se è possibile aggiungere altri host al cluster.

Un ITN rappresenta un percorso dall'iniziatore dell'host alla destinazione del sistema di storage. Il numero massimo di ITN per nodo nelle configurazioni FC e FC-NVMe è 2,048. Se si è al di sotto del numero massimo di ITN, è possibile continuare ad aggiungere host al cluster.

Per determinare il numero di ITN utilizzati nel cluster, attenersi alla seguente procedura per ciascun nodo del cluster.

#### **Fasi**

1. Identificare tutte le LIF su un nodo specifico.
2. Eseguire il seguente comando per ogni LIF sul nodo:

```
fcip initiator show -fields wwpn, lif
```

Il numero di voci visualizzate nella parte inferiore dell'output del comando rappresenta il numero di ITN per la LIF.

3. Registrare il numero di ITN visualizzati per ciascun LIF.
4. Aggiungere il numero di ITN per ogni LIF su ogni nodo del cluster.

Questo totale rappresenta il numero di ITN nel cluster.

#### **Determinare il numero di host supportati nelle configurazioni iSCSI**

Il numero massimo di host SAN che possono essere connessi nelle configurazioni iSCSI varia notevolmente in base alla combinazione specifica di più attributi del cluster, come il numero di host connessi a ciascun nodo del cluster, gli iniziatori per host, gli accessi per host e i nodi nel cluster.

#### **A proposito di questa attività**

Il numero di host che è possibile collegare direttamente a un nodo o tramite uno o più switch dipende dal numero di porte Ethernet disponibili. Il numero di porte Ethernet disponibili dipende dal modello del controller e dal numero e dal tipo di adattatori installati nel controller. Il numero di porte Ethernet supportate per controller e adattatori è disponibile in *Hardware Universe*.

Per tutte le configurazioni di cluster a più nodi, è necessario determinare il numero di sessioni iSCSI per nodo per sapere se è possibile aggiungere altri host al cluster. Se il cluster è al di sotto del numero massimo di sessioni iSCSI per nodo, è possibile continuare ad aggiungere host al cluster. Il numero massimo di sessioni iSCSI per nodo varia in base ai tipi di controller nel cluster.

#### **Fasi**

1. Identificare tutti i gruppi di portali di destinazione sul nodo.
2. Controllare il numero di sessioni iSCSI per ogni gruppo di portali di destinazione sul nodo:

```
iscsi session show -tpgroup tpgroup
```

Il numero di voci visualizzate nella parte inferiore dell'output del comando rappresenta il numero di sessioni iSCSI per il gruppo di portali di destinazione.

3. Registrare il numero di sessioni iSCSI visualizzate per ciascun gruppo di portali di destinazione.
4. Aggiungere il numero di sessioni iSCSI per ciascun gruppo di portali di destinazione sul nodo.

Il totale rappresenta il numero di sessioni iSCSI sul nodo.

## **Limiti di configurazione dello switch FC**

Gli switch Fibre Channel hanno limiti di configurazione massimi, incluso il numero di accessi supportati per porta, gruppo di porte, blade e switch. I vendor di switch documentano i propri limiti supportati.

Ogni interfaccia logica FC (LIF) accede a una porta dello switch FC. Il numero totale di accessi da una singola destinazione sul nodo equivale al numero di LIF più un accesso per la porta fisica sottostante. Non superare i limiti di configurazione del vendor dello switch per gli accessi o altri valori di configurazione. Ciò vale anche per gli iniziatori utilizzati sul lato host in ambienti virtualizzati con NPIV attivato. Non superare i limiti di configurazione del vendor dello switch per gli accessi per la destinazione o per gli iniziatori utilizzati nella soluzione.

### **Limiti dello switch Brocade**

I limiti di configurazione per gli switch Brocade sono indicati nelle *linee guida sulla scalabilità Brocade*.

### **Limiti degli switch Cisco Systems**

I limiti di configurazione per gli switch Cisco sono disponibili in "[Limiti di configurazione Cisco](#)" Guida alla versione del software dello switch Cisco in uso.

## **Panoramica della profondità della coda di calcolo**

Potrebbe essere necessario regolare la profondità della coda FC sull'host per ottenere i valori massimi per ITN per nodo e fan-in della porta FC. Il numero massimo di LUN e il numero di HBA che possono connettersi a una porta FC sono limitati dalla profondità di coda disponibile sulle porte di destinazione FC.

### **A proposito di questa attività**

Queue Depth (profondità coda) è il numero di richieste i/o (comandi SCSI) che possono essere accodate contemporaneamente su un controller di storage. Ogni richiesta di i/o dall'HBA iniziatore dell'host all'adattatore di destinazione del controller di storage consuma una voce di coda. In genere, una maggiore profondità della coda equivale a prestazioni migliori. Tuttavia, se viene raggiunta la profondità massima della coda del controller di storage, il controller di storage rifiuta i comandi in entrata restituendo una risposta QFULL. Se un gran numero di host accede a un controller di storage, è necessario pianificare attentamente per evitare le condizioni QFULL, che degradano significativamente le prestazioni del sistema e possono causare errori su alcuni sistemi.

In una configurazione con più iniziatori (host), tutti gli host devono avere profondità di coda simili. A causa della disuguaglianza nella profondità della coda tra gli host connessi allo storage controller attraverso la stessa porta di destinazione, gli host con profondità di coda inferiori vengono privati dell'accesso alle risorse da parte degli host con profondità di coda maggiori.

È possibile fornire i seguenti consigli generali sulle profondità della coda “tuning”:

- Per i sistemi di piccole e medie dimensioni, utilizzare una profondità di coda HBA di 32.
- Per i sistemi di grandi dimensioni, utilizzare una profondità della coda HBA pari a 128.
- In caso di eccezioni o di test delle prestazioni, utilizzare una profondità della coda di 256 per evitare possibili problemi di accodamento.
- Tutti gli host devono avere le profondità della coda impostate su valori simili per garantire un accesso uguale a tutti gli host.
- Per evitare errori o penalizzazioni delle performance, non superare la profondità della coda della porta FC di destinazione del controller di storage.

## Fasi

1. Contare il numero totale di iniziatori FC in tutti gli host che si connettono a una porta di destinazione FC.
2. Moltiplicare per 128.
  - Se il risultato è inferiore a 2,048, impostare la profondità della coda per tutti gli iniziatori su 128. Si dispone di 15 host con un iniziatore connesso a ciascuna delle due porte di destinazione sul controller di storage.  $15 \times 128 = 1,920$ . Poiché 1,920 è inferiore al limite di profondità totale della coda di 2,048, è possibile impostare la profondità della coda per tutti gli iniziatori su 128.
  - Se il risultato è superiore a 2,048, passare alla fase 3. Si dispone di 30 host con un iniziatore connesso a ciascuna delle due porte di destinazione sul controller di storage.  $30 \times 128 = 3,840$ . Poiché 3,840 è maggiore del limite di profondità totale della coda di 2,048, è necessario scegliere una delle opzioni indicate al punto 3 per la risoluzione dei problemi.
3. Scegliere una delle seguenti opzioni per aggiungere altri host al controller dello storage.
  - Opzione 1:
    - i. Aggiungere altre porte di destinazione FC.
    - ii. Ridistribuire gli iniziatori FC.
  - iii. Ripetere i passaggi 1 e 2. + la profondità di coda desiderata di 3,840 supera la profondità di coda disponibile per porta. Per risolvere questo problema, è possibile aggiungere un adattatore di destinazione FC a due porte a ciascun controller, quindi eseguire la zona degli switch FC in modo che 15 host su 30 si connettano a un set di porte e gli altri 15 host si connettano a un secondo set di porte. La profondità della coda per porta viene quindi ridotta a  $15 \times 128 = 1,920$ .
  - Opzione 2:
    - i. Indicare ciascun host come “Large” o “sMall” in base alle esigenze di i/o previste.
    - ii. Moltiplicare il numero di iniziatori grandi per 128.
    - iii. Moltiplicare il numero di piccoli iniziatori per 32.
    - iv. Unire i due risultati.
    - v. Se il risultato è inferiore a 2,048, impostare la profondità della coda per gli host di grandi dimensioni su 128 e la profondità della coda per gli host di piccole dimensioni su 32.
    - vi. Se il risultato è ancora maggiore di 2,048 per porta, ridurre la profondità della coda per iniziatore fino a quando la profondità totale della coda non è inferiore o uguale a 2,048.



Per stimare la profondità della coda necessaria per ottenere un determinato throughput i/o al secondo, utilizzare questa formula:

Profondità della coda richiesta = (numero di i/o al secondo) × (tempo di risposta)

Ad esempio, se si necessita di 40,000 i/o al secondo con un tempo di risposta di 3 millisecondi, la profondità della coda richiesta =  $40,000 \times (.003) = 120$ .

Il numero massimo di host che è possibile collegare a una porta di destinazione è 64, se si decide di limitare la profondità della coda alla raccomandazione di base di 32. Tuttavia, se si decide di avere una profondità di coda di 128, è possibile collegare un massimo di 16 host a una porta di destinazione. Maggiore è la profondità della coda, minore è il numero di host supportati da una singola porta di destinazione. Se il tuo requisito è tale da non poter scendere a compromessi sulla profondità della coda, dovresti ottenere più porte di destinazione.

La profondità della coda desiderata di 3,840 supera la profondità della coda disponibile per porta. Sono disponibili 10 host “Large” con esigenze di i/o dello storage elevate e 20 host “sMall” con esigenze di i/o ridotte. Impostare la profondità della coda dell’iniziatore sugli host di grandi dimensioni su 128 e la profondità della coda dell’iniziatore sugli host di piccole dimensioni su 32.

La profondità totale della coda risultante è  $(10 \times 128) + (20 \times 32) = 1,920$ .

È possibile distribuire la profondità della coda disponibile in modo uniforme in ciascun iniziatore.

La profondità della coda risultante per iniziatore è di  $2,048 \div 30 = 68$ .

### Impostare le profondità delle code sugli host SAN

Potrebbe essere necessario modificare le profondità della coda sull’host per ottenere i valori massimi per ITN per nodo e fan-in della porta FC.

#### Host AIX

È possibile modificare la profondità della coda sugli host AIX utilizzando `chdev` comando. Modifiche apportate utilizzando `chdev` il comando persiste durante i riavvii.

Esempi:

- Per modificare la profondità della coda per il dispositivo `hdisk7`, utilizzare il seguente comando:

```
chdev -l hdisk7 -a queue_depth=32
```

- Per modificare la profondità della coda per l’HBA `fcs0`, utilizzare il seguente comando:

```
chdev -l fcs0 -a num_cmd_elems=128
```

Il valore predefinito per `num_cmd_elems` è 200. Il valore massimo è 2,048.



Potrebbe essere necessario portare l’HBA offline per modificarlo `num_cmd_elems` e poi riportarlo online utilizzando `rmdev -l fcs0 -R e.makdev -l fcs0 -P` comandi.

## Host HP-UX

È possibile modificare la profondità della coda LUN o periferica sugli host HP-UX utilizzando il parametro `kernel scsi_max_qdepth`. È possibile modificare la profondità della coda HBA utilizzando il parametro `kernel max_fcp_reqs`.

- Il valore predefinito per `scsi_max_qdepth` è 8. Il valore massimo è 255.

`scsi_max_qdepth` può essere modificato dinamicamente su un sistema in esecuzione utilizzando `-u` sul `kmtune` comando. La modifica sarà effettiva per tutti i dispositivi del sistema. Ad esempio, utilizzare il seguente comando per aumentare la profondità della coda LUN a 64:

```
kmtune -u -s scsi_max_qdepth=64
```

È possibile modificare la profondità della coda per i singoli file del dispositivo utilizzando `scsictl` comando. Modifiche tramite `scsictl` i comandi non sono persistenti durante i riavvii del sistema. Per visualizzare e modificare la profondità della coda per un determinato file di dispositivo, eseguire il seguente comando:

```
scsictl -a /dev/rdisk/c2t2d0
```

```
scsictl -m queue_depth=16 /dev/rdisk/c2t2d0
```

- Il valore predefinito per `max_fcp_reqs` è 512. Il valore massimo è 1024.

Il kernel deve essere ricostruito e il sistema deve essere riavviato per apportare modifiche a `max_fcp_reqs` per avere effetto. Per impostare la profondità della coda HBA su 256, ad esempio, utilizzare il seguente comando:

```
kmtune -u -s max_fcp_reqs=256
```

## Host Solaris

È possibile impostare la profondità della coda LUN e HBA per gli host Solaris.

- Per la profondità della coda LUN: Il numero di LUN in uso su un host moltiplicato per l'accelerazione per LUN (`lun-queue-depth`) deve essere inferiore o uguale al valore `tgt-queue-depth` sull'host.
- Per la profondità della coda in uno stack Sun: I driver nativi non consentono per LUN o per destinazione `max_throttle` Impostazioni a livello di HBA. Metodo consigliato per l'impostazione di `max_throttle` Il valore per i driver nativi si trova a livello di tipo per dispositivo (`VID_PID`) in `/kernel/drv/sd.conf` e `/kernel/drv/ssd.conf` file. L'utilità `host` imposta questo valore su 64 per le configurazioni MPIxIO e 8 per le configurazioni Veritas DMP.

## Fasi

1. # `cd/kernel/drv`
2. # `vi lpfc.conf`
3. Cercare `/tft-queue (/tgt-queue)`

```
tgt-queue-depth=32
```



Il valore predefinito viene impostato su 32 al momento dell'installazione.

4. Impostare il valore desiderato in base alla configurazione dell'ambiente.
5. Salvare il file.
6. Riavviare l'host utilizzando `sync; sync; sync; reboot -- -r` comando.

### VMware ospita un HBA QLogic

Utilizzare `esxcfg-module` Per modificare le impostazioni di timeout dell'HBA. Aggiornamento manuale di `esx.conf` file sconsigliato.

#### Fasi

1. Accedere alla console di servizio come utente root.
2. Utilizzare `#vmkload_mod -l` Comando per verificare quale modulo Qlogic HBA è attualmente caricato.
3. Per una singola istanza di un HBA Qlogic, eseguire il seguente comando:

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```



In questo esempio viene utilizzato il modulo `qla2300_707`. Utilizzare il modulo appropriato in base all'output di `vmkload_mod -l`.

4. Salvare le modifiche utilizzando il seguente comando:

```
#!/usr/sbin/esxcfg-boot -b
```

5. Riavviare il server utilizzando il seguente comando:

```
#reboot
```

6. Confermare le modifiche utilizzando i seguenti comandi:

- a. `#esxcfg-module -g qla2300_707`
- b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

### VMware ospita un HBA Emulex

Utilizzare `esxcfg-module` Per modificare le impostazioni di timeout dell'HBA. Aggiornamento manuale di `esx.conf` file sconsigliato.

#### Fasi

1. Accedere alla console di servizio come utente root.
2. Utilizzare `#vmkload_mod -l grep lpfc` Comando per verificare quale HBA Emulex è attualmente caricato.
3. Per una singola istanza di un HBA Emulex, immettere il seguente comando:

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```



A seconda del modello dell'HBA, il modulo può essere `lpfcdd_7xx` o `lpfcdd_732`. Il comando precedente utilizza il modulo `lpfcdd_7xx`. Utilizzare il modulo appropriato in base al risultato di `vmkload_mod -l`.



L'esecuzione di questo comando imposta la profondità della coda LUN su 16 per l'HBA rappresentato da lpfc0.

4. Per istanze multiple di un HBA Emulex, eseguire il seguente comando:

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

La profondità della coda LUN per lpfc0 e la profondità della coda LUN per lpfc1 è impostata su 16.

5. Immettere il seguente comando:

```
#esxcfg-boot -b
```

6. Riavviare utilizzando #reboot.

### Host Windows per un HBA Emulex

Sugli host Windows, è possibile utilizzare LPUTILNT Utility per aggiornare la profondità della coda per gli HBA Emulex.

#### Fasi

1. Eseguire LPUTILNT utility disponibile in C:\WINNT\system32 directory.
2. Selezionare **Drive Parameters** (parametri unità) dal menu a destra.
3. Scorrere verso il basso e fare doppio clic su **QueueDepth**.



Se si imposta **QueueDepth** maggiore di 150, è necessario aumentare in modo appropriato anche il seguente valore del Registro di sistema di Windows:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests
```

### Host Windows per un HBA Qlogic

Sugli host Windows, è possibile utilizzare il e il SANsurfer Utility di gestione HBA per aggiornare le profondità delle code per gli HBA Qlogic.

#### Fasi

1. Eseguire SANsurfer Utility HBA Manager.
2. Fare clic su **porta HBA > Impostazioni**.
3. Fare clic su **Advanced HBA port settings** (Impostazioni avanzate porta HBA) nella casella di riepilogo.
4. Aggiornare Execution Throttle parametro.

### Host Linux per HBA Emulex

È possibile aggiornare le profondità della coda di un HBA Emulex su un host Linux. Per rendere gli aggiornamenti persistenti durante i riavvii, è necessario creare una nuova immagine del disco RAM e riavviare l'host.

#### Fasi

1. Identificare i parametri di profondità della coda da modificare:

```
modinfo lpfc|grep queue_depth
```

Viene visualizzato l'elenco dei parametri di profondità della coda con la relativa descrizione. A seconda della versione del sistema operativo in uso, è possibile modificare uno o più dei seguenti parametri di profondità della coda:

- ° `lpfc_lun_queue_depth`: Numero massimo di comandi FC che è possibile mettere in coda a un LUN specifico (uint)
- ° `lpfc_hba_queue_depth`: Numero massimo di comandi FC che è possibile mettere in coda a un HBA `lpfc` (uint)
- ° `lpfc_tgt_queue_depth`: Numero massimo di comandi FC che è possibile mettere in coda a una specifica porta di destinazione (uint)

Il `lpfc_tgt_queue_depth` Il parametro è valido solo per i sistemi Red Hat Enterprise Linux 7.x, SUSE Linux Enterprise Server 11 SP4 e 12.x.

2. Aggiornare le profondità della coda aggiungendo i parametri di profondità della coda a `/etc/modprobe.conf` File per un sistema Red Hat Enterprise Linux 5.x e per `/etc/modprobe.d/scsi.conf` File per un sistema Red Hat Enterprise Linux 6.x o 7.x o un sistema SUSE Linux Enterprise Server 11.x o 12.x.

A seconda della versione del sistema operativo in uso, è possibile aggiungere uno o più dei seguenti comandi:

- ° `options lpfc lpfc_hba_queue_depth=new_queue_depth`
- ° `options lpfc lpfc_lun_queue_depth=new_queue_depth`
- ° `options lpfc tgt_queue_depth=new_queue_depth`

3. Creare una nuova immagine del disco RAM, quindi riavviare l'host per rendere gli aggiornamenti persistenti durante i riavvii.

Per ulteriori informazioni, consultare ["Amministrazione del sistema"](#) Per la versione del sistema operativo Linux in uso.

4. Verificare che i valori di profondità della coda siano aggiornati per ciascun parametro di profondità della coda modificato:

```
root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
30
```

Viene visualizzato il valore corrente della profondità della coda.

## Host Linux per QLogic HBA

È possibile aggiornare la profondità della coda dei dispositivi di un driver QLogic su un host Linux. Per rendere gli aggiornamenti persistenti durante i riavvii, è necessario creare una nuova immagine del disco RAM e riavviare l'host. È possibile utilizzare la GUI di gestione dell'HBA QLogic o l'interfaccia della riga di comando (CLI) per modificare la profondità della coda dell'HBA QLogic.

Questa attività mostra come utilizzare la CLI QLogic HBA per modificare la profondità della coda QLogic HBA

## Fasi

1. Identificare il parametro Device queue depth da modificare:

```
modinfo qla2xxx | grep ql2xmaxqdepth
```

È possibile modificare solo il ql2xmaxqdepth Queue depth, che indica la profondità massima della coda che può essere impostata per ogni LUN. Il valore predefinito è 64 per RHEL 7.5 e versioni successive. Il valore predefinito è 32 per RHEL 7.4 e versioni precedenti.

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:          ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. Aggiornare il valore di profondità della coda della periferica:

- Se si desidera rendere persistenti le modifiche, attenersi alla seguente procedura:
  - i. Aggiornare le profondità della coda aggiungendo il parametro queue depth al /etc/modprobe.conf File per un sistema Red Hat Enterprise Linux 5.x e per /etc/modprobe.d/scsi.conf File per un sistema Red Hat Enterprise Linux 6.x o 7.x o per un sistema SUSE Linux Enterprise Server 11.x o 12.x: options qla2xxx ql2xmaxqdepth=new\_queue\_depth
  - ii. Creare una nuova immagine del disco RAM, quindi riavviare l'host per rendere gli aggiornamenti persistenti durante i riavvii.

Per ulteriori informazioni, consultare ["Amministrazione del sistema"](#) Per la versione del sistema operativo Linux in uso.

- Se si desidera modificare il parametro solo per la sessione corrente, eseguire il seguente comando:

```
echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Nell'esempio seguente, la profondità della coda è impostata su 128.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Verificare che i valori di profondità della coda siano aggiornati:

```
cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Viene visualizzato il valore corrente della profondità della coda.

4. Modificare la profondità della coda QLogic HBA aggiornando il parametro del firmware Execution Throttle Dal BIOS QLogic HBA.

- a. Accedere alla CLI di gestione dell'HBA QLogic:

```
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
```

b. Dal menu principale, selezionare Adapter Configuration opzione.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

          CLI - Version 2.2.0 (Build 15)

Main Menu

1:  Adapter Information
**2: Adapter Configuration**
3:  Adapter Updates
4:  Adapter Diagnostics
5:  Monitoring
6:  FabricCache CLI
7:  Refresh
8:  Help
9:  Exit

Please Enter Selection: 2
```

c. Dall'elenco dei parametri di configurazione dell'adattatore, selezionare HBA Parameters opzione.

```
1:  Adapter Alias
2:  Adapter Port Alias
**3: HBA Parameters**
4:  Persistent Names (udev)
5:  Boot Devices Configuration
6:  Virtual Ports (NPIV)
7:  Target Link Speed (iidMA)
8:  Export (Save) Configuration
9:  Generate Reports
10: Personality
11: FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 3
```

d. Dall'elenco delle porte HBA, selezionare la porta HBA richiesta.

#### Fibre Channel Adapter Configuration

HBA Model QLE2562 SN: BFD1524C78510

1: Port 1: WWPN: 21-00-00-24-FF-8D-98-E0 Online

2: Port 2: WWPN: 21-00-00-24-FF-8D-98-E1 Online

HBA Model QLE2672 SN: RFE1241G81915

3: Port 1: WWPN: 21-00-00-0E-1E-09-B7-62 Online

4: Port 2: WWPN: 21-00-00-0E-1E-09-B7-63 Online

(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)

Please Enter Selection: 1

Vengono visualizzati i dettagli della porta HBA.

e. Dal menu HBA Parameters (parametri HBA), selezionare Display HBA Parameters per visualizzare il valore corrente di Execution Throttle opzione.

Il valore predefinito di Execution Throttle l'opzione è 65535.

#### HBA Parameters Menu

```
=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02
WWPN         : 21-00-00-24-FF-8D-98-E0
WWNN         : 20-00-00-24-FF-8D-98-E0
Link         : Online
=====
```

- 1: Display HBA Parameters
- 2: Configure HBA Parameters
- 3: Restore Defaults

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)

Please Enter Selection: 1

```
-----
-----
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-07-00
```

Link: Online

```
-----
Connection Options           : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                    : Auto
Frame Size                   : 2048
Hard Loop ID                 : 0
Loop Reset Delay (seconds)   : 5
Enable Host HBA BIOS         : Enabled
Enable Hard Loop ID          : Disabled
Enable FC Tape Support       : Enabled
Operation Mode               : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us) : 0
**Execution Throttle         : 65535**
Login Retry Count            : 8
Port Down Retry Count        : 30
Enable LIP Full Login        : Enabled
Link Down Timeout (seconds)  : 30
Enable Target Reset          : Enabled
LUNs Per Target              : 128
Out Of Order Frame Assembly  : Disabled
Enable LR Ext. Credits       : Disabled
Enable Fabric Assigned WWN   : N/A
```

Press <Enter> to continue:

- a. Premere **Invio** per continuare.
- b. Dal menu HBA Parameters (parametri HBA), selezionare Configure HBA Parameters Opzione per modificare i parametri HBA.
- c. Dal menu Configure Parameters (Configura parametri), selezionare Execute Throttle e aggiornare il valore di questo parametro.

## Configure Parameters Menu

```
=====
HBA          : 2 Port: 1
SN           : BFD1524C78510
HBA Model    : QLE2562
HBA Desc.    : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version   : 8.01.02
WWPN         : 21-00-00-24-FF-8D-98-E0
WWNN         : 20-00-00-24-FF-8D-98-E0
Link         : Online
=====
```

- 1: Connection Options
- 2: Data Rate
- 3: Frame Size
- 4: Enable HBA Hard Loop ID
- 5: Hard Loop ID
- 6: Loop Reset Delay (seconds)
- 7: Enable BIOS
- 8: Enable Fibre Channel Tape Support
- 9: Operation Mode
- 10: Interrupt Delay Timer (100 microseconds)
- 11: Execution Throttle
- 12: Login Retry Count
- 13: Port Down Retry Count
- 14: Enable LIP Full Login
- 15: Link Down Timeout (seconds)
- 16: Enable Target Reset
- 17: LUNs per Target
- 18: Enable Receive Out Of Order Frame
- 19: Enable LR Ext. Credits
- 20: Commit Changes
- 21: Abort Changes

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)

Please Enter Selection: 11

Enter Execution Throttle [1-65535] [65535]: 65500

d. Premere **Invio** per continuare.

e. Dal menu Configure Parameters (Configura parametri), selezionare Commit Changes opzione per salvare le modifiche.

f. Uscire dal menu.

# Gestione dello storage a oggetti S3

## Scopri il supporto S3 in ONTAP 9

### Panoramica della configurazione S3

A partire da ONTAP 9.8, è possibile attivare un server di storage a oggetti S3 (Simple Storage Service) di ONTAP in un cluster ONTAP.

ONTAP supporta due scenari di casi d'utilizzo on-premise per il servizio dello storage a oggetti S3:

- Tier FabricPool per un bucket su cluster locale (Tier to a local bucket) o cluster remoto (Tier cloud).
- Accesso dell'applicazione client S3 a un bucket sul cluster locale o su un cluster remoto.

A partire da ONTAP 9.14.1, è possibile abilitare un server per lo storage a oggetti S3 su una SVM in un aggregato con mirroring o senza mirror nelle configurazioni IP e FC di MetroCluster.

A partire da ONTAP 9.12.1, è possibile abilitare un server di storage a oggetti S3 su una SVM in un aggregato senza mirror in una configurazione IP MetroCluster. Per ulteriori informazioni sulle limitazioni degli aggregati senza mirror nelle configurazioni MetroCluster IP, vedere ["Considerazioni per gli aggregati senza mirror"](#).

Utilizzare queste procedure se si desidera configurare lo storage a oggetti S3 nel modo seguente:

- Si desidera fornire lo storage a oggetti S3 da un cluster esistente che esegue ONTAP.

ONTAP S3 è adatto per le funzionalità S3 sui cluster esistenti senza hardware e gestione aggiuntivi. Tuttavia, il software NetApp StorageGRID continua a essere la soluzione NetApp di punta per lo storage a oggetti. Per ulteriori informazioni, consultare ["Documentazione StorageGRID"](#).

- Si dispone di privilegi di amministratore del cluster, non di amministratore SVM.

### Configurazione S3 con Gestore di sistema e CLI ONTAP

È possibile configurare e gestire ONTAP S3 con Gestore di sistema e l'interfaccia utente di ONTAP. Quando si attiva S3 e si creano bucket utilizzando Gestione sistema, ONTAP seleziona le impostazioni predefinite delle Best practice per una configurazione semplificata. Se è necessario specificare i parametri di configurazione, è possibile utilizzare l'interfaccia utente di ONTAP. Se si configurano il server S3 e i bucket dalla CLI, è comunque possibile gestirli con System Manager, se lo si desidera, o viceversa.

Quando si crea un bucket S3 utilizzando Gestione di sistema, ONTAP configura un livello di servizio delle performance predefinito il più alto disponibile sul sistema. Ad esempio, su un sistema AFF, l'impostazione predefinita è **estrema**. I livelli di servizio delle performance sono gruppi di criteri QoS (Quality of Service) adattivi predefiniti. Invece di uno dei livelli di servizio predefiniti, è possibile specificare un gruppo di criteri QoS personalizzato o nessun gruppo di criteri.

I gruppi di policy QoS adattivi predefiniti sono:

- **Extreme:** Utilizzato per le applicazioni che si aspettano la latenza più bassa e le performance più elevate.
- **Performance:** Utilizzato per applicazioni con esigenze di performance e latenza modeste.
- **Valore:** Utilizzato per applicazioni per le quali throughput e capacità sono più importanti della latenza.
- **Custom:** Specificare un criterio QoS personalizzato o nessun criterio QoS.



Se si seleziona **Use for Tiering** (Usa per il tiering), non viene selezionato alcun livello di servizio delle performance e il sistema tenta di selezionare supporti a basso costo con performance ottimali per i dati a più livelli.

Vedere anche: ["Utilizzare gruppi di policy QoS adattivi"](#).

ONTAP tenta di eseguire il provisioning di questo bucket su Tier locali che dispongono dei dischi più appropriati, soddisfacendo il livello di servizio scelto. Tuttavia, se è necessario specificare quali dischi includere nel bucket, è consigliabile configurare lo storage a oggetti S3 dalla CLI specificando i Tier locali (aggregato). Se si configura il server S3 dalla CLI, è comunque possibile gestirlo con System Manager, se necessario.

Se si desidera specificare gli aggregati da utilizzare per i bucket, è possibile farlo solo utilizzando la CLI.

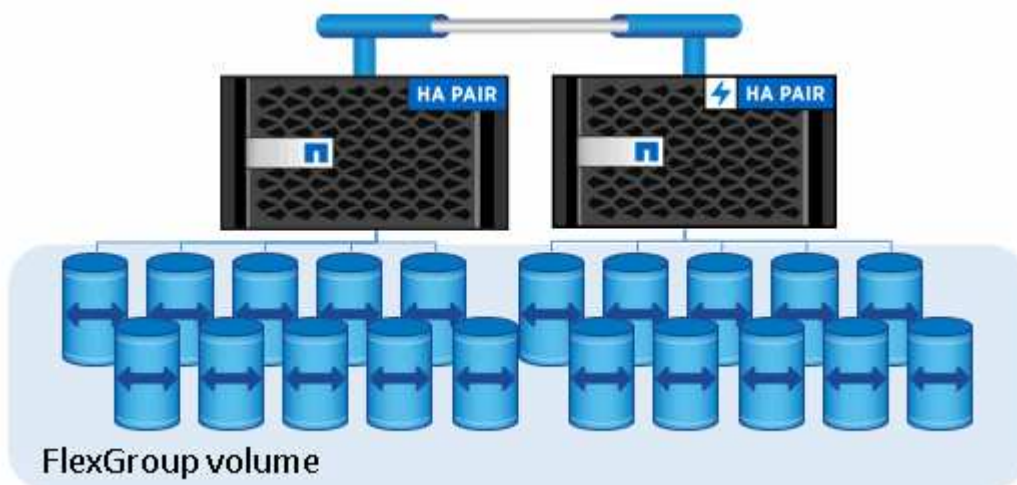
### Configurazione dei bucket S3 su Cloud Volumes ONTAP

Se si desidera utilizzare i bucket di Cloud Volumes ONTAP, si consiglia di selezionare manualmente gli aggregati sottostanti per assicurarsi che utilizzino un solo nodo. L'utilizzo di aggregati di entrambi i nodi può influire sulle performance, poiché i nodi si trovano in zone di disponibilità separate geograficamente e quindi suscettibili a problemi di latenza. Pertanto, negli ambienti Cloud Volumes ONTAP, è necessario [Configurare i bucket S3 dalla CLI](#).

In caso contrario, i server S3 su Cloud Volumes ONTAP vengono configurati e mantenuti allo stesso modo in Cloud Volumes ONTAP come negli ambienti on-premise.

## Architettura

In ONTAP, l'architettura sottostante per un bucket è un volume FlexGroup, ovvero un singolo namespace costituito da più volumi membri costituenti, ma gestito come un singolo volume.

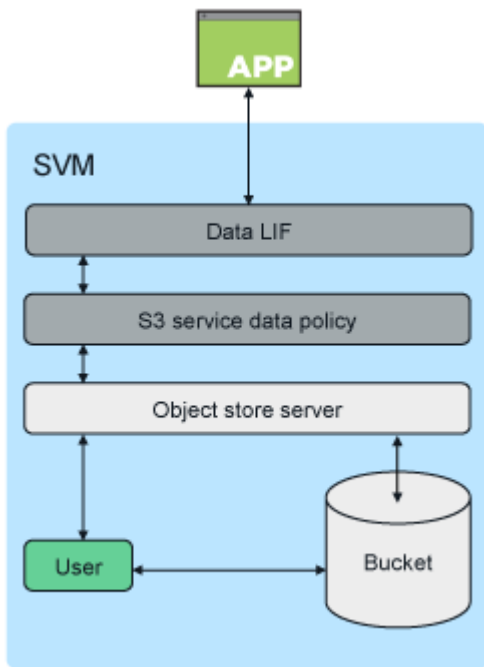


I bucket sono limitati solo dai massimi fisici dell'hardware sottostante e i massimi architetturici potrebbero essere più elevati. I bucket possono sfruttare il dimensionamento elastico di FlexGroup per far crescere automaticamente un componente di un volume FlexGroup se lo spazio è esaurito. Esiste un limite di 1000 bucket per volume FlexGroup o di 1/3 della capacità del volume FlexGroup (per tenere conto della crescita dei dati nei bucket).



Non è consentito l'accesso al protocollo NAS o SAN al volume FlexGroup che contiene bucket S3.

L'accesso al bucket viene fornito tramite utenti autorizzati e applicazioni client.



## Casi di utilizzo

Esistono tre casi di utilizzo principali per l'accesso client ai servizi ONTAP S3:

- Per i sistemi ONTAP che utilizzano ONTAP S3 come Tier di capacità FabricPool remota (cloud)

Il server S3 e il bucket contenente il Tier di capacità (per *cold* dati) si trovano su un cluster diverso dal Tier di performance (per *hot* dati).

- Per i sistemi ONTAP che utilizzano ONTAP S3 come Tier FabricPool locale

Il server S3 e il bucket contenente il Tier di capacità si trovano sullo stesso cluster, ma su una coppia ha diversa, come il Tier di performance.

- Per applicazioni client S3 esterne

ONTAP S3 serve applicazioni client S3 eseguite su sistemi non NetApp.

È consigliabile fornire l'accesso ai bucket ONTAP S3 utilizzando HTTPS. Quando HTTPS è attivato, i certificati di sicurezza sono necessari per la corretta integrazione con SSL/TLS. Gli utenti client' devono quindi autenticare l'utente con ONTAP S3 e autorizzare le autorizzazioni di accesso degli utenti' per le operazioni in ONTAP S3. L'applicazione client deve anche avere accesso al certificato CA principale (certificato firmato dal server ONTAP S3) per poter autenticare il server e creare una connessione sicura tra client e server.

Gli utenti vengono creati all'interno della SVM abilitata per S3 e le relative autorizzazioni di accesso possono essere controllate a livello di bucket o SVM, ovvero possono avere accesso a uno o più bucket all'interno della SVM.

HTTPS è attivato per impostazione predefinita sui server ONTAP S3. È possibile disattivare HTTPS e attivare HTTP per l'accesso al client, nel qual caso non è richiesta l'autenticazione mediante certificati CA. Tuttavia, quando HTTP è attivato e HTTPS è disattivato, tutte le comunicazioni con il server ONTAP S3 vengono inviate

sulla rete in testo non crittografato.

Per ulteriori informazioni, vedere ["Report tecnico: Le Best practice S3 in ONTAP"](#)

#### Informazioni correlate

["Gestione dei volumi FlexGroup"](#)

## Pianificare

### Supporto della versione di ONTAP per lo storage a oggetti S3

ONTAP supporta lo storage a oggetti S3 per ambienti on-premise a partire da ONTAP 9.8. Cloud Volumes ONTAP supporta lo storage a oggetti S3 per ambienti cloud a partire da ONTAP 9.9.1.

#### Supporto S3 con Cloud Volumes ONTAP

ONTAP S3 è configurato e funziona allo stesso modo in Cloud Volumes ONTAP come negli ambienti on-premise, con un'eccezione:

- Gli aggregati sottostanti devono provenire da un solo nodo. Scopri di più ["Creazione di bucket in ambienti CVO"](#).

Provider di cloud	Versione di ONTAP
Azure	ONTAP 9.9.1 e versioni successive
AWS	ONTAP 9.11.0 e versioni successive
Google Cloud	ONTAP 9.12.1 e versioni successive

#### Anteprima pubblica S3 in ONTAP 9.7

In ONTAP 9.7, lo storage a oggetti S3 è stato introdotto come anteprima pubblica. Tale versione non era destinata agli ambienti di produzione e non sarà più aggiornata a partire da ONTAP 9.8. Solo ONTAP 9.8 e versioni successive supportano lo storage a oggetti S3 negli ambienti di produzione.

I bucket S3 creati con l'anteprima pubblica 9.7 possono essere utilizzati in ONTAP 9.8 e versioni successive, ma non possono sfruttare i miglioramenti delle funzionalità. Se si dispone di bucket creati con l'anteprima pubblica 9.7, è necessario migrare il contenuto di tali bucket in 9.8 bucket per il supporto delle funzionalità, la sicurezza e i miglioramenti delle performance.

### Azioni supportate da ONTAP S3

Le azioni di ONTAP S3 sono supportate dalle API REST S3 standard, ad eccezione di quanto indicato di seguito. Per ulteriori informazioni, vedere ["Riferimento API Amazon S3"](#).

#### Operazioni della benna

In ONTAP sono supportate le seguenti operazioni utilizzando le API AWS S3:

Funzionamento della benna	Supporto ONTAP a partire da
CreateBucket	ONTAP 9.11.1
DeleteBucket	ONTAP 9.11.1
DeleteBucketPolicy	ONTAP 9.12.1
GetBucketAcl	ONTAP 9.8
GetBucketLifecycleConfiguration	ONTAP 9.13.1 + * sono supportate solo le azioni di scadenza
GetBucketLocation	ONTAP 9.10.1
GetBucketPolicy	ONTAP 9.12.1
HeadBucket	ONTAP 9.8
ListBucket	ONTAP 9.8
ListBucketVersioning	ONTAP 9.11.1
ListObjectVersions	ONTAP 9.11.1
PutBucket	<ul style="list-style-type: none"> <li>• ONTAP 9.11.1</li> <li>• ONTAP 9,8: Supportato solo con API REST ONTAP</li> </ul>
PutBucketLifecycleConfiguration	ONTAP 9.13.1 + * sono supportate solo le azioni di scadenza
PutBucketPolicy	ONTAP 9.12.1

## Operazioni a oggetti

A partire da ONTAP 9.9.1, ONTAP S3 supporta metadati e tagging degli oggetti.

- PutObject e CreateMultipartUpload includono coppie chiave-valore utilizzando `x-amz-meta-<key>`.

Ad esempio: `x-amz-meta-project: ontap_s3`.

- GetObject. E HeadObject restituiscono metadati definiti dall'utente.
- A differenza dei metadati, i tag possono essere letti indipendentemente dagli oggetti utilizzando:
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

A partire da ONTAP 9.11.1, ONTAP S3 supporta il controllo della versione degli oggetti e le azioni associate a queste API ONTAP:

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

<b>Operazione a oggetti</b>	<b>Supporto ONTAP a partire da</b>
AbortMultipartUpload	ONTAP 9.8
CompleteMultipartUpload	ONTAP 9.8
Oggetto CopyObject	ONTAP 9.12.1
CreateMultipartUpload	ONTAP 9.8
DeleteObject (Elimina oggetto)	ONTAP 9.8
DeleteObjects	ONTAP 9.11.1
DeleteObjectTagging	ONTAP 9.9.1
GetBucketVersioning	ONTAP 9.11.1
GetObject	ONTAP 9.8
GetObjectAcl	ONTAP 9.8
GetObjectRetention	ONTAP 9.14.1
GetObjectTagging	ONTAP 9.9.1
HeadObject (oggetto intestazione)	ONTAP 9.8
ListMultipartUpload	ONTAP 9.8
ListObjects (oggetti elenco)	ONTAP 9.8
ListObjectsV2	ONTAP 9.8
ListBucketVersions	ONTAP 9.11.1
ListParts	ONTAP 9.8
PutBucketVersioning	ONTAP 9.11.1
PutObject	ONTAP 9.8
PutObjectLockConfiguration	ONTAP 9.14.1
PutObjectRetention	ONTAP 9.14.1
PutObjectTagging	ONTAP 9.9.1
UploadPart	ONTAP 9.8
UploadPartCopy	ONTAP 9.12.1

## **Policy di gruppo**

Queste operazioni non sono specifiche di S3 e sono generalmente associate ai processi di identità e gestione (IAM). ONTAP supporta questi comandi ma non utilizza le API REST IAM.

- Crea policy
- Policy AttachGroup

## **Gestione degli utenti**

Queste operazioni non sono specifiche di S3 e sono generalmente associate ai processi IAM.

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

## Interoperabilità di ONTAP S3

Il server ONTAP S3 interagisce normalmente con altre funzionalità di ONTAP, ad eccezione di quanto indicato in questa tabella.

Area delle funzioni	Supportato	Non supportato
Cloud Volumes ONTAP	<ul style="list-style-type: none"> <li>• Client Azure in ONTAP 9.9.1 e versioni successive</li> <li>• Client AWS in ONTAP 9.11.0 e versioni successive</li> <li>• Client Google Cloud in ONTAP 9.12.1 e versioni successive</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud Volumes ONTAP per qualsiasi client in ONTAP 9.8 e versioni precedenti</li> </ul>
Protezione dei dati	<ul style="list-style-type: none"> <li>• Cloud Sync</li> <li>• <a href="#">"Versione degli oggetti"</a> (A partire da ONTAP 9.11.1)</li> <li>• <a href="#">"S3 SnapMirror"</a> (A partire da ONTAP 9.10.1)</li> <li>• Configurazioni IP MetroCluster (a partire da ONTAP 9.12.1)</li> <li>• SnapLock (a partire da ONTAP 9.14.1)</li> <li>• WORM (a partire da ONTAP 9.14.1)</li> </ul>	<ul style="list-style-type: none"> <li>• Erasure coding</li> <li>• Gestione del ciclo di vita delle informazioni</li> <li>• NDMP</li> <li>• SMTape</li> <li>• SnapMirror Cloud</li> <li>• Disaster recovery SVM</li> <li>• SyncMirror</li> <li>• Copie Snapshot create dall'utente</li> </ul>
Crittografia	<ul style="list-style-type: none"> <li>• NetApp aggregate Encryption (NAE)</li> <li>• NetApp Volume Encryption (NVE)</li> <li>• NetApp Storage Encryption (NSE)</li> <li>• TLS/SSL</li> </ul>	<ul style="list-style-type: none"> <li>• SCORIE</li> </ul>
Efficienza dello storage	<ul style="list-style-type: none"> <li>• Deduplica</li> <li>• Compressione</li> <li>• Compattazione</li> </ul>	<ul style="list-style-type: none"> <li>• Efficienze a livello di aggregato</li> <li>• Clone di volume del volume FlexGroup contenente i bucket ONTAP S3</li> </ul>
Virtualizzazione dello storage	-	Virtualizzazione NetApp FlexArray

Area delle funzioni	Supportato	Non supportato
Qualità del servizio (QoS)	<ul style="list-style-type: none"> <li>• QoS massimi (limiti)</li> <li>• QoS minimi (piani)</li> </ul>	-
Funzionalità aggiuntive	<ul style="list-style-type: none"> <li>• <a href="#">"Controllare gli eventi S3"</a> (A partire da ONTAP 9.10.1)</li> </ul>	<ul style="list-style-type: none"> <li>• Volumi FlexCache</li> <li>• FPolicy</li> <li>• Qtree</li> <li>• Quote</li> </ul>

## Soluzioni di terze parti validate da ONTAP S3

NetApp ha validato le seguenti soluzioni di terze parti per l'utilizzo con ONTAP S3. Se la soluzione che stai cercando non è presente nell'elenco, contatta il tuo rappresentante commerciale NetApp.

### Soluzioni di terze parti validate su ONTAP S3

NetApp ha testato queste soluzioni in collaborazione con i rispettivi partner.

- Amazon SageMaker
- Client Apache Hadoop S3A
- Apache Kafka
- CommVault (V11)
- Kafka confluyente
- Red Hat Quay
- Rubrik
- Fiocco di neve
- Trino
- Veeam (V12)

## Configurare

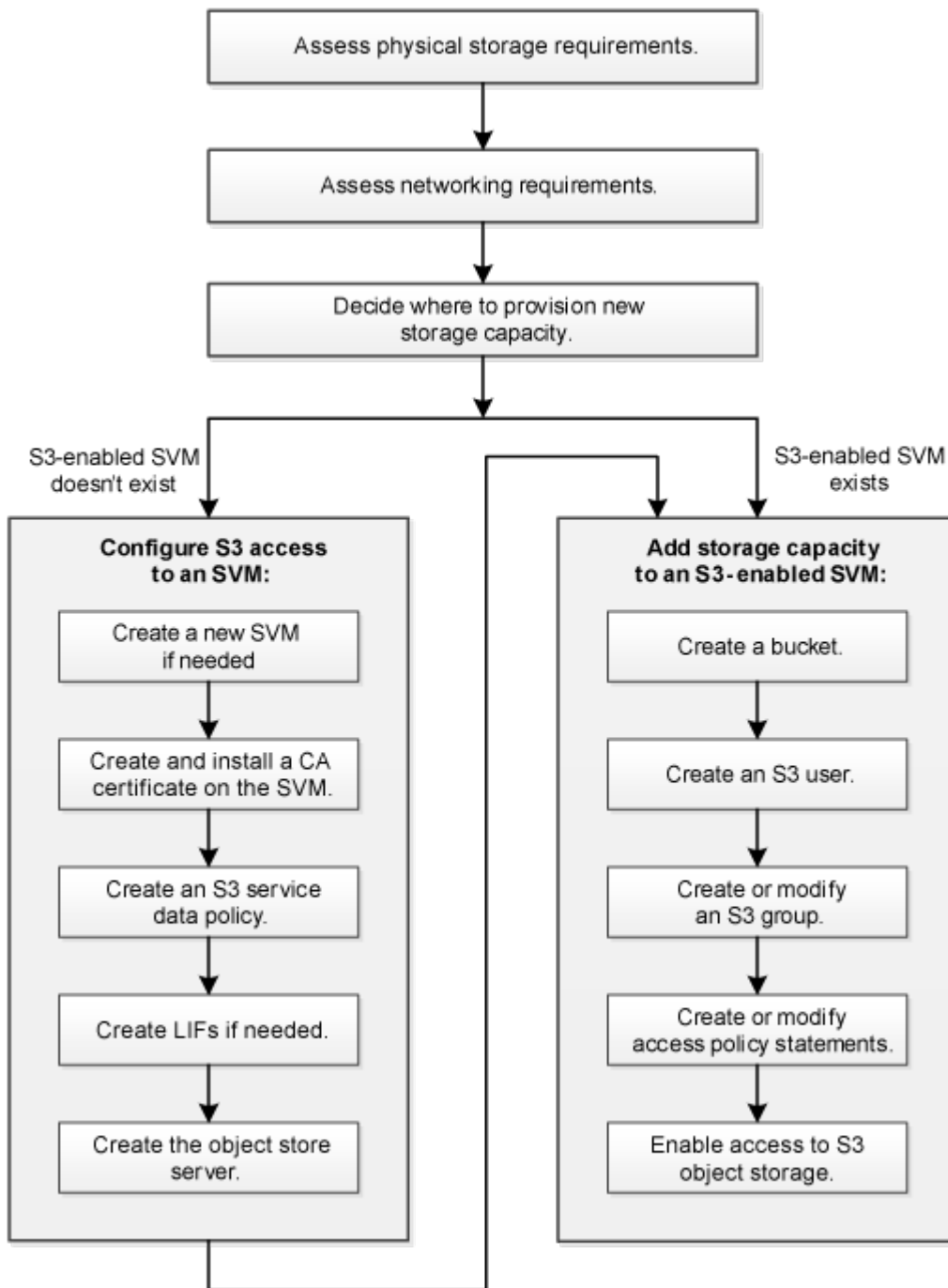
### Informazioni sul processo di configurazione S3

#### Workflow di configurazione S3

La configurazione di S3 implica la valutazione dei requisiti di storage fisico e di rete, quindi la scelta di un workflow specifico per il tuo obiettivo: Configurare l'accesso S3 a una SVM nuova o esistente oppure aggiungere un bucket e utenti a una SVM esistente già completamente configurata per l'accesso S3.

Quando si configura l'accesso S3 a una nuova macchina virtuale di storage utilizzando System Manager, viene richiesto di inserire le informazioni relative a certificato e rete e di creare la macchina virtuale di storage e il

server di storage a oggetti S3 in una singola operazione.



### Valutare i requisiti di storage fisico

Prima di eseguire il provisioning dello storage S3 per i client, è necessario assicurarsi che vi sia spazio sufficiente negli aggregati esistenti per il nuovo archivio di oggetti. In caso contrario, è possibile aggiungere dischi agli aggregati esistenti o creare nuovi aggregati del tipo e della posizione desiderati.

### A proposito di questa attività

Quando si crea un bucket S3 in una SVM abilitata per S3, viene creato automaticamente un volume FlexGroup per supportare il bucket. È possibile lasciare che ONTAP Select gli aggregati sottostanti e i componenti



FlexGroup automaticamente (impostazione predefinita) oppure selezionare gli aggregati sottostanti e i componenti FlexGroup autonomamente.

Se si decide di specificare gli aggregati e i componenti FlexGroup, ad esempio se si dispone di requisiti di performance specifici per i dischi sottostanti, è necessario assicurarsi che la configurazione dell'aggregato sia conforme alle linee guida delle Best practice per il provisioning di un volume FlexGroup. Scopri di più:

- ["Gestione dei volumi FlexGroup"](#)
- ["Report tecnico NetApp 4571-a: Best practice per il volume NetApp ONTAP FlexGroup"](#)

Se si utilizzano bucket di Cloud Volumes ONTAP, si consiglia di selezionare manualmente gli aggregati sottostanti per assicurarsi che utilizzino un solo nodo. L'utilizzo di aggregati di entrambi i nodi può influire sulle performance, poiché i nodi si trovano in zone di disponibilità separate geograficamente e quindi suscettibili a problemi di latenza. Scopri di più ["Creazione di bucket per Cloud Volumes ONTAP"](#).

È possibile utilizzare il server ONTAP S3 per creare un Tier di capacità FabricPool locale, ovvero nello stesso cluster del Tier di performance. Questo può essere utile, ad esempio, se si dispone di dischi SSD collegati a una coppia ha e si desidera eseguire il tiering dei dati *cold* su dischi HDD in un'altra coppia ha. In questo caso di utilizzo, il server S3 e il bucket contenente il Tier di capacità locale devono pertanto trovarsi in una coppia ha diversa dal Tier di performance. Il tiering locale non è supportato nei cluster a un nodo e a due nodi.

## Fasi

1. Visualizzare lo spazio disponibile negli aggregati esistenti:

```
storage aggregate show
```

Se esiste un aggregato con spazio sufficiente o una posizione del nodo richiesta, registrare il nome della configurazione S3.

```
cluster-1::> storage aggregate show
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID Status
aggr_0	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_1	239.0GB	11.13GB	95%	online	1	node1	raid_dp, normal
aggr_2	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_3	239.0GB	11.13GB	95%	online	1	node2	raid_dp, normal
aggr_4	239.0GB	238.9GB	95%	online	5	node3	raid_dp, normal
aggr_5	239.0GB	239.0GB	95%	online	4	node4	raid_dp, normal

6 entries were displayed.

2. Se non sono presenti aggregati con spazio sufficiente o posizione del nodo richiesta, aggiungere i dischi a un aggregato esistente utilizzando `storage aggregate add-disks` oppure creare un nuovo aggregato utilizzando il comando `storage aggregate create` comando.

## Valutare i requisiti di rete

Prima di fornire storage S3 ai client, è necessario verificare che la rete sia configurata correttamente per soddisfare i requisiti di provisioning S3.

### Prima di iniziare

È necessario configurare i seguenti oggetti di rete del cluster:

- Porte fisiche e logiche
- Domini di broadcast
- Subnet (se richieste)
- IPspaces (come richiesto, oltre all'IPSpace predefinito)
- Gruppi di failover (secondo necessità, oltre al gruppo di failover predefinito per ciascun dominio di broadcast)
- Firewall esterni

### A proposito di questa attività

Per i Tier di capacità FabricPool (cloud) remoti e i client S3 remoti, è necessario utilizzare una SVM di dati e configurare le LIF di dati. Per i livelli cloud FabricPool, è necessario configurare anche le LIF tra cluster; il peering dei cluster non è richiesto.

Per i Tier di capacità FabricPool locali, è necessario utilizzare la SVM di sistema (chiamata "Cluster"), ma sono disponibili due opzioni per la configurazione LIF:

- È possibile utilizzare le LIF del cluster.

In questa opzione, non è richiesta alcuna ulteriore configurazione LIF, ma il traffico sulle LIF del cluster aumenterà. Inoltre, il Tier locale non sarà accessibile ad altri cluster.

- È possibile utilizzare le LIF di dati e intercluster.

Questa opzione richiede un'ulteriore configurazione, inclusa l'abilitazione delle LIF per il protocollo S3, ma il Tier locale sarà accessibile anche come Tier cloud FabricPool remoto ad altri cluster.

### Fasi

1. Visualizzare le porte fisiche e virtuali disponibili:

```
network port show
```

- Quando possibile, utilizzare la porta con la velocità massima per la rete dati.
- Per ottenere le migliori prestazioni, tutti i componenti della rete dati devono avere la stessa impostazione MTU.

2. Se si intende utilizzare un nome di sottorete per assegnare l'indirizzo IP e il valore della maschera di rete per una LIF, verificare che la subnet esista e che gli indirizzi disponibili siano sufficienti:

```
network subnet show
```

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Le subnet vengono create utilizzando `network subnet create` comando.

### 3. Visualizzare gli spazi IP disponibili:

```
network ipspace show
```

È possibile utilizzare l'IPSpace predefinito o un IPSpace personalizzato.

### 4. Se si desidera utilizzare gli indirizzi IPv6, verificare che IPv6 sia attivato sul cluster:

```
network options ipv6 show
```

Se necessario, è possibile attivare IPv6 utilizzando `network options ipv6 modify` comando.

## Decidere dove eseguire il provisioning della nuova capacità di storage S3

Prima di creare un nuovo bucket S3, è necessario decidere se posizionarlo in una SVM nuova o esistente. Questa decisione determina il tuo flusso di lavoro.

### Scelte

- Se si desidera eseguire il provisioning di un bucket in un nuovo SVM o SVM non abilitato per S3, completare la procedura descritta nei seguenti argomenti.

["Creare una SVM per S3"](#)

["Creare un bucket per S3"](#)

Sebbene S3 possa coesistere in una SVM con NFS e SMB, è possibile scegliere di creare una nuova SVM se si verifica una delle seguenti condizioni:

- Si sta abilitando S3 su un cluster per la prima volta.
  - Esistono SVM in un cluster in cui non si desidera attivare il supporto S3.
  - Si dispone di una o più SVM abilitate per S3 in un cluster e si desidera un altro server S3 con caratteristiche di performance diverse. Dopo aver attivato S3 sulla SVM, procedere con il provisioning di un bucket.
- Se si desidera eseguire il provisioning del bucket iniziale o di un bucket aggiuntivo su una SVM abilitata S3 esistente, completare la procedura descritta nel seguente argomento.

["Creare un bucket per S3"](#)

## Configurare l'accesso S3 a una SVM

### Creare una SVM per S3

Sebbene S3 possa coesistere con altri protocolli in una SVM, potrebbe essere necessario creare una nuova SVM per isolare lo spazio dei nomi e il carico di lavoro.

### A proposito di questa attività

Se si fornisce solo lo storage a oggetti S3 da una SVM, il server S3 non richiede alcuna configurazione DNS. Tuttavia, se si utilizzano altri protocolli, è possibile configurare il DNS sulla SVM.

Quando si configura l'accesso S3 a una nuova macchina virtuale di storage utilizzando System Manager, viene richiesto di inserire le informazioni relative a certificato e rete e di creare la macchina virtuale di storage e il

server di storage a oggetti S3 in una singola operazione.

## Esempio 15. Fasi

### System Manager

Si consiglia di immettere il nome del server S3 come FQDN (Fully Qualified Domain Name), utilizzato dai client per l'accesso S3. L'FQDN del server S3 non deve iniziare con un nome bucket.

Si consiglia di inserire gli indirizzi IP per i dati del ruolo dell'interfaccia.

Se si utilizza un certificato firmato da una CA esterna, viene richiesto di inserirlo durante questa procedura; è inoltre possibile utilizzare un certificato generato dal sistema.

1. Abilitare S3 su una VM di storage.

- a. Aggiungere una nuova VM di storage: Fare clic su **Storage > Storage VMS**, quindi fare clic su **Add** (Aggiungi).

Se si tratta di un nuovo sistema senza macchine virtuali di storage esistenti, fare clic su **Dashboard > Configure Protocols** (Configura protocolli).

Se si aggiunge un server S3 a una VM di storage esistente: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings** (Impostazioni), quindi fare clic su  Sotto **S3**.

- a. Fare clic su **Enable S3** (attiva S3), quindi immettere il nome del server S3.
- b. Selezionare il tipo di certificato.

Se si seleziona un certificato generato dal sistema o uno dei propri, questo sarà necessario per l'accesso del client.

- c. Inserire le interfacce di rete.

2. Se è stato selezionato il certificato generato dal sistema, le informazioni del certificato vengono visualizzate quando viene confermata la creazione della nuova VM di storage. Fare clic su **Download** e salvarlo per accedere al client.

- La chiave segreta non viene visualizzata di nuovo.
- Se sono necessarie nuovamente le informazioni del certificato: Fare clic su **Storage > Storage VMS**, selezionare la VM di storage e fare clic su **Settings** (Impostazioni).

### CLI

1. Verificare che S3 sia concesso in licenza sul cluster:

```
system license show -package s3
```

In caso contrario, contattare il rappresentante commerciale.

2. Creare una SVM:

```
vserver create -vserver <svm_name> -subtype default -rootvolume  
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security  
-style unix -language C.UTF-8 -data-services <data-s3-server>  
-ipSPACE <ipSPACE_name>
```

- Utilizzare l'impostazione UNIX per `-rootvolume-security-style` opzione.
- Utilizzare il C.UTF-8 predefinito `-language` opzione.
- Il `ipSPACE` l'impostazione è facoltativa.

### 3. Verificare la configurazione e lo stato della SVM appena creata:

```
vserver show -vserver <svm_name>
```

Il `Vserver Operational State` il campo deve visualizzare `running` stato. Se viene visualizzato il `initializing` indica che alcune operazioni intermedie, ad esempio la creazione del volume root, non sono riuscite ed è necessario eliminare la SVM e ricrearla.

## Esempi

Il seguente comando crea una SVM per l'accesso ai dati in IPSPACE `ipSPACEA`:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume  
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language  
C.UTF-8 -data-services _data-s3-server_ -ipSPACE ipSPACEA
```

```
[Job 2059] Job succeeded:  
Vserver creation completed
```

Il seguente comando indica che è stata creata una SVM con un volume root di 1 GB, che è stata avviata automaticamente e si trova in `running` stato. Il volume root dispone di un criterio di esportazione predefinito che non include alcuna regola, pertanto il volume root non viene esportato al momento della creazione. Per impostazione predefinita, l'account utente `vsadmin` viene creato e si trova in `locked` stato. Il ruolo `vsadmin` viene assegnato all'account utente `vsadmin` predefinito.

```

cluster-1::> vserver show -vserver svm1.example.com
                                Vserver: svm1.example.com
                                Vserver Type: data
                                Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736

                                Root Volume: root_svm1
                                Aggregate: aggr1
                                NIS Domain: -
                                Root Volume Security Style: unix
                                LDAP Client: -
                                Default Volume Language Code: C.UTF-8
                                Snapshot Policy: default
                                Comment:
                                Quota Policy: default
                                List of Aggregates Assigned: -
                                Limit on Maximum Number of Volumes allowed: unlimited
                                Vserver Admin State: running
                                Vserver Operational State: running
                                Vserver Operational State Stopped Reason: -
                                Allowed Protocols: nfs, cifs
                                Disallowed Protocols: -
                                QoS Policy Group: -
                                Config Lock: false
                                IPspace Name: ipspaceA

```

## Creare e installare un certificato CA sulla SVM

Per abilitare il traffico HTTPS dai client S3 alla SVM abilitata per S3, è necessario un certificato CA (Certificate Authority).

### A proposito di questa attività

Sebbene sia possibile configurare un server S3 in modo che utilizzi solo HTTP e sebbene sia possibile configurare i client senza un requisito di certificato CA, è consigliabile proteggere il traffico HTTPS ai server ONTAP S3 con un certificato CA.

Un certificato CA non è necessario per un caso di utilizzo del tiering locale, in cui il traffico IP passa solo attraverso le LIF del cluster.

Le istruzioni di questa procedura consentono di creare e installare un certificato autofirmato ONTAP. Sono supportati anche i certificati CA di fornitori terzi; per ulteriori informazioni, consultare la documentazione di autenticazione dell'amministratore.

### "Autenticazione amministratore e RBAC"

Vedere `security certificate` pagine man per ulteriori opzioni di configurazione.

## Fasi

### 1. Creare un certificato digitale autofirmato:

```
security certificate create -vserver svm_name -type root-ca -common-name  
ca_cert_name
```

Il `-type root-ca` L'opzione crea e installa un certificato digitale autofirmato per firmare altri certificati agendo come autorità di certificazione (CA).

Il `-common-name` L'opzione crea il nome dell'autorità di certificazione (CA) di SVM e verrà utilizzata per generare il nome completo del certificato.

La dimensione predefinita del certificato è 2048 bit.

#### Esempio

```
cluster-1::> security certificate create -vserver svm1.example.com -type  
root-ca -common-name svm1_ca
```

```
The certificate's generated name for reference:  
svm1_ca_159D1587CE21E9D4_svm1_ca
```

Quando viene visualizzato il nome generato del certificato, assicurarsi di salvarlo per i passaggi successivi di questa procedura.

### 2. Generare una richiesta di firma del certificato:

```
security certificate generate-csr -common-name s3_server_name  
[additional_options]
```

Il `-common-name` Il parametro per la richiesta di firma deve essere il nome del server S3 (FQDN).

Se lo si desidera, è possibile fornire la posizione e altre informazioni dettagliate sulla SVM.

Viene richiesto di conservare una copia della richiesta di certificato e della chiave privata per riferimenti futuri.

### 3. Firmare la CSR utilizzando SVM\_CA per generare il certificato del server S3:

```
security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial  
ca_cert_serial_number [additional_options]
```

Immettere le opzioni di comando utilizzate nei passaggi precedenti:

- `-ca` — il nome comune della CA immesso nel passaggio 1.
- `-ca-serial` — il numero di serie della CA dal punto 1. Ad esempio, se il nome del certificato CA è `svm1_ca_159D1587CE21E9D4_svm1_ca`, il numero di serie è `159D1587CE21E9D4`.

Per impostazione predefinita, il certificato firmato scadrà tra 365 giorni. È possibile selezionare un altro valore e specificare altri dettagli della firma.



Quando richiesto, copiare e inserire la stringa di richiesta del certificato salvata nel passaggio 2.

Viene visualizzato un certificato firmato; salvarlo per un utilizzo successivo.

4. Installare il certificato firmato sulla SVM abilitata per S3:

```
security certificate install -type server -vserver svm_name
```

Quando richiesto, inserire il certificato e la chiave privata.

Se si desidera inserire una catena di certificati, è possibile immettere i certificati intermedi.

Quando vengono visualizzate la chiave privata e il certificato digitale firmato dalla CA, salvarle per riferimenti futuri.

5. Ottenere il certificato della chiave pubblica:

```
security certificate show -vserver svm_name -common-name ca_cert_name -type  
root-ca -instance
```

Salvare il certificato della chiave pubblica per una configurazione successiva lato client.

Esempio

```

cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca -instance

                Name of Vserver: svm1.example.com
        FQDN or Custom Common Name: svm1_ca
    Serial Number of Certificate: 159D1587CE21E9D4
        Certificate Authority: svm1_ca
            Type of Certificate: root-ca
(DEPRECATED)-Certificate Subtype: -
        Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
        Certificate Start Date: Thu May 09 10:58:39 2020
        Certificate Expiration Date: Fri May 08 10:58:39 2021
        Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----

                Country Name: US
        State or Province Name:
                Locality Name:
                Organization Name:
                Organization Unit:
Contact Administrator's Email Address:
                Protocol: SSL
                Hashing Function: SHA256
        Self-Signed Certificate: true
        Is System Internal Certificate: false

```

### Creare una policy sui dati del servizio S3

È possibile creare policy di servizio per i dati S3 e i servizi di gestione. Per abilitare il traffico dati S3 su LIF, è necessaria una policy dei dati del servizio S3.

#### A proposito di questa attività

Se si utilizzano LIF di dati e LIF di intercluster, è necessaria una policy sui dati di servizio S3. Non è necessario se si utilizzano le LIF del cluster per il caso di utilizzo del tiering locale.

Quando viene specificata una policy di servizio per una LIF, questa viene utilizzata per creare un ruolo predefinito, una policy di failover e un elenco di protocolli dati per la LIF.

Sebbene sia possibile configurare più protocolli per SVM e LIFF, è consigliabile che S3 sia l'unico protocollo per la fornitura di dati a oggetti.

#### Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

## 2. Creare una policy sui dati del servizio:

```
network interface service-policy create -vserver svm_name -policy policy_name  
-services data-core,data-s3-server
```

Il data-core e. data-s3-server I servizi sono gli unici necessari per abilitare ONTAP S3, anche se è possibile includere altri servizi in base alle esigenze.

### Creazione di LIF di dati

Se hai creato una nuova SVM, le LIF dedicate create per l'accesso S3 dovrebbero essere le LIF dei dati.

#### Prima di iniziare

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore up stato.
- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando `network subnet create` comando.

- La politica di servizio LIF deve già esistere.

#### A proposito di questa attività

- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster utilizzando `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).
- Se si abilita il tiering remoto della capacità FabricPool (cloud), è necessario configurare anche le LIF intercluster.

#### Fasi

##### 1. Creare una LIF:

```
network interface create -vserver svm_name -lif lif_name -service-policy  
service_policy_names -home-node node_name -home-port port_name {-address  
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy  
data -auto-revert {true|false}
```

- -home-node È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

È inoltre possibile specificare se il LIF deve ripristinare automaticamente il nodo home e la porta home con `-auto-revert` opzione.

- -home-port È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
- È possibile specificare un indirizzo IP con `-address` e. `-netmask` oppure attivare l'allocazione da una subnet con `-subnet_name` opzione.

- Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene automaticamente aggiunto un percorso predefinito a tale gateway.
- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- Per `-firewall-policy` utilizzare lo stesso valore predefinito `data` Come ruolo LIF.

Se lo si desidera, è possibile creare e aggiungere un criterio firewall personalizzato in un secondo momento.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

- `-auto-revert` Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `false` in base alle policy di gestione della rete nel proprio ambiente.
- Il `-service-policy` l'opzione specifica la policy creata per i dati e i servizi di gestione e qualsiasi altra policy necessaria.

## 2. Se si desidera assegnare un indirizzo IPv6 in `-address` opzione:

- Utilizzare `network ndp prefix show` Per visualizzare l'elenco dei prefissi RA appresi su varie interfacce.

Il `network ndp prefix show` il comando è disponibile a livello di privilegio avanzato.

- Utilizzare il formato `prefix:id` Per costruire manualmente l'indirizzo IPv6.

`prefix` è il prefisso appreso sulle varie interfacce.

Per derivare il `id`, scegliere un numero esadecimale casuale a 64 bit.

- Verificare che la LIF sia stata creata correttamente utilizzando `network interface show` comando.
- Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

## Esempi

Il comando seguente mostra come creare una LIF di dati S3 assegnata a `my-S3-policy` politica di servizio:

```
network interface create -vserver svml.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

Il seguente comando mostra tutti i LIF nel cluster-1. Data LIF datalif1 e datalif3 sono configurati con indirizzi IPv4 e datalif4 è configurato con un indirizzo IPv6:

```
cluster-1::> network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----
----					
cluster-1					
	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
true					
node-1					
	clus1	up/up	192.0.2.12/24	node-1	e0a
true					
	clus2	up/up	192.0.2.13/24	node-1	e0b
true					
	mgmt1	up/up	192.0.2.68/24	node-1	e1a
true					
node-2					
	clus1	up/up	192.0.2.14/24	node-2	e0a
true					
	clus2	up/up	192.0.2.15/24	node-2	e0b
true					
	mgmt1	up/up	192.0.2.69/24	node-2	e1a
true					
vs1.example.com					
	datalif1	up/down	192.0.2.145/30	node-1	e1c
true					
vs3.example.com					
	datalif3	up/up	192.0.2.146/30	node-2	e0c
true					
	datalif4	up/up	2001::2/64	node-2	e0c
true					

5 entries were displayed.

### Creazione di LIF intercluster per tiering FabricPool remoto

Se si abilita il tiering della capacità FabricPool remota (cloud) utilizzando ONTAP S3, è necessario configurare le LIF tra cluster. È possibile configurare le LIF di intercluster sulle

porte condivise con la rete dati. In questo modo si riduce il numero di porte necessarie per la rete tra cluster.

**Prima di iniziare**

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore up stato.
- La politica di servizio LIF deve già esistere.

**A proposito di questa attività**

Le LIF intercluster non sono richieste per il tiering del pool di fabric locale o per la fornitura di applicazioni S3 esterne.

**Fasi**

1. Elencare le porte nel cluster:

```
network port show
```

L'esempio seguente mostra le porte di rete in cluster01:

```
cluster01::> network port show
```

(Mbps)						Speed	
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	
-----							
-----							
cluster01-01							
	e0a	Cluster	Cluster	up	1500	auto/1000	
	e0b	Cluster	Cluster	up	1500	auto/1000	
	e0c	Default	Default	up	1500	auto/1000	
	e0d	Default	Default	up	1500	auto/1000	
cluster01-02							
	e0a	Cluster	Cluster	up	1500	auto/1000	
	e0b	Cluster	Cluster	up	1500	auto/1000	
	e0c	Default	Default	up	1500	auto/1000	
	e0d	Default	Default	up	1500	auto/1000	

2. Creazione di LIF intercluster sulla SVM di sistema:

```
network interface create -vserver Cluster -lif LIF_name -service-policy
default-intercluster -home-node node -home-port port -address port_IP -netmask
netmask
```

Nell'esempio seguente vengono create le LIF tra cluster cluster01\_icl01 e cluster01\_icl02:

```

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0

```

### 3. Verificare che le LIF dell'intercluster siano state create:

```
network interface show -service-policy default-intercluster
```

```

cluster01::> network interface show -service-policy default-intercluster

```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01 e0c
true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02 e0c
true				

### 4. Verificare che le LIF dell'intercluster siano ridondanti:

```
network interface show -service-policy default-intercluster -failover
```

L'esempio seguente mostra che le LIF dell'intercluster cluster01\_icl01 e cluster01\_icl02 su e0c viene eseguito il failover della porta su e0d porta.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster01				
	cluster01_icl01	cluster01-01:e0c	local-only	
192.168.1.201/24				
			Failover Targets: cluster01-01:e0c,	
			cluster01-01:e0d	
	cluster01_icl02	cluster01-02:e0c	local-only	
192.168.1.201/24				
			Failover Targets: cluster01-02:e0c,	
			cluster01-02:e0d	

### Creare il server archivio oggetti S3

Il server di archiviazione a oggetti ONTAP gestisce i dati come oggetti S3, invece dello storage a blocchi o file fornito dai server NAS e SAN ONTAP.

#### Prima di iniziare

Si consiglia di immettere il nome del server S3 come FQDN (Fully Qualified Domain Name), utilizzato dai client per l'accesso S3. L'FQDN non deve iniziare con un nome bucket.

È necessario disporre di un certificato CA autofirmato (creato nei passaggi precedenti) o di un certificato firmato da un vendor CA esterno. Un certificato CA non è necessario per un caso di utilizzo del tiering locale, in cui il traffico IP passa solo attraverso le LIF del cluster.

#### A proposito di questa attività

Quando viene creato un server archivio oggetti, viene creato un utente root con UID 0. Per questo utente root non viene generata alcuna chiave di accesso o chiave segreta. L'amministratore di ONTAP deve eseguire `object-store-server users regenerate-keys` per impostare la chiave di accesso e la chiave segreta per questo utente.



Come Best practice NetApp, non utilizzare questo utente root. Qualsiasi applicazione client che utilizza la chiave di accesso o la chiave segreta dell'utente root ha accesso completo a tutti i bucket e gli oggetti nell'archivio di oggetti.

Vedere `vserver object-store-server` pagine man per ulteriori opzioni di configurazione e visualizzazione.




## Esempio 16. Fasi

### System Manager

Utilizzare questa procedura se si aggiunge un server S3 a una VM di storage esistente. Per aggiungere un server S3 a una nuova VM di storage, vedere ["Creare una SVM di storage per S3"](#).

Si consiglia di inserire gli indirizzi IP per i dati del ruolo dell'interfaccia.

#### 1. Abilitare S3 su una VM di storage esistente.

- Selezionare la VM di storage: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings**, quindi fare clic su  Sotto **S3**.
- Fare clic su **Enable S3** (attiva S3), quindi immettere il nome del server S3.
- Selezionare il tipo di certificato.

Se si seleziona un certificato generato dal sistema o uno dei propri, questo sarà necessario per l'accesso del client.

#### d. Inserire le interfacce di rete.

#### 2. Se è stato selezionato il certificato generato dal sistema, le informazioni del certificato vengono visualizzate quando viene confermata la creazione della nuova VM di storage. Fare clic su **Download** e salvarlo per accedere al client.

- La chiave segreta non viene visualizzata di nuovo.
- Se sono necessarie nuovamente le informazioni del certificato: Fare clic su **Storage > Storage VMS**, selezionare la VM di storage e fare clic su **Settings** (Impostazioni).

### CLI

#### 1. Creare il server S3:

```
vserver object-store-server create -vserver svm_name -object-store-server  
s3_server_fqdn -certificate-name server_certificate_name -comment text  
[additional_options]
```

È possibile specificare opzioni aggiuntive durante la creazione del server S3 o in qualsiasi momento successivo.

- In caso di configurazione del tiering locale, il nome della SVM può essere un nome di una SVM dati o di una SVM di sistema (cluster).
- Il nome del certificato deve essere il nome del certificato del server (certificato dell'utente finale o del foglio) e non il certificato della CA del server (certificato della CA intermedia o di origine).
- HTTPS è attivato per impostazione predefinita sulla porta 443. È possibile modificare il numero di porta con `-secure-listener-port` opzione.

Quando HTTPS è attivato, i certificati CA sono necessari per la corretta integrazione con SSL/TLS.

- HTTP è disattivato per impostazione predefinita. Quando questa opzione è attivata, il server è in attesa sulla porta 80. È possibile attivarlo con `-is-http-enabled` oppure modificare il numero di porta con il `-listener-port` opzione.

Quando HTTP è attivato, la richiesta e le risposte vengono inviate in rete in formato non

crittografato.

2. Verificare che S3 sia configurato:

```
vserver object-store-server show
```

### Esempio

Questo comando verifica i valori di configurazione di tutti i server di storage a oggetti:

```
cluster1::> vserver object-store-server show

Vserver: vs1

Object Store Server Name: s3.example.com
Administrative State: up
Listener Port For HTTP: 80
Secure Listener Port For HTTPS: 443
HTTP Enabled: false
HTTPS Enabled: true
Certificate for HTTPS Connections: svm1_ca
Comment: Server comment
```

## Aggiungere capacità di storage a una SVM abilitata per S3

### Creare un bucket

Gli oggetti S3 sono conservati in *bucket*. Non sono nidificati come file all'interno di una directory all'interno di altre directory.

### Prima di iniziare

Una VM di storage contenente un server S3 deve già esistere.

### A proposito di questa attività

- A partire da ONTAP 9.14.1, il ridimensionamento automatico è stato abilitato sui volumi FlexGroup S3 quando vengono creati i bucket su di essi. In questo modo si elimina l'allocazione eccessiva di capacità durante la creazione del bucket su volumi FlexGroup nuovi ed esistenti. I volumi FlexGroup vengono ridimensionati a una dimensione minima richiesta in base alle seguenti linee guida. La dimensione minima richiesta è la dimensione totale di tutti i bucket S3 in un volume FlexGroup.
  - A partire da ONTAP 9.14.1, se viene creato un volume FlexGroup S3 come parte di una nuova creazione di bucket, il volume FlexGroup viene creato con le dimensioni minime richieste.
  - Se è stato creato un volume S3 FlexGroup prima di ONTAP 9.14.1, il primo bucket creato o eliminato successivamente a ONTAP 9.14.1 ridimensiona il volume FlexGroup alla dimensione minima richiesta.
  - Se un volume S3 FlexGroup è stato creato prima di ONTAP 9.14.1 e aveva già le dimensioni minime richieste, la creazione o l'eliminazione di un bucket successivo a ONTAP 9.14.1 mantiene le dimensioni del volume S3 FlexGroup.
- I livelli di servizio dello storage sono gruppi di criteri QoS (Quality of Service) adattivi predefiniti, con livelli

predefiniti *value*, *performance* e *Extreme*. Invece di uno dei livelli di servizio storage predefiniti, è possibile definire un gruppo di policy QoS personalizzato e applicarlo a un bucket. Per ulteriori informazioni sulle definizioni dei servizi di archiviazione, vedere ["Definizioni dei servizi di storage"](#). Per ulteriori informazioni sulla gestione delle prestazioni, vedere ["Gestione delle performance"](#).

A partire da ONTAP 9.8, quando si esegue il provisioning dello storage, la qualità del servizio viene attivata per impostazione predefinita. È possibile disattivare la QoS o scegliere una policy QoS personalizzata durante il processo di provisioning o in un secondo momento.

- Se stai configurando il tiering locale della capacità, creerai bucket e utenti in una VM per lo storage dei dati, non nella VM di storage del sistema in cui si trova il server S3.
- Per l'accesso client remoto, è necessario configurare i bucket in una VM di storage abilitata per S3. Se si crea un bucket in una VM storage non abilitata per S3, sarà disponibile solo per il tiering locale.
- A partire da ONTAP 9.14.1, è possibile ["Crea un bucket su un aggregato con mirroring o senza mirror in una configurazione MetroCluster"](#).
- Per la CLI, quando si crea un bucket, sono disponibili due opzioni di provisioning:
  - Lasciare ONTAP Select gli aggregati sottostanti e i componenti FlexGroup (impostazione predefinita)
    - ONTAP crea e configura un volume FlexGroup per il primo bucket selezionando automaticamente gli aggregati. Verrà selezionato automaticamente il livello di servizio più alto disponibile per la piattaforma oppure sarà possibile specificare il livello di servizio storage. Tutti i bucket aggiuntivi che Aggiungi in seguito nella VM di storage avranno lo stesso volume FlexGroup sottostante.
    - In alternativa, è possibile specificare se il bucket verrà utilizzato per il tiering, nel qual caso ONTAP tenta di selezionare supporti a basso costo con performance ottimali per i dati su più livelli.
  - Si selezionano gli aggregati sottostanti e i componenti FlexGroup (richiede opzioni avanzate dei comandi con privilegi): Si può selezionare manualmente gli aggregati in cui deve essere creato il bucket e il volume FlexGroup contenente, quindi specificando il numero dei componenti in ogni aggregato. Quando si aggiungono bucket aggiuntivi:
    - Se si specificano aggregati e costituenti per un nuovo bucket, verrà creato un nuovo FlexGroup per il nuovo bucket.
    - Se non si specificano aggregati e componenti per un nuovo bucket, il nuovo bucket verrà aggiunto a un FlexGroup esistente. Vedere [Gestione dei volumi FlexGroup](#) per ulteriori informazioni.

Quando si specificano aggregati e costituenti durante la creazione di un bucket, non vengono applicati gruppi di criteri QoS, predefiniti o personalizzati. È possibile farlo in un secondo momento con `vserver object-store-server bucket modify` comando.

Vedere ["vserver object-store-server modifica bucket"](#) per ulteriori informazioni.

**Nota:** se si utilizzano bucket da Cloud Volumes ONTAP, è necessario utilizzare la procedura CLI. Si consiglia di selezionare manualmente gli aggregati sottostanti per assicurarsi che utilizzino un solo nodo. L'utilizzo di aggregati di entrambi i nodi può influire sulle performance, poiché i nodi si trovano in zone di disponibilità separate geograficamente e quindi suscettibili a problemi di latenza.

### Crea bucket S3 con l'interfaccia a riga di comando di ONTAP

1. Se si prevede di selezionare autonomamente aggregati e componenti FlexGroup, impostare il livello di privilegio su Advanced (altrimenti, il livello di privilegio admin è sufficiente): `set -privilege advanced`
2. Creare un bucket:

```
vserver object-store-server bucket create -vserver svm_name -bucket
```

```
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

Il nome della macchina virtuale storage può essere una macchina virtuale per lo storage dei dati o. Cluster (Il nome della VM di storage del sistema) se si sta configurando il tiering locale.

Se non si specifica alcuna opzione, ONTAP crea un bucket 800GB con il livello di servizio al livello più alto disponibile per il sistema.

Se si desidera che ONTAP crei un bucket in base alle performance o all'utilizzo, utilizzare una delle seguenti opzioni:

- livello di servizio

Includere il `-storage-service-level` con uno dei seguenti valori: `value`, `performance`, o, `extreme`.

- tiering

Includere il `-used-as-capacity-tier true` opzione.

Se si desidera specificare gli aggregati su cui creare il volume FlexGroup sottostante, utilizzare le seguenti opzioni:

- Il `-aggr-list` Parametro specifica l'elenco di aggregati da utilizzare per i componenti del volume FlexGroup.

Ogni voce dell'elenco crea un costituente nell'aggregato specificato. È possibile specificare un aggregato più volte per creare più costituenti sull'aggregato.

Per ottenere performance costanti nel volume FlexGroup, tutti gli aggregati devono utilizzare lo stesso tipo di disco e le stesse configurazioni del gruppo RAID.

- Il `-aggr-list-multiplier` il parametro specifica il numero di iterazioni degli aggregati elencati con `-aggr-list` Quando si crea un volume FlexGroup.

Il valore predefinito di `-aggr-list-multiplier` il parametro è 4.

### 3. Aggiungere un gruppo di criteri QoS, se necessario:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
-group qos_policy_group
```

### 4. Verificare la creazione del bucket:

```
vserver object-store-server bucket show [-instance]
```

## Esempio

L'esempio seguente crea un bucket per VM di storage `vs1` di dimensione 1TB e specificando l'aggregato:

```
cluster-1::*> vservers object-store-server bucket create -vservers
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

## Crea bucket S3 con System Manager

1. Aggiungi un nuovo bucket su una VM di storage abilitata per S3.
  - a. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
  - b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.
    - Se si fa clic su **Save** (Salva) a questo punto, viene creato un bucket con le seguenti impostazioni predefinite:
      - A nessun utente viene concesso l'accesso al bucket, a meno che non siano già in vigore policy di gruppo.



Non utilizzare l'utente root S3 per gestire lo storage a oggetti ONTAP e condividerne le autorizzazioni, in quanto dispone di accesso illimitato all'archivio di oggetti. Creare invece un utente o un gruppo con privilegi amministrativi assegnati.

- Un livello di qualità del servizio (performance) il più alto disponibile per il sistema.
- Fare clic su **Salva** per creare un bucket con questi valori predefiniti.

## Configurare autorizzazioni e restrizioni aggiuntive

È possibile fare clic su **altre opzioni** per configurare le impostazioni per il blocco degli oggetti, le autorizzazioni utente e il livello di prestazioni quando si configura il bucket oppure è possibile modificare queste impostazioni in un secondo momento.

Se si intende utilizzare l'archivio di oggetti S3 per il tiering FabricPool, si consiglia di selezionare **Use for Tiering** (utilizzare supporti a basso costo con performance ottimali per i dati a più livelli) piuttosto che un livello di servizio per le performance.

Se si desidera abilitare il controllo delle versioni per gli oggetti per un successivo ripristino, selezionare **Abilita controllo versioni**. La versione è abilitata per impostazione predefinita se si attiva il blocco degli oggetti nel bucket. Per informazioni sulla versione oggetto, vedere la ["Utilizzo della versione in bucket S3 per Amazon"](#).

A partire dalla versione 9.14.1, il blocco degli oggetti è supportato su bucket S3. S3 il blocco degli oggetti richiede una licenza SnapLock standard. Questa licenza è inclusa con ["ONTAP uno"](#).

Prima di ONTAP One, la licenza SnapLock era inclusa nel pacchetto sicurezza e conformità. Il bundle Security and Compliance non è più offerto, ma è ancora valido. Sebbene non sia attualmente richiesto, i clienti esistenti possono scegliere di farlo ["Eseguire l'aggiornamento a ONTAP One"](#).

Se si attiva il blocco degli oggetti su un bucket, è necessario ["Verificare che sia installata una licenza SnapLock"](#). Se non è installata una licenza SnapLock, è necessario ["installare"](#) prima di poter attivare il blocco degli oggetti.

Una volta verificata l'installazione della licenza SnapLock, per evitare che gli oggetti nel bucket vengano eliminati o sovrascritti, selezionare **attiva blocco oggetti**. Il blocco può essere abilitato su tutte le versioni o versioni specifiche di oggetti, e solo quando il clock di conformità SnapLock viene inizializzato per i nodi del cluster. Attenersi alla seguente procedura:

1. Se il clock di conformità SnapLock non è inizializzato su nessun nodo del cluster, viene visualizzato il pulsante **Inizializza orologio di conformità SnapLock**. Fare clic su **Inizializza orologio conformità**

**SnapLock** per inizializzare il clock di conformità SnapLock sui nodi del cluster.

2. Selezionare la modalità **Governance** per attivare un blocco basato sul tempo che consenta *Write Once, Read Many (WORM)* autorizzazioni sugli oggetti. Anche in modalità *Governance*, gli oggetti possono essere eliminati dagli utenti amministratori con autorizzazioni specifiche.
3. Selezionare la modalità **conformità** se si desidera assegnare regole più severe di eliminazione e aggiornamento sugli oggetti. In questa modalità di blocco degli oggetti, gli oggetti possono essere scaduti solo al termine del periodo di conservazione specificato. A meno che non venga specificato un periodo di conservazione, gli oggetti rimangono bloccati a tempo indeterminato.
4. Specificare il mantenimento per il blocco in giorni o anni se si desidera che il blocco sia efficace per un determinato periodo.



Il bloccaggio è applicabile alle benne S3 versione e non versione. Il blocco degli oggetti non è applicabile agli oggetti NAS.

È possibile configurare le impostazioni di protezione e autorizzazione e il livello di servizio delle prestazioni per il bucket.



È necessario aver già creato utenti e gruppi prima di configurare le autorizzazioni.

Per ulteriori informazioni, vedere ["Crea mirror per il nuovo bucket"](#).

## Verificare l'accesso alla benna

Nelle applicazioni client S3 (ONTAP S3 o un'applicazione esterna di terze parti), è possibile verificare l'accesso al bucket appena creato immettendo quanto segue:

- Certificato CA del server S3.
- La chiave di accesso e la chiave segreta dell'utente.
- Il nome FQDN e il nome bucket del server S3.

## Crea un bucket su un aggregato con mirroring o senza mirror in una configurazione MetroCluster

A partire da ONTAP 9.14.1, è possibile eseguire il provisioning di un bucket su un aggregato con mirroring o senza mirror nelle configurazioni FC e IP di MetroCluster.

### A proposito di questa attività

- Per impostazione predefinita, i bucket sono in provisioning su aggregati con mirroring.
- Le stesse linee guida per il provisioning delineate in ["Creare un bucket"](#) Applicare per creare un bucket in un ambiente MetroCluster.
- Le seguenti funzioni di storage a oggetti S3 sono **non** supportate negli ambienti MetroCluster:
  - S3 SnapMirror
  - S3 Gestione del ciclo di vita della benna
  - S3 blocco degli oggetti in modalità **conformità**



S3 è supportato il blocco degli oggetti in modalità **Governance**.

- Tiering FabricPool locale

### **Prima di iniziare**

Una SVM contenente un server S3 deve già esistere.

### **Processo per la creazione di bucket**

## CLI

1. Se si prevede di selezionare autonomamente aggregati e componenti FlexGroup, impostare il livello di privilegio su Advanced (altrimenti, il livello di privilegio admin è sufficiente): `set -privilege advanced`
2. Creare un bucket:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket  
<bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates  
true/false]
```

Impostare `-use-mirrored-aggregates` opzione a. `true` oppure `false` a seconda che si desideri utilizzare un aggregato con mirroring o senza mirror.



Per impostazione predefinita, il `-use-mirrored-aggregates` l'opzione è impostata su `true`.

- Il nome della SVM deve essere una SVM dati.
- Se non si specifica alcuna opzione, ONTAP crea un bucket 800GB con il livello di servizio al livello più alto disponibile per il sistema.
- Se si desidera che ONTAP crei un bucket in base alle performance o all'utilizzo, utilizzare una delle seguenti opzioni:
  - `livello di servizio`  
  
Includere il `-storage-service-level` con uno dei seguenti valori: `value`, `performance`, o. `extreme`.
  - `tiering`  
  
Includere il `-used-as-capacity-tier true` opzione.
- Se si desidera specificare gli aggregati su cui creare il volume FlexGroup sottostante, utilizzare le seguenti opzioni:
  - Il `-aggr-list` Parametro specifica l'elenco di aggregati da utilizzare per i componenti del volume FlexGroup.  
  
Ogni voce dell'elenco crea un costituente nell'aggregato specificato. È possibile specificare un aggregato più volte per creare più costituenti sull'aggregato.

Per ottenere performance costanti nel volume FlexGroup, tutti gli aggregati devono utilizzare lo stesso tipo di disco e le stesse configurazioni del gruppo RAID.

- Il `-aggr-list-multiplier` il parametro specifica il numero di iterazioni degli aggregati elencati con `-aggr-list` Quando si crea un volume FlexGroup.

Il valore predefinito di `-aggr-list-multiplier` il parametro è 4.

3. Aggiungere un gruppo di criteri QoS, se necessario:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy  
-group qos_policy_group
```



#### 4. Verificare la creazione del bucket:

```
vserver object-store-server bucket show [-instance]
```

#### Esempio

L'esempio seguente crea un bucket per SVM VS1 di dimensione 1TB su un aggregato mirrorato:

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svm1.example.com -bucket testbucket -size 1TB -use-mirrored-aggregates  
true
```

#### System Manager

1. Aggiungi un nuovo bucket su una VM di storage abilitata per S3.
  - a. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
  - b. Immettere un nome, selezionare la VM di storage e immettere una dimensione.

Per impostazione predefinita, il bucket è in provisioning su un aggregato con mirroring. Se si desidera creare un bucket su un aggregato senza mirror, selezionare **altre opzioni** e deselezionare la casella **Usa il livello SyncMirror in protezione** come mostrato nell'immagine seguente:



- È necessario aver già creato utenti e gruppi prima di utilizzare **altre opzioni** per configurare le relative autorizzazioni.
  - Se si intende utilizzare l'archivio di oggetti S3 per il tiering FabricPool, si consiglia di selezionare **Use for Tiering** (utilizzare supporti a basso costo con performance ottimali per i dati a più livelli) piuttosto che un livello di servizio per le performance.
2. Sulle applicazioni client S3 – un altro sistema ONTAP o un'applicazione esterna di terze parti – verificare l'accesso al nuovo bucket immettendo quanto segue:
- Certificato CA del server S3.
  - La chiave di accesso e la chiave segreta dell'utente.
  - Il nome FQDN e il nome bucket del server S3.

## Creare una regola di gestione del ciclo di vita del bucket

A partire da ONTAP 9.13.1, puoi creare regole di Lifecycle management per gestire i cicli di vita degli oggetti nei tuoi bucket S3. È possibile definire regole di eliminazione per oggetti specifici in un bucket e, attraverso queste regole, scadono tali oggetti bucket. Ciò consente di soddisfare i requisiti di conservazione e di gestire in modo efficiente lo storage a oggetti complessivo S3.



Se il blocco degli oggetti è attivato per gli oggetti bucket, le regole di gestione del ciclo di vita per la scadenza degli oggetti non verranno applicate agli oggetti bloccati. Per informazioni sul blocco degli oggetti, vedere ["Creare un bucket"](#).

### Prima di iniziare

Una SVM abilitata per S3 contenente un server S3 e un bucket deve già esistere. Vedere ["Creare una SVM per S3"](#) per ulteriori informazioni.

### A proposito di questa attività

Quando si creano le regole di gestione del ciclo di vita, è possibile applicare le seguenti azioni di eliminazione agli oggetti bucket:

- Eliminazione delle versioni correnti - questa azione scade gli oggetti identificati dalla regola. Se il controllo delle versioni è abilitato nel bucket, S3 rende non disponibili tutti gli oggetti scaduti. Se il controllo delle versioni non è abilitato, questa regola elimina gli oggetti in modo permanente. L'azione CLI è `Expiration`.
- Eliminazione di versioni non correnti - questa azione specifica quando S3 può rimuovere in modo permanente oggetti non correnti. L'azione CLI è `NoncurrentVersionExpiration`.
- Eliminazione dei marcatori di eliminazione scaduti - questa azione elimina i marcatori di eliminazione degli oggetti scaduti.  
Nei bucket abilitati per le versioni, gli oggetti con marcatori di eliminazione diventano le versioni correnti degli oggetti. Gli oggetti non vengono eliminati e non è possibile eseguire alcuna azione su di essi. Questi oggetti diventano scaduti quando non sono associate versioni correnti. L'azione CLI è `Expiration`.
- Eliminazione dei caricamenti di più parti incompleti - questa azione imposta il tempo massimo (in giorni) per il quale si desidera consentire il caricamento di più parti. Successivamente, vengono eliminati. L'azione CLI è `AbortIncompleteMultipartUpload`.

La procedura seguente dipende dall'interfaccia utilizzata. Con ONTAP 9.13,1, è necessario utilizzare la CLI. A

partire da ONTAP 9.14.1, è possibile utilizzare anche Gestione sistema.

### Gestisci le regole di Lifecycle management con la CLI

A partire da ONTAP 9.13.1, puoi utilizzare l'interfaccia a riga di comando di ONTAP per creare regole di Lifecycle management per scadere gli oggetti nei bucket S3.

#### Prima di iniziare

Per la CLI, è necessario definire i campi obbligatori per ogni tipo di azione di scadenza quando si crea una regola di gestione del ciclo di vita bucket. Questi campi possono essere modificati dopo la creazione iniziale. Nella seguente tabella vengono visualizzati i campi univoci per ciascun tipo di azione.

Tipo di azione	Campi univoci
NonCurrentVersionExpiration (scadenza versione non attuale)	<ul style="list-style-type: none"><li>• <code>-non-curr-days</code> - Numero di giorni dopo i quali verranno eliminate le versioni non correnti</li><li>• <code>-new-non-curr-versions</code> - Numero di versioni non correnti più recenti da conservare</li></ul>
Scadenza	<ul style="list-style-type: none"><li>• <code>-obj-age-days</code> - Numero di giorni dalla creazione, dopo i quali è possibile eliminare la versione corrente degli oggetti</li><li>• <code>-obj-exp-date</code> - Data specifica in cui gli oggetti devono scadere</li><li>• <code>-expired-obj-del-markers</code> - Pulisci i marcatori di eliminazione degli oggetti</li></ul>
AbortIncompleteMultipartUpload	<ul style="list-style-type: none"><li>• <code>-after-initiation-days</code> - Numero di giorni di avvio, dopo i quali è possibile interrompere il caricamento</li></ul>

Affinché la regola di gestione del ciclo di vita del bucket venga applicata solo a un sottoinsieme specifico di oggetti, gli amministratori devono impostare ciascun filtro durante la creazione della regola. Se questi filtri non vengono impostati durante la creazione della regola, la regola verrà applicata a tutti gli oggetti all'interno del bucket.

Tutti i filtri possono essere modificati dopo la creazione iniziale *tranne* per i seguenti elementi: +

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

#### Fasi

1. Utilizzare `vserver object-store-server bucket lifecycle-management-rule create` comando con campi obbligatori per il tipo di azione di scadenza per creare la regola di gestione del ciclo di vita del bucket.

#### Esempio

Il seguente comando crea una regola di gestione del ciclo di vita del bucket NonCurrentVersionExpiration:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

### Esempio

Il seguente comando crea una regola di gestione del ciclo di vita del bucket di scadenza:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

### Esempio


Il seguente comando crea una regola di gestione del ciclo di vita del bucket AbortIncompleteMultipartUpload:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

### Gestisci le regole di Lifecycle management con System Manager

A partire da ONTAP 9.14.1, è possibile scade S3 oggetti utilizzando Gestione sistema. È possibile aggiungere, modificare ed eliminare regole di Lifecycle management per gli oggetti S3. Inoltre, è possibile importare una regola del ciclo di vita creata per un bucket e utilizzarla per gli oggetti in un altro bucket. È possibile disattivare una regola attiva e attivarla in un secondo momento.

### Aggiungere una regola di gestione del ciclo di vita

1. Fare clic su **Storage > Bucket**.
2. Selezionare il bucket per il quale si desidera specificare la regola di scadenza.
3. Fare clic su  E selezionare **Gestisci regole del ciclo di vita**.
4. Fare clic su **Aggiungi > regola ciclo di vita**.
5. Nella pagina Add a Lifecycle rule (Aggiungi una regola del ciclo di vita), aggiungere il nome della regola.

6. Definire l'ambito della regola, se si desidera che venga applicata a tutti gli oggetti nel bucket o a oggetti specifici. Se si desidera specificare gli oggetti, aggiungere almeno uno dei seguenti criteri di filtro:
  - a. **Prefix (prefisso):** Specificare un prefisso dei nomi delle chiavi dell'oggetto a cui applicare la regola. In genere si tratta del percorso o della cartella dell'oggetto. È possibile immettere un prefisso per regola. A meno che non venga fornito un prefisso valido, la regola si applica a tutti gli oggetti in un bucket.
  - b. **Tag:** Specificare fino a tre coppie chiave e valore (tag) per gli oggetti a cui la regola deve essere applicata. Per il filtraggio vengono utilizzate solo chiavi valide. Il valore è facoltativo. Tuttavia, se si aggiungono valori, assicurarsi di aggiungere solo valori validi per le chiavi corrispondenti.
  - c. **Dimensioni:** È possibile limitare l'ambito tra le dimensioni minime e massime degli oggetti. È possibile immettere uno o entrambi i valori. L'unità predefinita è MiB.
7. Specificare l'azione:
  - a. **Scade la versione corrente degli oggetti:** Impostare una regola per rendere tutti gli oggetti correnti permanentemente non disponibili dopo un numero specifico di giorni dalla loro creazione o in una data specifica. Questa opzione non è disponibile se è selezionata l'opzione **Elimina marcatori eliminazione oggetto scaduto**.
  - b. **Eliminare definitivamente le versioni non correnti:** Specificare il numero di giorni dopo il quale la versione diventa non corrente e successivamente può essere eliminata, e il numero di versioni da conservare.
  - c. **Elimina marcatori di eliminazione oggetto scaduto:** Selezionare questa azione per eliminare gli oggetti con marcatori di eliminazione scaduti, ovvero i marcatori di eliminazione senza un oggetto corrente associato.



Questa opzione non è disponibile quando si seleziona l'opzione **scadenza della versione corrente degli oggetti** che elimina automaticamente tutti gli oggetti dopo il periodo di conservazione. Questa opzione diventa anche non disponibile quando si utilizzano i tag degli oggetti per il filtraggio.

- d. **Elimina upload multiparte incompleti:** Consente di impostare il numero di giorni dopo il quale i caricamenti multiparte incompleti devono essere eliminati. Se i caricamenti multiparte in corso non riescono entro il periodo di conservazione specificato, è possibile eliminare i caricamenti multiparte incompleti. Questa opzione diventa non disponibile quando si utilizzano i tag degli oggetti per il filtraggio.
- e. Fare clic su **Save** (Salva).

## Importare una regola del ciclo di vita

1. Fare clic su **Storage > Bucket**.
2. Selezionare il bucket per il quale si desidera importare la regola di scadenza.
3. Fare clic su **:** E selezionare **Gestisci regole del ciclo di vita**.
4. Fare clic su **Aggiungi > Importa una regola**.
5. Selezionare il bucket dal quale si desidera importare la regola. Vengono visualizzate le regole di gestione del ciclo di vita definite per il bucket selezionato.
6. Selezionare la regola che si desidera importare. È possibile selezionare una regola alla volta, mentre la selezione predefinita è la prima regola.
7. Fare clic su **Importa**.

## Modificare, eliminare o disattivare una regola

È possibile modificare solo le azioni di Lifecycle management associate alla regola. Se la regola è stata filtrata con tag Object, le opzioni **Delete Expired Object DELETE Marker** e **Delete incomplete Multipart Uploads** non sono disponibili.

Quando si elimina una regola, tale regola non verrà più applicata agli oggetti precedentemente associati.

1. Fare clic su **Storage > Bucket**.
2. Selezionare il bucket per il quale si desidera modificare, eliminare o disattivare la regola di gestione del ciclo di vita.
3. Fare clic su **:** E selezionare **Gestisci regole del ciclo di vita**.
4. Selezionare la regola richiesta. È possibile modificare e disattivare una regola alla volta. È possibile eliminare più regole contemporaneamente.
5. Selezionare **Modifica**, **Elimina** o **Disabilita** e completare la procedura.

## Creare un utente S3

Per limitare la connettività ai client autorizzati, è necessaria l'autorizzazione dell'utente in tutti gli archivi di oggetti ONTAP.

### Prima di iniziare.

Una macchina virtuale per lo storage abilitata per S3 deve già esistere.

### A proposito di questa attività

A un utente S3 può essere concesso l'accesso a qualsiasi bucket in una VM di storage. Quando si crea un utente S3, vengono generate anche una chiave di accesso e una chiave segreta per l'utente. Devono essere condivisi con l'utente insieme all'FQDN dell'archivio oggetti e al nome del bucket. Con è possibile visualizzare le chiavi di un utente S3 `vserver object-store-server user show` comando.

È possibile concedere autorizzazioni di accesso specifiche agli utenti S3 in un criterio bucket o in un criterio del server di oggetti.



Quando si crea un nuovo server archivio oggetti, ONTAP crea un utente root (UID 0), che è un utente con privilegi con accesso a tutti i bucket. Invece di amministrare ONTAP S3 come utente root, NetApp consiglia di creare un ruolo di utente amministratore con privilegi specifici.

## CLI

### 1. Creare un utente S3:

```
vserver object-store-server user create -vserver svm_name -user user_name  
-comment [-comment text] -key-time-to-live time
```

- L'aggiunta di un commento è facoltativa.
- A partire da ONTAP 9.14.1, è possibile definire il periodo di validità della chiave in `-key-time-to-live` parametro. È possibile aggiungere il periodo di conservazione in questo formato, per indicare il periodo dopo il quale la chiave di accesso scade:

`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`


Ad esempio, se si desidera immettere un periodo di conservazione di un giorno, due ore, tre minuti e quattro secondi, immettere il valore come `P1DT2H3M4S`. Se non specificato, la chiave è valida per un periodo di tempo indeterminato.

Nell'esempio riportato di seguito viene creato un utente con nome `sm_user1` Sulla VM di storage `vs0`, con un periodo di conservazione della chiave di una settimana.

```
vserver object-store-server user create -vserver vs0 -user sm_user1  
-key-time-to-live P1W
```

- ### 2. Assicurarsi di salvare la chiave di accesso e la chiave segreta. Saranno richiesti per l'accesso da S3 client.

## System Manager

1. Fare clic su **Storage > Storage VM** (Storage > Storage VM). Selezionare la VM di archiviazione a cui si desidera aggiungere un utente, selezionare **Impostazioni** e fare clic su  Sotto S3.
2. Per aggiungere un utente, fare clic su **utenti > Aggiungi**.
3. Immettere un nome per l'utente.
4. A partire da ONTAP 9.14.1, è possibile specificare il periodo di conservazione delle chiavi di accesso create per l'utente. È possibile specificare il periodo di conservazione in giorni, ore, minuti o secondi, dopo il quale le chiavi scadono automaticamente. Per impostazione predefinita, il valore è impostato su 0 ciò indica che la chiave è valida a tempo indeterminato.
5. Fare clic su **Save** (Salva). L'utente viene creato e vengono generate una chiave di accesso e una chiave segreta per l'utente.
6. Scaricare o salvare la chiave di accesso e la chiave segreta. Saranno richiesti per l'accesso da S3 client.

## Passi successivi

- [Creare o modificare gruppi S3](#)

## Creare o modificare gruppi S3

È possibile semplificare l'accesso bucket creando gruppi di utenti con autorizzazioni di accesso appropriate.

## Prima di iniziare



Gli utenti S3 in una SVM abilitata per S3 devono già esistere.

### A proposito di questa attività

Gli utenti di un gruppo S3 possono avere accesso a qualsiasi bucket di una SVM, ma non a più SVM. Le autorizzazioni di accesso al gruppo possono essere configurate in due modi:


- A livello di benna

Dopo aver creato un gruppo di utenti S3, specificare le autorizzazioni di gruppo nelle istruzioni dei criteri bucket e applicarle solo a quel bucket.

- A livello di SVM

Dopo aver creato un gruppo di utenti S3, specificare i nomi dei criteri del server di oggetti nella definizione di gruppo. Tali policy determinano i bucket e l'accesso per i membri del gruppo.

### System Manager

1. Modificare la VM di storage: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.
2. Aggiungere un gruppo: Selezionare **gruppi**, quindi selezionare **Aggiungi**.
3. Immettere un nome di gruppo e selezionarlo da un elenco di utenti.
4. È possibile selezionare un criterio di gruppo esistente o aggiungerne uno ora oppure aggiungerne uno in un secondo momento.

### CLI

1. Creare un gruppo S3:  

```
vserver object-store-server group create -vserver svm_name -name group_name  
-users user_name\(\s\) [-policies policy_names] [-comment text\]\`Il \`-  
policies
```

l'opzione può essere omessa nelle configurazioni con un solo bucket in un archivio di oggetti; il nome del gruppo può essere aggiunto al criterio bucket. Il `-policies` l'opzione può essere aggiunta in seguito con `vserver object-store-server group modify` comando dopo la creazione dei criteri del server di storage a oggetti.

### Rigenerare le chiavi e modificarne il periodo di conservazione

Le chiavi di accesso e le chiavi segrete vengono generate automaticamente durante la creazione dell'utente per abilitare l'accesso client S3. È possibile rigenerare le chiavi di un utente se una chiave è scaduta o compromessa.

Per informazioni sulla generazione delle chiavi di accesso, vedere ["Creare un utente S3"](#).



## CLI

1. Rigenerare le chiavi di accesso e segrete di un utente eseguendo `vserver object-store-server user regenerate-keys` comando.
2. Per impostazione predefinita, le chiavi generate sono valide a tempo indeterminato. A partire da 9.14.1, è possibile modificare il periodo di conservazione, dopo il quale le chiavi scadono automaticamente. È possibile aggiungere il periodo di conservazione in questo formato:  
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`  
Ad esempio, se si desidera immettere un periodo di conservazione di un giorno, due ore, tre minuti e quattro secondi, immettere il valore come `P1DT2H3M4S`.

```
vserver object-store-server user regenerate-keys -vserver svm_name  
-user user -key-time-to-live 0
```

3. Salvare le chiavi di accesso e le chiavi segrete. Saranno richiesti per l'accesso da S3 client.

## System Manager

1. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
2. Nella scheda **Impostazioni**, fare clic su  Nel riquadro **S3**.
3. Nella scheda **utenti**, verificare che non vi sia alcuna chiave di accesso o che la chiave sia scaduta per l'utente.
4. Se si desidera rigenerare la chiave, fare clic su  Accanto all'utente, quindi fare clic su **Rigenera chiave**.
5. Per impostazione predefinita, le chiavi generate sono valide per un periodo di tempo indefinito. A partire da 9.14.1, è possibile modificare il periodo di conservazione, dopo il quale le chiavi scadono automaticamente. Immettere il periodo di conservazione in giorni, ore, minuti o secondi.
6. Fare clic su **Save** (Salva). La chiave viene rigenerata. Qualsiasi modifica del periodo di conservazione della chiave ha effetto immediato.
7. Scaricare o salvare la chiave di accesso e la chiave segreta. Saranno richiesti per l'accesso da S3 client.

## Creare o modificare le dichiarazioni dei criteri di accesso

### Informazioni sulle policy dei server bucket e degli archivi di oggetti

L'accesso degli utenti e dei gruppi alle risorse S3 è controllato dalle policy del server bucket e dell'archivio di oggetti. Se si dispone di un numero limitato di utenti o gruppi, probabilmente è sufficiente controllare l'accesso a livello di bucket, ma se si dispone di molti utenti e gruppi, è più semplice controllare l'accesso a livello di server dell'archivio di oggetti.

### Modificare una policy bucket

È possibile aggiungere regole di accesso al criterio bucket predefinito. L'ambito del controllo degli accessi è il bucket contenente, quindi è più appropriato quando è presente

un singolo bucket.

### **Prima di iniziare**

Una VM di storage abilitata per S3 contenente un server S3 e un bucket deve già esistere.

Prima di concedere le autorizzazioni, è necessario aver già creato utenti o gruppi.

### **A proposito di questa attività**

È possibile aggiungere nuove istruzioni per nuovi utenti e gruppi oppure modificare gli attributi delle istruzioni esistenti. Per ulteriori opzioni, vedere `vserver object-store-server bucket policy` pagine man.

Le autorizzazioni per utenti e gruppi possono essere concesse al momento della creazione del bucket o in seguito in base alle necessità. È inoltre possibile modificare la capacità del bucket e l'assegnazione del gruppo di policy QoS.

A partire da ONTAP 9.9.1, se si prevede di supportare la funzionalità di tagging degli oggetti client AWS con il server ONTAP S3, le azioni `GetObjectTagging`, `PutObjectTagging`, e `DeleteObjectTagging` devono essere consentite utilizzando le policy di gruppo o bucket.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

### Fasi

1. Modificare il bucket: Fare clic su **Storage > Bucket**, fare clic sul bucket desiderato, quindi su **Edit** (Modifica). Quando si aggiungono o modificano le autorizzazioni, è possibile specificare i seguenti parametri:

- **Principal:** L'utente o il gruppo a cui viene concesso l'accesso.
- **Effect:** Consente o nega l'accesso a un utente o a un gruppo.
- **Azioni:** Azioni consentite nel bucket per un dato utente o gruppo.
- **Resources:** Percorsi e nomi degli oggetti all'interno del bucket per i quali viene concesso o negato l'accesso.

I valori predefiniti **bucketname** e **bucketname/\*** concedono l'accesso a tutti gli oggetti nel bucket. È inoltre possibile concedere l'accesso a singoli oggetti, ad esempio **nome\_carico di lavoro/\*\_readme.txt**.

- **Condizioni** (opzionale): Espressioni che vengono valutate al tentativo di accesso. Ad esempio, è possibile specificare un elenco di indirizzi IP per i quali l'accesso verrà consentito o negato.



A partire da ONTAP 9.14.1, è possibile specificare le variabili per il criterio bucket nel campo **risorse**. Queste variabili sono segnaposto che vengono sostituiti con valori contestuali quando il criterio viene valutato. Ad esempio, se `${aws:username}` viene specificata come variabile per un criterio, quindi questa variabile viene sostituita con il nome utente del contesto della richiesta e l'azione del criterio può essere eseguita come configurato per quell'utente.

### CLI

#### Fasi

1. Aggiungere una dichiarazione a una policy bucket:

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid  
text] [-index integer]
```

I seguenti parametri definiscono le autorizzazioni di accesso:

-effect	L'istruzione può consentire o negare l'accesso
-action	È possibile specificare * per tutte le azioni o un elenco di una o più delle seguenti azioni: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, e. ListMultipartUploadParts.

-principal	<p>Un elenco di uno o più utenti o gruppi S3.</p> <ul style="list-style-type: none"> <li>• È possibile specificare un massimo di 10 utenti o gruppi.</li> <li>• Se viene specificato un gruppo S3, deve essere nel modulo <code>group/group_name</code>.</li> <li>• * può essere specificato per indicare l'accesso pubblico, ovvero l'accesso senza chiave di accesso e chiave segreta.</li> <li>• Se non viene specificato alcun principal, a tutti gli utenti S3 nella VM di storage viene concesso l'accesso.</li> </ul>
-resource	<p>Il bucket e qualsiasi oggetto in esso contenuto. I caratteri jolly * e . ? può essere utilizzato per formare un'espressione regolare per specificare una risorsa. Per una risorsa, è possibile specificare le variabili in un criterio. Si tratta di variabili dei criteri, che vengono sostituite con i valori contestuali al momento della valutazione del criterio.</p>

È possibile specificare una stringa di testo come commento con `-sid` opzione.

## Esempi

Nell'esempio seguente viene creata un'istruzione del criterio del bucket del server di archiviazione oggetti per la VM di archiviazione `svm1.example.com` e `bucket1` che specifica l'accesso consentito a una cartella `Leggimi` per l'utente del server di archiviazione oggetti `user1`.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

Nell'esempio seguente viene creata un'istruzione dei criteri del bucket server di archivio oggetti per la VM di storage `svm1.example.com` e `bucket1` che specifica l'accesso consentito a tutti gli oggetti per il gruppo di server di archivio oggetti `group1`.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

A partire da ONTAP 9.14.1, è possibile specificare le variabili per un criterio bucket. Nell'esempio seguente viene creata un'istruzione del criterio bucket server per la VM di storage `svm1` e `bucket1`, e specifica `${aws:username}` come variabile per una risorsa di criterio. Quando il criterio viene valutato, la variabile di criterio viene sostituita con il nome utente del contesto della richiesta e l'azione del criterio può essere eseguita come configurato per quell'utente. Ad esempio, quando viene valutata la seguente istruzione di criterio, `${aws:username}` Viene sostituito con l'utente che esegue l'operazione S3. Se un utente `user1` esegue l'operazione, a cui l'utente può accedere `bucket1` come `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver  
svml -bucket bucket1 -effect allow -action * -principal - -resource  
bucket1,bucket1/${aws:username}/*##
```

## Creare o modificare un criterio del server di archiviazione oggetti

È possibile creare policy applicabili a uno o più bucket in un archivio di oggetti. È possibile collegare le policy del server dell'archivio di oggetti a gruppi di utenti, semplificando in tal modo la gestione dell'accesso alle risorse in più bucket.

### Prima di iniziare

Una SVM abilitata per S3 contenente un server S3 e un bucket deve già esistere.

### A proposito di questa attività

È possibile attivare i criteri di accesso a livello di SVM specificando un criterio predefinito o personalizzato in un gruppo di server di storage a oggetti. I criteri non hanno effetto fino a quando non vengono specificati nella definizione di gruppo.



Quando si utilizzano i criteri del server di storage a oggetti, si specificano le entità (ovvero utenti e gruppi) nella definizione di gruppo, non nel criterio stesso.

Esistono tre criteri predefiniti di sola lettura per l'accesso alle risorse di ONTAP S3:

- Accesso completo
- NoS3Accesso
- ReadOnlyAccess

È inoltre possibile creare nuovi criteri personalizzati, quindi aggiungere nuove istruzioni per nuovi utenti e gruppi oppure modificare gli attributi delle istruzioni esistenti. Per ulteriori opzioni, vedere `vserver object-store-server policy` ["riferimento al comando"](#).


A partire da ONTAP 9.9.1, se si prevede di supportare la funzionalità di tagging degli oggetti client AWS con il server ONTAP S3, le azioni `GetObjectTagging`, `PutObjectTagging`, e `DeleteObjectTagging` devono essere consentite utilizzando le policy di gruppo o bucket.

La procedura da seguire dipende dall'interfaccia in uso - System Manager o CLI:

## System Manager

### Utilizzare System Manager per creare o modificare un criterio del server archivio oggetti

#### Fasi

1. Modificare la VM di storage: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.
2. Aggiungere un utente: Fare clic su **Policies**, quindi su **Add**.
  - a. Inserire un nome di policy e selezionarlo da un elenco di gruppi.
  - b. Selezionare un criterio predefinito esistente o aggiungerne uno nuovo.

Quando si aggiunge o si modifica un criterio di gruppo, è possibile specificare i seguenti parametri:

- **Group (Gruppo):** I gruppi ai quali viene concesso l'accesso.
- **Effetto:** Consente o nega l'accesso a uno o più gruppi.
- **Azioni:** Azioni consentite in uno o più bucket per un dato gruppo.
- **Resources (risorse):** Percorsi e nomi di oggetti all'interno di uno o più bucket per i quali l'accesso viene concesso o negato. Ad esempio:
  - \* Garantisce l'accesso a tutti i bucket nella VM di storage.
  - **bucketname e bucketname/\*** concedono l'accesso a tutti gli oggetti in un bucket specifico.
  - **bucketname/readme.txt** concede l'accesso a un oggetto in un bucket specifico.
- c. Se lo si desidera, aggiungere le istruzioni ai criteri esistenti.

#### CLI

### Utilizzare la CLI per creare o modificare un criterio del server archivio oggetti

#### Fasi

1. Creare un criterio del server di storage a oggetti:

```
vserver object-store-server policy create -vserver svm_name -policy policy_name [-comment text]
```

2. Creare un'istruzione per la policy:

```
vserver object-store-server policy statement create -vserver svm_name -policy policy_name -effect {allow|deny} -action object_store_actions -resource object_store_resources [-sid text]
```

I seguenti parametri definiscono le autorizzazioni di accesso:

-effect	L'istruzione può consentire o negare l'accesso
---------	--

-action	È possibile specificare * per tutte le azioni o un elenco di una o più delle seguenti azioni: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads, e. ListMultipartUploadParts.
-resource	Il bucket e qualsiasi oggetto in esso contenuto. I caratteri jolly * e. ? può essere utilizzato per formare un'espressione regolare per specificare una risorsa.

È possibile specificare una stringa di testo come commento con -sid opzione.

Per impostazione predefinita, le nuove dichiarazioni vengono aggiunte alla fine dell'elenco delle dichiarazioni, che vengono elaborate in ordine. Quando si aggiungono o modificano le dichiarazioni in un secondo momento, è possibile modificarle -index impostazione per modificare l'ordine di elaborazione.

## Configurare l'accesso S3 per i servizi di directory esterni

A partire da ONTAP 9.14.1, i servizi per le directory esterne sono stati integrati con lo storage a oggetti ONTAP S3. Questa integrazione semplifica la gestione degli utenti e degli accessi tramite servizi di directory esterni.

È possibile fornire ai gruppi utente appartenenti a un servizio di directory esterno l'accesso all'ambiente di storage a oggetti ONTAP. LDAP (Lightweight Directory Access Protocol) è un'interfaccia per la comunicazione con i servizi di directory, come Active Directory, che forniscono un database e servizi per la gestione delle identità e degli accessi (IAM). Per fornire l'accesso, è necessario configurare i gruppi LDAP nell'ambiente ONTAP S3. Dopo aver configurato l'accesso, i membri del gruppo dispongono delle autorizzazioni per i bucket di ONTAP S3. Per informazioni su LDAP, vedere ["Panoramica sull'utilizzo di LDAP"](#).

È inoltre possibile configurare i gruppi di utenti di Active Directory per la modalità di associazione rapida, in modo che le credenziali utente possano essere convalidate e le applicazioni S3 di terze parti e open-source possano essere autenticate tramite connessioni LDAP.

### Prima di iniziare

Prima di configurare i gruppi LDAP e attivare la modalità di associazione rapida per l'accesso ai gruppi, verificare quanto segue:

1. È stata creata una macchina virtuale di storage abilitata per S3 contenente un server S3. Vedere ["Creare una SVM per S3"](#).
2. È stato creato un bucket in quella VM per lo storage. Vedere ["Creare un bucket"](#).
3. Il DNS è configurato sulla macchina virtuale di storage. Vedere ["Configurare i servizi DNS"](#).
4. Sulla VM di storage viene installato un certificato CA (root Certification Authority) autofirmato del server LDAP. Vedere ["Installare il certificato della CA principale autofirmato su SVM"](#).
5. Un client LDAP è configurato con TLS attivato nella SVM. Vedere ["Creare una configurazione del client"](#).



LDAP" e. ["Associare la configurazione del client LDAP alle SVM per ottenere informazioni"](#).

### Configurare l'accesso S3 per i servizi di directory esterni

1. Specificare LDAP come *name service database* della SVM per il gruppo e la password per LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Per ulteriori informazioni su questo comando, vedere ["modifica del ns-switch del name service dei servizi vserver"](#) comando.

2. Creare un'istruzione del criterio del bucket dell'archivio oggetti con il `principal` Impostare sul gruppo LDAP a cui si desidera concedere l'accesso:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

Esempio: Nell'esempio seguente viene creata un'istruzione criterio bucket per `buck1`. Il criterio consente l'accesso al gruppo LDAP `group1` alla risorsa (bucket e relativi oggetti) `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
ListBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verificare che un utente del gruppo LDAP `group1` È in grado di eseguire operazioni S3 dal client S3.

### Utilizzare la modalità di associazione rapida LDAP per l'autenticazione

1. Specificare LDAP come *name service database* della SVM per il gruppo e la password per LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Per ulteriori informazioni su questo comando, vedere ["modifica del ns-switch del name service dei servizi vserver"](#) comando.

2. Assicurarsi che un utente LDAP che accede al bucket S3 disponga delle autorizzazioni definite nei criteri bucket. Per ulteriori informazioni, vedere ["Modificare una policy bucket"](#).
3. Verificare che un utente del gruppo LDAP possa eseguire le seguenti operazioni:
  - a. Configurare la chiave di accesso sul client S3 in questo formato:  
`"NTAPFASTBIND" + base64-encode(user-name:password)`  
Esempio: `"NTAPFASTBIND" + base64-encode(ldapuser:password)`, che risulta in  
`NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`



Il client S3 potrebbe richiedere una chiave segreta. In assenza di una chiave segreta, è possibile immettere qualsiasi password di almeno 16 caratteri.

- b. Eseguire operazioni S3 di base dal client S3 per cui l'utente dispone delle autorizzazioni.

### Consentire agli utenti LDAP o di dominio di generare le proprie chiavi di accesso S3

A partire da ONTAP 9.14.1, in qualità di amministratore ONTAP, è possibile creare ruoli personalizzati e concederli a gruppi locali o di dominio o a gruppi LDAP (Lightweight Directory Access Protocol), in modo che gli utenti appartenenti a tali gruppi possano generare le proprie chiavi di accesso e segrete per l'accesso client S3.

Devi eseguire alcuni passaggi di configurazione sulla macchina virtuale di storage, in modo che sia possibile creare e assegnare il ruolo personalizzato all'utente che richiama l'API per la generazione delle chiavi di accesso.

#### Prima di iniziare

Verificare quanto segue:

1. È stata creata una macchina virtuale di storage abilitata per S3 contenente un server S3. Vedere ["Creare una SVM per S3"](#).
2. È stato creato un bucket in quella VM per lo storage. Vedere ["Creare un bucket"](#).
3. Il DNS è configurato sulla macchina virtuale di storage. Vedere ["Configurare i servizi DNS"](#).
4. Sulla VM di storage viene installato un certificato CA (root Certification Authority) autofirmato del server LDAP. Vedere ["Installare il certificato della CA principale autofirmato su SVM"](#).
5. Un client LDAP è configurato con TLS attivato sulla macchina virtuale di storage. Vedere ["Creare una configurazione del client LDAP"](#) e .
6. Associare la configurazione del client al Vserver. Vedere ["Associare la configurazione del client LDAP alle SVM"](#) e ["creazione ldap del nome del servizio vserver"](#).
7. Se stai utilizzando una macchina virtuale per lo storage dei dati, crea un'interfaccia di rete di gestione (LIF) e una macchina virtuale, oltre a una policy di servizio per la LIF. Vedere ["creazione dell'interfaccia di rete"](#) e ["creazione della politica di servizio dell'interfaccia di rete"](#) comandi.

#### Configurare gli utenti per la generazione delle chiavi di accesso

1. Specificare LDAP come *name service database* della VM di archiviazione per il gruppo e la password per LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources  
files,ldap  
ns-switch modify -vserver <vserver-name> -database passwd -sources  
files,ldap
```

Per ulteriori informazioni su questo comando, vedere ["modifica del ns-switch del name service dei servizi vserver"](#) comando.

2. Creare un ruolo personalizzato con accesso all'endpoint API REST per S3 utenti:

```
security login rest-role create -vserver <vserver-name> -role <custom-role-  
name> -api "/api/protocols/s3/services/*/users" -access <access-type>
```

In questo esempio, il `s3-role` Viene generato un ruolo per gli utenti sulla VM di storage `svm-1`, a cui vengono concessi tutti i diritti di accesso, lettura, creazione e aggiornamento.

```
security login rest-role create -vserver svm-1 -role s3role -api  
"/api/protocols/s3/services/*/users" -access all
```

Per ulteriori informazioni su questo comando, vedere ["accesso di sicurezza creazione ruolo di pausa"](#) comando.

3. Creare un gruppo di utenti LDAP con il comando di accesso alla sicurezza e aggiungere il nuovo ruolo personalizzato per accedere all'endpoint dell'API REST utente S3. Per ulteriori informazioni su questo comando, vedere ["creazione dell'accesso di sicurezza"](#) comando.

```
security login create -user-or-group-name <ldap-group-name> -application  
http -authentication-method nsswitch -role <custom-role-name> -is-ns  
-switch-group yes
```

In questo esempio, il gruppo LDAP `ldap-group-1` viene creato in `svm-1` e il ruolo personalizzato `s3role` Viene aggiunto per accedere all'endpoint API, oltre ad abilitare l'accesso LDAP in modalità di associazione rapida.

```
security login create -user-or-group-name ldap-group-1 -application http  
-authentication-method nsswitch -role s3role -is-ns-switch-group yes  
-second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
```

Per ulteriori informazioni, vedere ["Utilizza il binding rapido LDAP per l'autenticazione nsswitch"](#).

L'aggiunta del ruolo personalizzato al dominio o al gruppo LDAP consente agli utenti di quel gruppo di accedere in modo limitato a ONTAP `/api/protocols/s3/services/{svm.uid}/users` endpoint. Richiamando l'API, gli utenti del dominio o del gruppo LDAP possono generare il proprio accesso e le proprie chiavi segrete per accedere al client S3. Possono generare le chiavi solo per se stessi e non per altri utenti.

### Come utente S3 o LDAP, generare le proprie chiavi di accesso

A partire da ONTAP 9.14.1, è possibile generare le proprie chiavi di accesso e segrete per l'accesso ai client S3, se l'amministratore ha concesso il ruolo di generazione delle proprie chiavi. Puoi generare le chiavi solo per te utilizzando il seguente endpoint dell'API REST ONTAP.

#### Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti. Per informazioni sugli altri metodi di questo endpoint, vedere il riferimento ["Documentazione API"](#).

Metodo HTTP	Percorso
POST	/api/protocolli/s3/servizi/{svm.uuid}/utenti

#### Esempio di arricciamento

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name": "_name_"}'
```

## Esempio di output JSON

```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```

## Abilitare l'accesso del client allo storage a oggetti S3

### Abilitare l'accesso ONTAP S3 per il tiering FabricPool remoto

Per utilizzare ONTAP S3 come Tier di capacità FabricPool remota (cloud), l'amministratore di ONTAP S3 deve fornire informazioni sulla configurazione del server S3 all'amministratore remoto del cluster ONTAP.

#### A proposito di questa attività

Per configurare i livelli cloud FabricPool sono necessarie le seguenti informazioni sul server S3:

- Nome server (FQDN)
- nome bucket
- Certificato CA
- tasto di accesso
- password (chiave di accesso segreta)

Inoltre, è necessaria la seguente configurazione di rete:

- Nel server DNS configurato per la SVM amministrativa deve essere presente una voce per il nome host del server ONTAP S3 remoto, compreso il nome FQDN del server S3 e gli indirizzi IP sui relativi LIF.

- Le LIF di intercluster devono essere configurate sul cluster locale, anche se non è richiesto il peering del cluster.

Consultare la documentazione di FabricPool sulla configurazione di ONTAP S3 come Tier cloud.

## "Gestione dei Tier di storage mediante FabricPool"

### Abilitare l'accesso ONTAP S3 per il tiering FabricPool locale

Per utilizzare ONTAP S3 come Tier di capacità FabricPool locale, è necessario definire un archivio di oggetti in base al bucket creato e quindi associare l'archivio di oggetti a un aggregato di Tier di performance per creare un FabricPool.

#### Prima di iniziare

È necessario disporre del nome del server ONTAP S3 e del nome del bucket e il server S3 deve essere stato creato utilizzando le LIF del cluster (con `-vserver Cluster` parametro).

#### A proposito di questa attività

La configurazione dell'archivio di oggetti contiene informazioni sul Tier di capacità locale, inclusi i nomi dei server S3 e dei bucket e i requisiti di autenticazione.

Una volta creata, la configurazione di un archivio di oggetti non deve essere riassociata a un altro archivio di oggetti o bucket. È possibile creare più bucket per i Tier locali, ma non è possibile creare più archivi di oggetti in un singolo bucket.

Non è richiesta una licenza FabricPool per un livello di capacità locale.

#### Fasi

1. Creare l'archivio di oggetti per il livello di capacità locale:

```
storage aggregate object-store config create -object-store-name store_name
-ipospace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
-name bucket_name -access-key access_key -secret-password password
```

- Il `-container-name` È il bucket S3 creato.
- Il `-access-key` Il parametro autorizza le richieste al server ONTAP S3.
- Il `-secret-password` Il parametro (chiave di accesso segreta) autentica le richieste al server ONTAP S3.
- È possibile impostare `-is-certificate-validation-enabled` parametro a `false` Per disattivare il controllo dei certificati per ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipospace Cluster -provider-type
ONTAP_S3 -server s3.example.com
-container-name bucket1 -access-key myS3key -secret-password myS3pass
```

2. Visualizzare e verificare le informazioni di configurazione dell'archivio di oggetti:

```
storage aggregate object-store config show
```

3. Facoltativo: Per verificare la quantità di dati inattivi in un volume, seguire la procedura descritta in ["Determinare la quantità di dati inattivi in un volume utilizzando il reporting dei dati inattivi"](#).

La visualizzazione della quantità di dati inattivi in un volume consente di decidere quale aggregato utilizzare per il tiering locale di FabricPool.

4. Collegare l'archivio di oggetti a un aggregato:

```
storage aggregate object-store attach -aggregate aggr_name -object-store-name store_name
```

È possibile utilizzare `allow-flexgroup true` Possibilità di collegare aggregati che contengono componenti del volume FlexGroup.

```
cluster1::> storage aggregate object-store attach  
-aggregate aggr1 -object-store-name MyLocalObjStore
```

5. Visualizzare le informazioni sull'archivio di oggetti e verificare che l'archivio di oggetti collegato sia disponibile:

```
storage aggregate object-store show
```

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability State
-----	-----	-----
aggr1	MyLocalObjStore	available

## Abilitare l'accesso client da un'applicazione S3

Affinché le applicazioni client S3 possano accedere al server ONTAP S3, l'amministratore di ONTAP S3 deve fornire le informazioni di configurazione all'utente S3.

### Prima di iniziare

L'applicazione client S3 deve essere in grado di eseguire l'autenticazione con il server ONTAP S3 utilizzando le seguenti versioni delle firme AWS:

- Signature versione 4, ONTAP 9.8 e versioni successive
- Signature versione 2, ONTAP 9.11.1 e versioni successive

ONTAP S3 non supporta altre versioni delle firme.

L'amministratore di ONTAP S3 deve aver creato gli utenti S3 e concesso loro le autorizzazioni di accesso, come singoli utenti o come membro di gruppo, nella policy del bucket o nella policy del server di storage a oggetti.

L'applicazione client S3 deve essere in grado di risolvere il nome del server ONTAP S3, il che richiede che l'amministratore di ONTAP S3 fornisca il nome del server S3 (FQDN) e gli indirizzi IP per le LIF del server S3.

**A proposito di questa attività**

Per accedere a un bucket ONTAP S3, un utente dell'applicazione client S3 inserisce le informazioni fornite dall'amministratore di ONTAP S3.

A partire da ONTAP 9.9.1, il server ONTAP S3 supporta le seguenti funzionalità del client AWS:

- metadati degli oggetti definiti dall'utente

Un insieme di coppie chiave-valore può essere assegnato agli oggetti come metadati quando vengono creati usando PUT (o POST). Quando viene eseguita un'operazione GET/HEAD sull'oggetto, i metadati definiti dall'utente vengono restituiti insieme ai metadati di sistema.

- tagging degli oggetti

È possibile assegnare un insieme separato di coppie chiave-valore come tag per la classificazione degli oggetti. A differenza dei metadati, i tag vengono creati e letti con API REST indipendentemente dall'oggetto e implementati quando gli oggetti vengono creati o in qualsiasi momento.



Per consentire ai client di ottenere e inserire informazioni di tagging, le azioni `GetObjectTagging`, `PutObjectTagging`, e `DeleteObjectTagging` devono essere consentite utilizzando le policy di gruppo o bucket.

Per ulteriori informazioni, consultare la documentazione di AWS S3.

**Fasi**

1. Autenticare l'applicazione client S3 con il server ONTAP S3 immettendo il nome del server S3 e il certificato CA.
2. Autenticare un utente sull'applicazione client S3 inserendo le seguenti informazioni:
  - Nome server S3 (FQDN) e nome bucket
  - la chiave di accesso e la chiave segreta dell'utente

**Definizioni dei servizi di storage**

ONTAP include servizi di storage predefiniti mappati ai corrispondenti fattori di performance minimi.

L'insieme effettivo di servizi storage disponibili in un cluster o SVM è determinato dal tipo di storage che costituisce un aggregato nella SVM.

La seguente tabella mostra come i fattori minimi di performance sono mappati ai servizi di storage predefiniti:

Servizio di storage	IOPS previsti (SLA)	IOPS di picco (SLO)	Volume minimo IOPS	Latenza stimata	Gli IOPS previsti sono applicati?
valore	128 per TB	512 per TB	75	17 ms.	Su AFF: Sì Altrimenti: No
performance	2048 per TB	4096 per TB	500	2 ms.	Sì



Servizio di storage	IOPS previsti (SLA)	IOPS di picco (SLO)	Volume minimo IOPS	Latenza stimata	Gli IOPS previsti sono applicati?
estremo	6144 per TB	12288 per TB	1000	1 ms.	Sì

La seguente tabella definisce il livello di servizio dello storage disponibile per ciascun tipo di supporto o nodo:

Media o nodo	Livello di servizio dello storage disponibile
Disco	valore
Disco della macchina virtuale	valore
LUN FlexArray	valore
Ibrido	valore
Flash ottimizzato per la capacità	valore
Solid-state Drive (SSD) - non AFF	valore
Flash ottimizzata per le performance - SSD (AFF)	estremi, performance, valore

## Proteggi i bucket con S3 SnapMirror

### Panoramica di S3 SnapMirror

A partire da ONTAP 9.10.1, puoi proteggere i bucket in archivi di oggetti ONTAP S3 usando la funzionalità di mirroring e backup di SnapMirror. A differenza di SnapMirror standard, S3 SnapMirror consente il mirroring e i backup in destinazioni non NetApp come AWS S3.

S3 SnapMirror supporta mirror attivi e Tier di backup dai bucket ONTAP S3 alle seguenti destinazioni:

Destinazione	Supporta mirror attivi e Takeover?	Supporta backup e ripristino?
ONTAP S3 <ul style="list-style-type: none"> <li>• Bucket nella stessa SVM</li> <li>• Bucket in diverse SVM sullo stesso cluster</li> <li>• Bucket in SVM su cluster diversi</li> </ul>	✓	✓
StorageGRID		✓
AWS S3		✓

Destinazione	Supporta mirror attivi e Takeover?	Supporta backup e ripristino?
Cloud Volumes ONTAP per Azure	✓	✓
Cloud Volumes ONTAP per AWS	✓	✓
Cloud Volumes ONTAP per Google Cloud	✓	✓

È possibile proteggere i bucket esistenti sui server ONTAP S3 o creare nuovi bucket con la protezione dei dati attivata immediatamente.

## Requisiti di S3 SnapMirror

- Versione di ONTAP  
ONTAP 9.10.1 o versione successiva deve essere in esecuzione sui cluster di origine e di destinazione.
- Licenze i seguenti bundle di licenze sono richiesti sui sistemi di origine e destinazione ONTAP:
  - Bundle principale per protocollo e storage ONTAP S3.
  - Bundle per la protezione dei dati per S3 SnapMirror destinato ad altri archivi di oggetti NetApp (ONTAP S3, StorageGRID e Cloud Volumes ONTAP).
  - Bundle di data Protection e bundle cloud ibrido  
Per S3 SnapMirror è destinato ad archivi di oggetti di terze parti, tra cui AWS S3.
- ONTAP S3
  - I server ONTAP S3 devono eseguire SVM di origine e di destinazione.
  - Si consiglia, ma non è obbligatorio, di installare i certificati CA per l'accesso TLS sui sistemi che ospitano server S3.
    - I certificati CA utilizzati per firmare i certificati dei server S3 devono essere installati nella VM di storage amministrativa dei cluster che ospitano server S3.
    - È possibile utilizzare un certificato CA autofirmato o un certificato firmato da un fornitore CA esterno.
    - Se le VM di storage di origine o di destinazione non sono in ascolto su HTTPS, non è necessario installare i certificati CA.
- Peering (per target ONTAP S3)
  - È necessario configurare le LIF di intercluster (per le destinazioni ONTAP remote).
  - I cluster di origine e di destinazione vengono peering (per le destinazioni ONTAP remote).
  - Le VM storage di origine e di destinazione sono in peering (per tutte le destinazioni ONTAP).
- Policy di SnapMirror
  - Per tutte le relazioni di S3 SnapMirror è necessario un criterio SnapMirror specifico di S3, ma è possibile utilizzare lo stesso criterio per più relazioni.
  - È possibile creare un criterio personalizzato o accettare il criterio **continuo** predefinito, che include i seguenti valori:
    - Throttle (limite superiore di throughput/larghezza di banda) - illimitato.
    - Tempo per l'obiettivo del punto di ripristino: 1 ora (3600 secondi).
- Le chiavi utente root Storage VM root sono necessarie per le relazioni S3 SnapMirror; ONTAP non le assegna per impostazione predefinita. La prima volta che si crea una relazione SnapMirror S3, è necessario verificare che le chiavi esistano sia sulle macchine virtuali storage di origine che di destinazione

e rigenerarle in caso contrario. Se è necessario rigenerarli, è necessario assicurarsi che tutti i client e tutte le configurazioni dell'archivio di oggetti SnapMirror che utilizzano la coppia di chiavi di accesso e segrete siano aggiornati con le nuove chiavi.

Per informazioni sulla configurazione del server S3, consultare i seguenti argomenti:

- ["Abilitare un server S3 su una VM di storage"](#)
- ["Informazioni sul processo di configurazione S3"](#)

Per informazioni sul peering delle macchine virtuali di storage e cluster, consultare il seguente argomento:

- ["Preparazione per il mirroring e il vaulting \(System Manager, fasi 1-6\)"](#)
- ["Peering cluster e SVM \(CLI\)"](#)

## **Relazioni SnapMirror supportate**

S3 SnapMirror supporta le relazioni fan-out e cascata. Per una panoramica, vedere ["Implementazioni di protezione dei dati fan-out e cascata"](#).

S3 SnapMirror non supporta le implementazioni fan-in (relazioni di data Protection tra più bucket di origine e un singolo bucket di destinazione). S3 SnapMirror può supportare più mirror bucket da più cluster a un singolo cluster secondario, ma ogni bucket di origine deve avere un proprio bucket di destinazione sul cluster secondario.

## **Controllare l'accesso alle benne S3**

Quando si creano nuovi bucket, è possibile controllare l'accesso creando utenti e gruppi. Per ulteriori informazioni, consulta i seguenti argomenti:

- ["Aggiunta di utenti e gruppi S3 \(System Manager\)"](#)
- ["Creazione di un utente S3 \(CLI\)"](#)
- ["Creare o modificare gruppi S3 \(CLI\)"](#)

## **Protezione del mirroring e del backup su un cluster remoto**

### **Creare una relazione mirror per un nuovo bucket (cluster remoto)**

Quando si creano nuovi bucket S3, è possibile proteggerli immediatamente a una destinazione S3 SnapMirror su un cluster remoto.



### **A proposito di questa attività**


È necessario eseguire attività sui sistemi di origine e di destinazione.

### **Prima di iniziare**


- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra i cluster di origine e di destinazione e esiste una relazione di peering tra le VM di storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

## System Manager

1. Se si tratta della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che di destinazione e rigenerarle in caso contrario:
  - a. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
  - b. Nella scheda **Impostazioni**, fare clic su  Nel riquadro **S3**.
  - c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root.
  - d. In caso contrario, fare clic su  Accanto a **root**, quindi fare clic su **Rigenera chiave**. Non rigenerare la chiave se ne esiste già una.
2. Modificare la VM di storage per aggiungere utenti e utenti ai gruppi, sia nelle VM di storage di origine che di destinazione:

Fare clic su **Storage > Storage VMS**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.

Vedere "[Aggiungere utenti e gruppi S3](#)" per ulteriori informazioni.

3. Nel cluster di origine, creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare il criterio predefinito:
  - a. Fare clic su **protezione > Panoramica**, quindi su **Impostazioni policy locale**.
  - b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
    - Immettere il nome e la descrizione della policy.
    - Selezionare l'ambito del criterio, il cluster o SVM
    - Selezionare **Continuous** per le relazioni di S3 SnapMirror.
    - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Crea un bucket con la protezione SnapMirror:
  - a. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi). La verifica delle autorizzazioni è facoltativa ma consigliata.
  - b. Immettere un nome, selezionare la VM di storage, immettere una dimensione, quindi fare clic su **altre opzioni**.
  - c. In **Permissions**, fare clic su **Add** (Aggiungi).
    - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
    - **Azioni**- assicurarsi che vengano visualizzati i seguenti valori:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Risorse** - utilizzare le impostazioni predefinite (*bucketname*, *bucketname/\**) o altri valori di cui hai bisogno.

Vedere "[Gestire l'accesso degli utenti ai bucket](#)" per ulteriori informazioni su questi campi.

d. In **protezione**, selezionare **attiva SnapMirror (ONTAP o Cloud)**. Quindi, immettere i seguenti valori:

- Destinazione
  - **DESTINAZIONE: Sistema ONTAP**
  - **CLUSTER**: Selezionare il cluster remoto.
  - **STORAGE VM**: Selezionare una storage VM sul cluster remoto.
  - **Certificato CA del SERVER S3**: Copia e incolla il contenuto del certificato *source*.
- Origine
  - **CERTIFICATO CA del SERVER S3**: copiare e incollare il contenuto del certificato *destination*.

5. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
6. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
7. Fare clic su **Save** (Salva). Viene creato un nuovo bucket nella VM per lo storage di origine e viene eseguito il mirroring in un nuovo bucket che viene creato la VM per lo storage di destinazione.

### Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere ["Creare un bucket"](#).

### CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:

```
vserver object-store-server user show
```

Verificare che sia presente una chiave di accesso per l'utente root. In caso contrario, immettere:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Non rigenerare la chiave se ne esiste già una.

2. Creare bucket nelle SVM di origine e di destinazione:

```
vserver object-store-server bucket create -vserver svm_name -bucket
```

```
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Aggiungere regole di accesso alle policy di bucket predefinite nelle SVM di origine e di destinazione:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

**Esempio**

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Nella SVM di origine, crea una policy SnapMirror S3 se non ne hai già una e non vuoi utilizzare la policy predefinita:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

**Parametri:**

- tipo continuous - L'unico tipo di policy per le relazioni SnapMirror S3 (obbligatorio).
- -rpo - specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo).
- -throttle - specifica il limite superiore di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

**Esempio**

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installare i certificati del server CA sulle SVM amministrative dei cluster di origine e di destinazione:

a. Nel cluster di origine, installare il certificato CA che ha firmato il certificato del server S3 *destination*:

```
security certificate install -type server-ca -vserver src_admin_svm
-cert-name dest_server_certificate
```

b. Nel cluster di destinazione, installare il certificato CA che ha firmato il certificato del server S3 *source*:

```
security certificate install -type server-ca -vserver dest_admin_svm
-cert-name src_server_certificate
```

Se si utilizza un certificato firmato da un vendor CA esterno, installare lo stesso certificato sulla SVM amministrativa di origine e destinazione.

Vedere `security certificate install` pagina man per i dettagli.

6. Sulla SVM di origine, creare una relazione SnapMirror S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy  
policy_name]
```

È possibile utilizzare un criterio creato o accettare quello predefinito.

**Esempio**

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy  
test-policy
```

7. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```

**Creare una relazione mirror per un bucket esistente (cluster remoto)**

È possibile iniziare a proteggere i bucket S3 esistenti in qualsiasi momento, ad esempio se è stata aggiornata una configurazione S3 da una release precedente a ONTAP 9.10.1.

**A proposito di questa attività**

Devi eseguire i task sui cluster di origine e destinazione.




**Prima di iniziare**

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra i cluster di origine e di destinazione e esiste una relazione di peering tra le VM di storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.



**Fasi**

È possibile creare una relazione di mirroring utilizzando System Manager o l'interfaccia a riga di comando di ONTAP.

## System Manager

1. Se si tratta della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che di destinazione e rigenerarle in caso contrario:
  - a. Selezionare **Storage > Storage VM**, quindi selezionare la VM di storage.
  - b. Nella scheda **Impostazioni**, fare clic su  Nel riquadro **S3**.
  - c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root.
  - d. In caso contrario, fare clic su  Accanto a **root**, quindi fare clic su **Rigenera chiave**. non rigenerare la chiave se ne esiste già una.
2. Verificare che l'accesso a utenti e gruppi sia corretto sia nelle macchine virtuali storage di origine che di destinazione:  
Selezionare **Storage > Storage VM**, quindi selezionare la VM di archiviazione, quindi **Settings**. Infine, selezionare  Sotto **S3**.

Vedere "[Aggiungere utenti e gruppi S3](#)" per ulteriori informazioni.

3. Nel cluster di origine, creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare il criterio predefinito:
  - a. Selezionare **protezione > Panoramica**, quindi fare clic su **Impostazioni criteri locali**.
  - b. Selezionare  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
  - c. Immettere il nome e la descrizione della policy.
  - d. Selezionare l'ambito del criterio, il cluster o SVM
  - e. Selezionare **Continuous** per le relazioni di S3 SnapMirror.
  - f. Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Verificare che la policy di accesso al bucket del bucket esistente soddisfi ancora le proprie esigenze:
  - a. Fare clic su **Storage > Bucket** (Storage > bucket), quindi selezionare il bucket che si desidera proteggere.
  - b. Nella scheda **Permissions**, fare clic su  **Modifica**, quindi fare clic su **Aggiungi in permessi**.
    - **Principal and Effect** (principale ed effetto): Selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
    - **Azioni**: Verificare che vengano visualizzati i seguenti valori:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Risorse**: Utilizzare le impostazioni predefinite (*bucketname*, *bucketname/\**) o altri valori di cui hai bisogno.

Vedere "[Gestire l'accesso degli utenti ai bucket](#)" per ulteriori informazioni su questi campi.

5. Proteggi un bucket esistente con la protezione di S3 SnapMirror:
  - a. Fare clic su **Storage > Bucket**, quindi selezionare il bucket che si desidera proteggere.
  - b. Fare clic su **Protect** (protezione) e immettere i seguenti valori:



- Destinazione
    - **DESTINAZIONE:** Sistema ONTAP
    - **CLUSTER:** Selezionare il cluster remoto.
    - **STORAGE VM:** Selezionare una storage VM sul cluster remoto.
    - **Certificato CA del SERVER S3:** Copia e incolla il contenuto del certificato *source*.
  - Origine
    - **Certificato CA server S3:** Copia e incolla il contenuto del certificato *destination*.
6. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
  7. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
  8. Fare clic su **Save** (Salva). Viene eseguito il mirroring del bucket esistente in un nuovo bucket nella VM di storage di destinazione.

### Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere ["Creare un bucket"](#).

### CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:

`vserver object-store-server user show+` verificare la presenza di una chiave di accesso per l'utente root. In caso contrario, immettere:

`vserver object-store-server user regenerate-keys -vserver svm_name -user root+` non rigenerare la chiave se ne esiste già una.

2. Creare un bucket sulla SVM di destinazione come destinazione mirror:

```
vserver object-store-server bucket create -vserver svm_name -bucket
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Verificare che le regole di accesso delle policy di bucket predefinite siano corrette sia nelle SVM di origine che di destinazione:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
```

```
text] [-index integer]
```

### Esempio

```
src_cluster::> vserver object-store-server bucket policy add-  
statement -bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc  
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -  
-resource test-bucket, test-bucket /*
```

4. Sulla SVM di origine, creare un criterio S3 SnapMirror se non si dispone di uno esistente e non si desidera utilizzare il criterio predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

### Parametri:

- `continuous` – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio).
- `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo).
- `-throttle` – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

### Esempio

```
src_cluster::> snapmirror policy create -vserver vs0 -type  
continuous -rpo 0 -policy test-policy
```

5. Installare i certificati CA sulle SVM amministrative dei cluster di origine e di destinazione:

- a. Nel cluster di origine, installare il certificato CA che ha firmato il certificato del server S3 *destination*:

```
security certificate install -type server-ca -vserver src_admin_svm  
-cert-name dest_server_certificate
```

- b. Nel cluster di destinazione, installare il certificato CA che ha firmato il certificato del server S3 *source*:

```
security certificate install -type server-ca -vserver dest_admin_svm  
-cert-name src_server_certificate+ se si utilizza un certificato firmato da un vendor CA  
esterno, installare lo stesso certificato sulla SVM amministrativa di origine e destinazione.
```

Vedere `security certificate install` pagina man per i dettagli.

6. Sulla SVM di origine, creare una relazione SnapMirror S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name  
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...] [-policy  
policy_name]
```

È possibile utilizzare un criterio creato o accettare quello predefinito.

### Esempio

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy  
test-policy
```

7. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```

## Acquisizione e distribuzione dei dati dal bucket di destinazione (cluster remoto)

Se i dati in un bucket di origine non sono più disponibili, è possibile interrompere la relazione SnapMirror per rendere il bucket di destinazione scrivibile e iniziare a fornire i dati.

### A proposito di questa attività


Quando viene eseguita un'operazione di Takeover, il bucket di origine viene convertito in sola lettura e il bucket di destinazione originale viene convertito in lettura-scrittura, invertendo così la relazione di S3 SnapMirror.

Quando il bucket di origine disattivato è nuovamente disponibile, S3 SnapMirror risincronizza automaticamente il contenuto dei due bucket. Non è necessario risincronizzare esplicitamente la relazione, come richiesto per le implementazioni di SnapMirror dei volumi.

L'operazione di Takeover deve essere avviata dal cluster remoto.

### System Manager

Eseguire il failover dal bucket non disponibile e iniziare a fornire i dati:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
2. Fare clic su , Selezionare **failover**, quindi fare clic su **failover**.

### CLI

1. Avviare un'operazione di failover per il bucket di destinazione:  

```
snapmirror failover start -destination-path svm_name:/bucket/bucket_name
```
2. Verificare lo stato dell'operazione di failover:  

```
snapmirror show -fields status
```

### Esempio

```
dest_cluster::> snapmirror failover start -destination-path  
dest_svm1:/bucket/test-bucket-mirror
```

## Ripristinare un bucket dalla VM di storage di destinazione (cluster remoto)

In caso di perdita o danneggiamento dei dati in un bucket di origine, sarà possibile

ripopolare i dati ripristinando gli oggetti da un bucket di destinazione.

**A proposito di questa attività**

È possibile ripristinare il bucket di destinazione su un bucket esistente o su un nuovo bucket. Il bucket di destinazione per l'operazione di ripristino deve essere più grande dello spazio utilizzato logico del bucket di destinazione.

Se si utilizza un bucket esistente, questo deve essere vuoto quando si avvia un'operazione di ripristino. Il ripristino non "esegue il rollback" di un bucket nel tempo, ma popola un bucket vuoto con i contenuti precedenti.

L'operazione di ripristino deve essere avviata dal cluster remoto.

## System Manager

Ripristinare i dati di backup:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
2. Fare clic su  Quindi selezionare **Ripristina**.
3. In **Source** (origine), selezionare **Existing Bucket** (bucket esistente) (impostazione predefinita) o **New Bucket** (nuovo bucket).
  - Per ripristinare un **bucket esistente** (impostazione predefinita), completare le seguenti azioni:
    - Selezionare il cluster e la VM di storage per cercare il bucket esistente.
    - Selezionare il bucket esistente.
    - Copiare e incollare il contenuto del certificato CA del server *S3 destination*.
  - Per ripristinare un **nuovo bucket**, immettere i seguenti valori:
    - Il cluster e la VM di storage per ospitare il nuovo bucket.
    - Il nome, la capacità e il livello di servizio delle prestazioni della nuova benna. Vedere "[Livelli di servizio dello storage](#)" per ulteriori informazioni.
    - Il contenuto del certificato CA del server *S3 destination*.
4. In **destinazione**, copiare e incollare il contenuto del certificato CA del server *S3 origine*.
5. Fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

## Ripristinare i bucket bloccati

A partire da ONTAP 9.14.1, puoi eseguire il backup dei bucket bloccati e ripristinarli in base alle necessità.

È possibile ripristinare un bucket object-locked in un bucket nuovo o esistente. È possibile selezionare un bucket a blocco di oggetti come destinazione nei seguenti scenari:

- **Ripristina in un nuovo bucket:** Quando il blocco degli oggetti è attivato, è possibile ripristinare un bucket creando un bucket che ha anche il blocco degli oggetti attivato. Quando si ripristina un bucket bloccato, la modalità di blocco degli oggetti e il periodo di conservazione del bucket originale vengono replicati. È inoltre possibile definire un periodo di blocco diverso per la nuova benna. Questo periodo di conservazione viene applicato a oggetti non bloccati provenienti da altre origini.
- **Ripristina in un bucket esistente:** Un bucket a blocco di oggetti può essere ripristinato in un bucket esistente, purché nel bucket esistente siano attivate la versione e una simile modalità di blocco di oggetti. Viene mantenuto il mantenimento della posizione di ritenzione della benna originale.
- **Restore non-locked bucket:** Anche se il blocco degli oggetti non è abilitato in un bucket, è possibile ripristinarlo in un bucket che ha il blocco degli oggetti attivato e si trova nel cluster di origine. Quando si ripristina il bucket, tutti gli oggetti non bloccati vengono bloccati e la modalità di conservazione e il mantenimento del bucket di destinazione diventano applicabili.

## CLI

1. Creare il nuovo bucket di destinazione per il ripristino. Per ulteriori informazioni, vedere "[Creare una relazione di backup per un nuovo bucket \(target cloud\)](#)".
2. Avviare un'operazione di ripristino per il bucket di destinazione:

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```

### Esempio

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-  
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

## Protezione del mirroring e del backup sul cluster locale




### Creare una relazione mirror per un nuovo bucket (cluster locale)

Quando si creano nuovi bucket S3, è possibile proteggerli immediatamente a una destinazione S3 SnapMirror sullo stesso cluster. È possibile eseguire il mirroring dei dati su un bucket in una VM di storage diversa o nella stessa VM di storage di origine.


#### Prima di iniziare

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra le VM storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

## System Manager

1. Se si tratta della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che di destinazione e rigenerarle in caso contrario:
  - a. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
  - b. Nella scheda **Impostazioni**, fare clic su  Nel riquadro S3.
  - c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root
  - d. In caso contrario, fare clic su  Accanto a **root**, quindi fare clic su **Rigenera chiave**. Non rigenerare la chiave se ne esiste già una.
2. Modificare la VM di storage per aggiungere utenti e utenti ai gruppi, sia nelle VM di storage di origine che di destinazione: Fare clic su **Storage > VM di storage**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.

Vedere ["Aggiungere utenti e gruppi S3"](#) per ulteriori informazioni.

3. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
  - a. Fare clic su **protezione > Panoramica**, quindi fare clic su **Impostazioni criteri locali**.
  - b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
    - Immettere il nome e la descrizione della policy.
    - Selezionare l'ambito del criterio, il cluster o SVM
    - Selezionare **Continuous** per le relazioni di S3 SnapMirror.
    - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Crea un bucket con la protezione SnapMirror:
  - a. Fare clic su **Storage > Bucket** (Storage > bucket), quindi su **Add** (Aggiungi).
  - b. Immettere un nome, selezionare la VM di storage, immettere una dimensione, quindi fare clic su **altre opzioni**.
  - c. In **Permissions**, fare clic su **Add** (Aggiungi). La verifica delle autorizzazioni è facoltativa ma consigliata.
    - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
    - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Risorse** - utilizzare le impostazioni predefinite (`bucketname`, `bucketname/*`) o altri valori di cui hai bisogno

Vedere ["Gestire l'accesso degli utenti ai bucket"](#) per ulteriori informazioni su questi campi.

- d. In **protezione**, selezionare **attiva SnapMirror (ONTAP o Cloud)**. Quindi, immettere i seguenti valori:

- Destinazione
    - **DESTINAZIONE:** Sistema ONTAP
    - **CLUSTER:** Selezionare il cluster locale.
    - **VM di STORAGE:** Selezionare una VM di storage sul cluster locale.
    - **Certificato CA del SERVER S3:** Copia e incolla il contenuto del certificato di origine.
  - Origine
    - **Certificato CA del SERVER S3:** Copia e incolla il contenuto del certificato di destinazione.
5. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
  6. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
  7. Fare clic su **Save** (Salva). Viene creato un nuovo bucket nella VM per lo storage di origine e viene eseguito il mirroring in un nuovo bucket che viene creato la VM per lo storage di destinazione.

### Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere ["Creare un bucket"](#).

### CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:

```
vserver object-store-server user show
```

Verificare che sia presente una chiave di accesso per l'utente root. In caso contrario, immettere:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Non rigenerare la chiave se ne esiste già una.

2. Creare bucket nelle SVM di origine e di destinazione:

```
vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. Aggiungere regole di accesso alle policy di bucket predefinite nelle SVM di origine e di destinazione:



```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parametri:

- continuous – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio).
- -rpo – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo).
- -throttle – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

**Esempio**

```
src_cluster::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installare i certificati del server CA sulla SVM amministrativa:

a. Installare il certificato CA che ha firmato il certificato del server S3 *source* sulla SVM amministrativa:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name src_server_certificate
```

b. Installare il certificato CA che ha firmato il certificato del server S3 di destinazione sulla SVM amministrativa:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name dest_server_certificate+ se si utilizza un certificato firmato da un vendor CA
esterno, è necessario installare questo certificato solo sulla SVM amministrativa.
```

Vedere `security certificate install` pagina man per i dettagli.

6. Creare una relazione SnapMirror S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy
policy_name]`
```

È possibile utilizzare un criterio creato o accettare quello predefinito.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror  
-policy test-policy
```

7. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```




### **Creare una relazione mirror per un bucket esistente (cluster locale)**

È possibile iniziare a proteggere i bucket S3 esistenti sullo stesso cluster in qualsiasi momento, ad esempio se è stata aggiornata una configurazione S3 da una release precedente a ONTAP 9.10.1. È possibile eseguire il mirroring dei dati su un bucket in una VM di storage diversa o nella stessa VM di storage di origine.



#### **Prima di iniziare**

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra le VM storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

## System Manager

1. Se si tratta della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che di destinazione e rigenerarle in caso contrario:
  - a. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
  - b. Nella scheda **Impostazioni**, fare clic su  Nel riquadro **S3**.
  - c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root.
  - d. In caso contrario, fare clic su  Accanto a **root**, quindi fare clic su **Rigenera chiave**. Non rigenerare la chiave se ne esiste già una
2. Verificare che l'accesso a utenti e gruppi sia corretto sia nelle macchine virtuali storage di origine che di destinazione:
  - Fare clic su **Storage > Storage VMS**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto S3.

Vedere ["Aggiungere utenti e gruppi S3"](#) per ulteriori informazioni.

3. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
  - a. Fare clic su **protezione > Panoramica**, quindi su **impostazione policy locale**.
  - b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
    - Immettere il nome e la descrizione della policy.
    - Selezionare l'ambito del criterio, il cluster o SVM
    - Selezionare **Continuous** per le relazioni di S3 SnapMirror.
    - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Verificare che la policy di accesso al bucket del bucket esistente continui a soddisfare le proprie esigenze:
  - a. Fare clic su **Storage > Bucket** (Storage > bucket), quindi selezionare il bucket che si desidera proteggere.
  - b. Nella scheda **Permissions**, fare clic su  **Modifica**, quindi fare clic su **Aggiungi in permessi**.
    - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
    - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori:

```
GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts
```

- **Risorse** - utilizzare le impostazioni predefinite (*bucketname*, *bucketname/\**) o altri valori di cui hai bisogno.

Vedere ["Gestire l'accesso degli utenti ai bucket"](#) per ulteriori informazioni su questi campi.

5. Proteggi un bucket esistente con S3 SnapMirror:
  - a. Fare clic su **Storage > Bucket** e selezionare il bucket che si desidera proteggere.

b. Fare clic su **Protect** (protezione) e immettere i seguenti valori:

- Destinazione
    - **DESTINAZIONE:** Sistema ONTAP
    - **CLUSTER:** Selezionare il cluster locale.
    - **STORAGE VM:** Consente di selezionare la stessa o una diversa storage VM.
    - **Certificato CA del SERVER S3:** Copia e incolla il contenuto del certificato *source*.
  - Origine
    - **Certificato CA server S3:** Copia e incolla il contenuto del certificato *destination*.
6. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
  7. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
  8. Fare clic su **Save** (Salva). Viene eseguito il mirroring del bucket esistente in un nuovo bucket nella VM di storage di destinazione.

### Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere ["Creare un bucket"](#).

### CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:

```
vserver object-store-server user show
```

Verificare che sia presente una chiave di accesso per l'utente root. In caso contrario, immettere:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Non rigenerare la chiave se ne esiste già una.

2. Creare un bucket sulla SVM di destinazione come destinazione mirror:

```
vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]
```

3. Verificare che le regole di accesso alle policy di bucket predefinite siano corrette sia nelle SVM di

origine che di destinazione:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

### Esempio

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parametri:

- ° continuous – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio).
- ° -rpo – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo).
- ° -throttle – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

### Esempio

```
clusterA::> snapmirror policy create -vserver vs0 -type
continuous -rpo 0 -policy test-policy
```

5. Installare i certificati del server CA sulla SVM amministrativa:

- a. Installare il certificato CA che ha firmato il certificato del server S3 *source* sulla SVM amministrativa:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name src_server_certificate
```

- b. Installare il certificato CA che ha firmato il certificato del server S3 di destinazione sulla SVM amministrativa:

```
security certificate install -type server-ca -vserver admin_svm -cert
-name dest_server_certificate+ se si utilizza un certificato firmato da un vendor CA
esterno, è necessario installare questo certificato solo sulla SVM amministrativa.
```

Vedere `security certificate install` pagina man per i dettagli.

6. Creare una relazione SnapMirror S3:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
```

```
-destination-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy policy_name]
```

È possibile utilizzare un criterio creato o accettare quello predefinito.

#### Esempio

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy test-policy
```

7. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```

### Acquisizione e distribuzione dei dati dal bucket di destinazione (cluster locale)

Se i dati in un bucket di origine non sono più disponibili, è possibile interrompere la relazione SnapMirror per rendere il bucket di destinazione scrivibile e iniziare a fornire i dati.

#### A proposito di questa attività


Quando viene eseguita un'operazione di Takeover, il bucket di origine viene convertito in sola lettura e il bucket di destinazione originale viene convertito in lettura-scrittura, invertendo così la relazione di S3 SnapMirror.

Quando il bucket di origine disattivato è nuovamente disponibile, S3 SnapMirror risincronizza automaticamente il contenuto dei due bucket. Non è necessario risincronizzare esplicitamente la relazione, come richiesto per le implementazioni di SnapMirror di volumi standard.

Se il bucket di destinazione si trova su un cluster remoto, l'operazione di Takeover deve essere avviata dal cluster remoto.

#### System Manager

Eseguire il failover dal bucket non disponibile e iniziare a fornire i dati:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
2. Fare clic su , Selezionare **failover**, quindi fare clic su **failover**.

#### CLI

1. Avviare un'operazione di failover per il bucket di destinazione:  

```
snapmirror failover start -destination-path svm_name:/bucket/bucket_name
```
2. Verificare lo stato dell'operazione di failover:  

```
snapmirror show -fields status
```

#### Esempio

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-bucket-mirror
```

## **Ripristino di un bucket dalla VM di storage di destinazione (cluster locale)**

In caso di perdita o danneggiamento dei dati in un bucket di origine, sarà possibile ripopolare i dati ripristinando gli oggetti da un bucket di destinazione.

### **A proposito di questa attività**

È possibile ripristinare il bucket di destinazione su un bucket esistente o su un nuovo bucket. Il bucket di destinazione per l'operazione di ripristino deve essere più grande del bucket di destinazione; lo spazio logico utilizzato.

Se si utilizza un bucket esistente, questo deve essere vuoto quando si avvia un'operazione di ripristino. Il ripristino non "esegue il rollback" di un bucket nel tempo, ma popola un bucket vuoto con i contenuti precedenti.

L'operazione di ripristino deve essere avviata dal cluster locale.

## System Manager

Ripristinare i dati di backup:

1. Fare clic su **protezione > Relazioni**, quindi selezionare il bucket.
2. Fare clic su  Quindi selezionare **Ripristina**.
3. In **Source** (origine), selezionare **Existing Bucket** (bucket esistente) (impostazione predefinita) o **New Bucket** (nuovo bucket).
  - Per ripristinare un **bucket esistente** (impostazione predefinita), completare le seguenti azioni:
    - Selezionare il cluster e la VM di storage per cercare il bucket esistente.
    - Selezionare il bucket esistente.
4. Copiare e incollare il contenuto del certificato CA del server S3 di destinazione.
  - Per ripristinare un **nuovo bucket**, immettere i seguenti valori:
    - Il cluster e la VM di storage per ospitare il nuovo bucket.
    - Il nome, la capacità e il livello di servizio delle prestazioni della nuova benna. Vedere "[Livelli di servizio dello storage](#)" per ulteriori informazioni.
    - Contenuto del certificato CA del server S3 di destinazione.
5. In **destinazione**, copiare e incollare il contenuto del certificato CA del server S3 di origine.
6. Fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

## Ripristinare i bucket bloccati

A partire da ONTAP 9.14.1, puoi eseguire il backup dei bucket bloccati e ripristinarli in base alle necessità.

È possibile ripristinare un bucket object-locked in un bucket nuovo o esistente. È possibile selezionare un bucket a blocco di oggetti come destinazione nei seguenti scenari:

- **Ripristina in un nuovo bucket:** Quando il blocco degli oggetti è attivato, è possibile ripristinare un bucket creando un bucket che ha anche il blocco degli oggetti attivato. Quando si ripristina un bucket bloccato, la modalità di blocco degli oggetti e il periodo di conservazione del bucket originale vengono replicati. È inoltre possibile definire un periodo di blocco diverso per la nuova benna. Questo periodo di conservazione viene applicato a oggetti non bloccati provenienti da altre origini.
- **Ripristina in un bucket esistente:** Un bucket a blocco di oggetti può essere ripristinato in un bucket esistente, purché nel bucket esistente siano attivate la versione e una simile modalità di blocco di oggetti. Viene mantenuto il mantenimento della posizione di ritenzione della benna originale.
- **Restore non-locked bucket:** Anche se il blocco degli oggetti non è abilitato in un bucket, è possibile ripristinarlo in un bucket che ha il blocco degli oggetti attivato e si trova nel cluster di origine. Quando si ripristina il bucket, tutti gli oggetti non bloccati vengono bloccati e la modalità di conservazione e il mantenimento del bucket di destinazione diventano applicabili.

## CLI

1. Se si ripristinano oggetti in un nuovo bucket, creare il nuovo bucket. Per ulteriori informazioni, vedere "[Creare una relazione di backup per un nuovo bucket \(target cloud\)](#)".
2. Avviare un'operazione di ripristino per il bucket di destinazione:

```
snapmirror restore -source-path svm_name:/bucket/bucket_name -destination  
-path svm_name:/bucket/bucket_name
```



### Esempio

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket  
-destination-path vs1:/bucket/test-bucket-mirror
```

## Protezione del backup con destinazioni cloud

### Requisiti per le relazioni di destinazione del cloud

Assicurati che gli ambienti di origine e di destinazione soddisfino i requisiti per la protezione di backup di S3 SnapMirror verso le destinazioni cloud.

Per accedere al bucket di dati, è necessario disporre di credenziali account valide con il provider dell'archivio di oggetti.

Le interfacce di rete tra cluster e un IPspace devono essere configurati sul cluster prima che il cluster possa connettersi a un archivio di oggetti cloud. È necessario creare interfacce di rete del cluster di invio su ciascun nodo per trasferire senza problemi i dati dallo storage locale all'archivio di oggetti cloud.

Per gli obiettivi StorageGRID, è necessario conoscere le seguenti informazioni:

- Nome del server, espresso come nome di dominio completo (FQDN) o indirizzo IP
- nome bucket; il bucket deve già esistere
- tasto di accesso
- chiave segreta

Inoltre, il certificato CA utilizzato per firmare il certificato del server StorageGRID deve essere installato sulla macchina virtuale di storage amministrativa del cluster ONTAP S3 utilizzando `security certificate install` command. Per ulteriori informazioni, vedere ["Installazione di un certificato CA"](#) Se si utilizza StorageGRID.

Per i target AWS S3, è necessario conoscere le seguenti informazioni:

- Nome del server, espresso come nome di dominio completo (FQDN) o indirizzo IP
- nome bucket; il bucket deve già esistere
- tasto di accesso
- chiave segreta

Il server DNS per la VM di storage amministrativa del cluster ONTAP deve essere in grado di risolvere gli FQDN (se utilizzati) in indirizzi IP.



### Creare una relazione di backup per un nuovo bucket (target cloud)

Quando crei nuovi bucket S3, puoi eseguirne immediatamente il backup su un bucket di destinazione di S3 SnapMirror su un provider di archivi di oggetti, che può essere un sistema StorageGRID o un'implementazione di Amazon S3.

### Prima di iniziare

- Si dispone di credenziali account e informazioni di configurazione valide per il provider dell'archivio di oggetti.
- Le interfacce di rete tra cluster e un IPSpace sono state configurate sul sistema di origine.
- • La configurazione DNS per la VM dello storage di origine deve essere in grado di risolvere il FQDN della destinazione.

## System Manager

1. Modificare la VM di storage per aggiungere utenti e utenti ai gruppi:
  - a. Fare clic su **Storage > Storage VMS**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su  Sotto **S3**.  
  
Vedere ["Aggiungere utenti e gruppi S3"](#) per ulteriori informazioni.
2. Aggiungere un Cloud Object Store sul sistema di origine:
  - a. Fare clic su **protezione > Panoramica**, quindi selezionare **Cloud Object Stores**.
  - b. Fare clic su **Aggiungi**, quindi selezionare **Amazon S3** o **StorageGRID**.
  - c. Immettere i seguenti valori:
    - Nome archivio oggetti cloud
    - Stile URL (path o virtual-hosted)
    - Storage VM (abilitato per S3)
    - Nome server archivio oggetti (FQDN)
    - Certificato dell'archivio di oggetti
    - Tasto di accesso
    - Chiave segreta
    - Nome del container (bucket)
3. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
  - a. Fare clic su **protezione > Panoramica**, quindi su **Impostazioni policy locale**.
  - b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
    - Immettere il nome e la descrizione della policy.
    - Selezionare l'ambito del criterio, il cluster o SVM
    - Selezionare **Continuous** per le relazioni di S3 SnapMirror.
    - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Crea un bucket con la protezione SnapMirror:
  - a. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
  - b. Immettere un nome, selezionare la VM di storage, immettere una dimensione, quindi fare clic su **altre opzioni**.
  - c. In **Permissions**, fare clic su **Add** (Aggiungi). La verifica delle autorizzazioni è facoltativa ma consigliata.
    - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
    - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori:

```
`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
```

- **Risorse** - utilizzare le impostazioni predefinite `_(bucketname, bucketname/*)` o altri valori di cui hai bisogno.

Vedere "[Gestire l'accesso degli utenti ai bucket](#)" per ulteriori informazioni su questi campi.

- d. In **protezione**, selezionare **attiva SnapMirror (ONTAP o Cloud)**, selezionare **archiviazione cloud**, quindi selezionare **Archivio oggetti cloud**.

Facendo clic su **Save** (Salva), viene creato un nuovo bucket nella VM dello storage di origine e viene eseguito il backup nell'archivio di oggetti cloud.

## CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:  
`vserver object-store-server user show+` confermare che esiste una chiave di accesso per l'utente root. In caso contrario, immettere:  
`vserver object-store-server user regenerate-keys -vserver svm_name -user root+` non rigenerare la chiave se ne esiste già una.

2. Creare un bucket nella SVM di origine:

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Aggiungere regole di accesso alla policy bucket predefinita:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

## Esempio

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parametri: \* `type continuous` – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio). \* `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo). \* `-throttle` – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

### Esempio

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous  
-rpo 0 -policy test-policy
```

5. Se la destinazione è un sistema StorageGRID, installare il certificato del server CA StorageGRID sulla SVM amministrativa del cluster di origine:

```
security certificate install -type server-ca -vserver src_admin_svm -cert  
-name storage_grid_server_certificate
```

Vedere `security certificate install` pagina man per i dettagli.

6. Definire l'archivio di oggetti di destinazione di S3 SnapMirror:

```
snapmirror object-store config create -vserver svm_name -object-store-name  
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server  
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port  
port_number -access-key target_access_key -secret-password  
target_secret_key
```

Parametri: \* `-object-store-name` – Il nome della destinazione dell'archivio di oggetti nel sistema ONTAP locale. \* `-usage` – utilizzare `data` per questo flusso di lavoro. \* `-provider-type` – `AWS_S3` e `SGWS` Sono supportati i target (StorageGRID). \* `-server` – L'indirizzo FQDN o IP del server di destinazione. \* `-is-ssl-enabled` – L'abilitazione di SSL è facoltativa ma consigliata. + vedere `snapmirror object-store config create` pagina man per i dettagli.

### Esempio

```
src_cluster::> snapmirror object-store config create -vserver vs0  
-object-store-name sgws-store -usage data -provider-type SGWS  
-server sgws.example.com -container-name target-test-bucket -is-ssl-  
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. Creare una relazione SnapMirror S3:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination  
-path object_store_name:/objstore -policy policy_name
```

Parametri:

\* `-destination-path` - il nome dell'archivio oggetti creato nel passo precedente e il valore fisso `objstore`.

È possibile utilizzare un criterio creato o accettare quello predefinito.

### Esempio

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-  
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```


## **Creare una relazione di backup per un bucket esistente (target cloud)**

È possibile iniziare il backup dei bucket S3 esistenti in qualsiasi momento, ad esempio se è stata aggiornata una configurazione S3 da una release precedente a ONTAP 9.10.1.



### **Prima di iniziare**

- Si dispone di credenziali account e informazioni di configurazione valide per il provider dell'archivio di oggetti.
- Le interfacce di rete tra cluster e un IPspace sono state configurate sul sistema di origine.
- La configurazione DNS per la VM dello storage di origine deve essere in grado di risolvere l'FQDN della destinazione.

## System Manager

1. Verificare che gli utenti e i gruppi siano definiti correttamente: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni) e quindi su  Sotto S3.

Vedere "[Aggiungere utenti e gruppi S3](#)" per ulteriori informazioni.

2. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
  - a. Fare clic su **protezione > Panoramica**, quindi su **Impostazioni policy locale**.
  - b. Fare clic su  Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
  - c. Immettere il nome e la descrizione della policy.
  - d. Selezionare l'ambito del criterio, il cluster o SVM
  - e. Selezionare **Continuous** per le relazioni di S3 SnapMirror.
  - f. Inserire i valori **Throttle** e **Recovery Point Objective**.
3. Aggiungere un Cloud Object Store sul sistema di origine:
  - a. Fare clic su **protezione > Panoramica**, quindi selezionare **Cloud Object Store**.
  - b. Fare clic su **Aggiungi**, quindi selezionare **Amazon S3** o **altri** per StorageGRID webscale.
  - c. Immettere i seguenti valori:
    - Nome archivio oggetti cloud
    - Stile URL (path o virtual-hosted)
    - Storage VM (abilitato per S3)
    - Nome server archivio oggetti (FQDN)
    - Certificato dell'archivio di oggetti
    - Tasto di accesso
    - Chiave segreta
    - Nome del container (bucket)
4. Verificare che la policy di accesso al bucket del bucket esistente soddisfi ancora le proprie esigenze:
  - a. Fare clic su **Storage > Bucket** e selezionare il bucket che si desidera proteggere.
  - b. Nella scheda **Permissions**, fare clic su  **Modifica**, quindi fare clic su **Aggiungi in permessi**.
    - **Principal e Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
    - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori:  
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
    - **Risorse** - utilizzare le impostazioni predefinite (`bucketname, bucketname/*`) o altri valori di cui hai bisogno.

Vedere "[Gestire l'accesso degli utenti ai bucket](#)" per ulteriori informazioni su questi campi.
5. Eseguire il backup del bucket utilizzando S3 SnapMirror:
  - a. Fare clic su **Storage > Bucket**, quindi selezionare il bucket di cui si desidera eseguire il backup.

- b. Fare clic su **Protect**, selezionare **Cloud Storage** sotto **Target**, quindi selezionare **Cloud Object Store**.

Facendo clic su **Save** (Salva), viene eseguito il backup del bucket esistente nell'archivio di oggetti cloud.

## CLI

1. Verificare che le regole di accesso nel criterio bucket predefinito siano corrette:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

### Esempio

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

2. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Parametri: \* `type continuous` – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio). \* `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo). \* `-throttle` – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

### Esempio

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

3. Se la destinazione è un sistema StorageGRID, installare il certificato CA StorageGRID sulla SVM amministrativa del cluster di origine:

```
security certificate install -type server-ca -vserver src_admin_svm -cert
-name storage_grid_server_certificate
```

Vedere `security certificate install` pagina man per i dettagli.

4. Definire l'archivio di oggetti di destinazione di S3 SnapMirror:

```
snapmirror object-store config create -vserver svm_name -object-store-name
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server
target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port
port_number -access-key target_access_key -secret-password
target_secret_key
```



Parametri: \* `-object-store-name` – Il nome della destinazione dell'archivio di oggetti nel sistema ONTAP locale. \* `-usage` – utilizzare `data` per questo flusso di lavoro. \* `-provider-type` – `AWS_S3` e `SGWS` Sono supportati i target (StorageGRID). \* `-server` – L'indirizzo FQDN o IP del server di destinazione. \* `-is-ssl-enabled` –L'abilitazione di SSL è facoltativa ma consigliata. + vedere `snapmirror object-store config create` pagina man per i dettagli.

### Esempio

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

### 5. Creare una relazione SnapMirror S3:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

#### Parametri:

\* `-destination-path` - il nome dell'archivio oggetti creato nel passo precedente e il valore fisso `objstore`.

È possibile utilizzare un criterio creato o accettare quello predefinito.

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

### 6. Verificare che il mirroring sia attivo:

```
snapmirror show -policy-type continuous -fields status
```

## Ripristinare un bucket da un target cloud

In caso di perdita o danneggiamento dei dati in un bucket di origine, sarà possibile ricompilare i dati ripristinandoli da un bucket di destinazione.


### A proposito di questa attività

È possibile ripristinare il bucket di destinazione su un bucket esistente o su un nuovo bucket. Il bucket di destinazione per l'operazione di ripristino deve essere più grande dello spazio logico utilizzato del bucket di destinazione.

Se si utilizza un bucket esistente, questo deve essere vuoto quando si avvia un'operazione di ripristino. Il ripristino non "esegue il rollback" di un bucket nel tempo, ma popola un bucket vuoto con i contenuti precedenti.

## System Manager

Ripristinare i dati di backup:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
2. Fare clic su  Quindi selezionare **Ripristina**.
3. In **Source** (origine), selezionare **Existing Bucket** (bucket esistente) (impostazione predefinita) o **New Bucket** (nuovo bucket).
  - Per ripristinare un **bucket esistente** (impostazione predefinita), completare le seguenti azioni:
    - Selezionare il cluster e la VM di storage per cercare il bucket esistente.
    - Selezionare il bucket esistente.
    - Copiare e incollare il contenuto del certificato CA del server S3 *destination*.
  - Per ripristinare un **nuovo bucket**, immettere i seguenti valori:
    - Il cluster e la VM di storage per ospitare il nuovo bucket.
    - Il nome, la capacità e il livello di servizio delle performance del nuovo bucket. Vedere "[Livelli di servizio dello storage](#)" per ulteriori informazioni.
    - Contenuto del certificato CA del server S3 di destinazione.
4. In **destinazione**, copiare e incollare il contenuto del certificato CA del server S3 *origine*.
5. Fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

## Procedura CLI

1. Creare il nuovo bucket di destinazione per il ripristino. Per ulteriori informazioni, vedere "[Creare una relazione di backup per un bucket \(target cloud\)](#)".
2. Avviare un'operazione di ripristino per il bucket di destinazione:

```
snapmirror restore -source-path object_store_name:/objstore -destination  
-path svm_name:/bucket/bucket_name
```

## Esempio

Nell'esempio seguente viene ripristinato un bucket di destinazione in un bucket esistente.


```
clusterA::> snapmirror restore -source-path sgws.store:/objstore  
-destination-path vs0:/bucket/test-bucket
```

## Modificare una policy mirror

È possibile modificare una policy di mirroring S3, ad esempio se si desidera regolare i valori RPO e THROTTLE.

## System Manager

Se si desidera modificare questi valori, è possibile modificare un criterio di protezione esistente.

1. Fare clic su **protezione > Relazioni**, quindi selezionare il criterio di protezione per la relazione che si desidera modificare.
2. Fare clic su  Accanto al nome del criterio, quindi fare clic su **Modifica**.

## CLI

Modifica di un criterio SnapMirror S3:

```
snapmirror policy modify -vserver svm_name -policy policy_name [-rpo integer]
[-throttle throttle_type] [-comment text]
```

Parametri:

- `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi.
- `-throttle` – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

# Controllare gli eventi S3

## Controllare gli eventi S3

A partire da ONTAP 9.10.1, è possibile controllare i dati e gli eventi di gestione negli ambienti ONTAP S3. La funzionalità di audit S3 è simile alle funzionalità di auditing NAS esistenti e l'auditing S3 e NAS può coesistere in un cluster.

Quando si crea e si attiva una configurazione di controllo S3 su una SVM, gli eventi S3 vengono registrati in un file di registro. È possibile specificare i seguenti eventi da registrare:

- Eventi di accesso a oggetti (dati)  
GetObject, PutObject e DeleteObject
- Eventi di gestione  
Putbucket e Deletebucket

Il formato del log è JavaScript Object Notation (JSON).

Il limite combinato per le configurazioni di controllo S3 e NFS è di 50 SVM per cluster.

È richiesto il seguente bundle di licenza:

- Bundle core, per protocollo e storage ONTAP S3

Per ulteriori informazioni, vedere ["Come funziona il processo di audit di ONTAP"](#).

## Auditing garantito

Per impostazione predefinita, è garantito il controllo S3 e NAS. ONTAP garantisce la registrazione di tutti gli eventi di accesso al bucket verificabili, anche se un nodo non è disponibile. Un'operazione bucket richiesta non può essere completata fino a quando il record di audit per tale operazione non viene salvato nel volume di staging sullo storage persistente. Se non è possibile eseguire il commit dei record di audit nei file di staging, a causa di spazio insufficiente o a causa di altri problemi, le operazioni del client vengono negate.

## Requisiti di spazio per il controllo

Nel sistema di audit ONTAP, i record di audit vengono inizialmente memorizzati in file di staging binari su singoli nodi. Periodicamente, vengono consolidati e convertiti in registri eventi leggibili dall'utente, memorizzati nella directory del registro eventi di controllo per SVM.

I file di staging vengono memorizzati in un volume di staging dedicato, creato da ONTAP al momento della creazione della configurazione di audit. Esiste un volume di staging per aggregato.

È necessario pianificare uno spazio disponibile sufficiente nella configurazione di controllo:

- Per i volumi di staging in aggregati che contengono bucket controllati.
- Per il volume contenente la directory in cui sono memorizzati i registri degli eventi convertiti.

È possibile controllare il numero di registri eventi e quindi lo spazio disponibile nel volume utilizzando uno dei due metodi per creare la configurazione di controllo S3:

- Un limite numerico; il `-rotate-limit` parametro controlla il numero minimo di file di audit che devono essere conservati.
- Un limite di tempo; il `-retention-duration` parametro controlla il periodo massimo di conservazione dei file.

In entrambi i parametri, una volta superato il valore configurato, è possibile eliminare i file di audit più vecchi per fare spazio a quelli più recenti. Per entrambi i parametri, il valore è 0, a indicare che tutti i file devono essere mantenuti. Per garantire uno spazio sufficiente, è quindi consigliabile impostare uno dei parametri su un valore diverso da zero.

A causa del controllo garantito, se lo spazio disponibile per i dati di audit si esaurisce prima del limite di rotazione, non è possibile creare dati di audit più recenti, con conseguente impossibilità per i client di accedere ai dati. Pertanto, la scelta di questo valore e dello spazio allocato per l'audit deve essere scelta con attenzione, ed è necessario rispondere agli avvisi sullo spazio disponibile dal sistema di audit.

Per ulteriori informazioni, vedere ["Concetti di controllo di base"](#).

## Pianificare una configurazione di controllo S3

È necessario specificare una serie di parametri per la configurazione di controllo S3 o accettare le impostazioni predefinite. In particolare, è necessario considerare quali parametri di rotazione del log contribuiranno a garantire un adeguato spazio libero.

Vedere `vserver object-store-server audit create` pagina man per i dettagli della sintassi.

## Parametri generali

Sono necessari due parametri da specificare quando si crea la configurazione di controllo. È possibile specificare anche tre parametri opzionali.

Tipo di informazione	Opzione	Obbligatorio
<b>Nome SVM</b>  Nome della SVM su cui creare la configurazione di controllo.  La SVM deve già esistere ed essere abilitata per S3.	<code>-verserver svm_name</code>	Sì
<b>Percorso di destinazione del registro</b>  Specifica dove sono memorizzati i log di audit convertiti. Il percorso deve già esistere sulla SVM.  Il percorso può contenere fino a 864 caratteri e deve disporre di permessi di lettura/scrittura.  Se il percorso non è valido, il comando di configurazione del controllo non riesce.	<code>-destination text</code>	Sì
<b>Categorie di eventi da controllare</b>  È possibile verificare le seguenti categorie di eventi: <ul style="list-style-type: none"><li>• Eventi Data GetObject, PutObject e DeleteObject</li><li>• Gestione degli eventi Putbucket e Deletebucket</li></ul> L'impostazione predefinita prevede solo l'audit degli eventi dati.	<code>-events {data management}, ...</code>	No

È possibile inserire uno dei seguenti parametri per controllare il numero di file di log di audit. Se non viene immesso alcun valore, tutti i file di registro vengono conservati.

Tipo di informazione	Opzione	Obbligatorio
<b>Limite di rotazione dei file di log</b>  Determina il numero di file di log di audit da conservare prima di estrarre il file di log più vecchio. Ad esempio, se si immette il valore 5, vengono conservati gli ultimi cinque file di registro.  Il valore 0 indica che tutti i file di log vengono conservati. Il valore predefinito è 0.	<code>-rotate-limit integer</code>	No

<p><i>Limite di durata dei file di log</i></p> <p>Determina per quanto tempo un file di log può essere conservato prima di essere cancellato. Ad esempio, se si immette un valore di 5d0h0m, i registri più vecchi di 5 giorni vengono cancellati.</p> <p>Il valore 0 indica che tutti i file di log vengono conservati. Il valore predefinito è 0.</p>	<p>-retention duration <i>integer_time</i></p>	<p>No</p>
---	--	-----------

## Parametri per la rotazione del registro di controllo

È possibile ruotare i registri di audit in base alle dimensioni o alla pianificazione. L'impostazione predefinita prevede la rotazione dei registri di controllo in base alle dimensioni.

### Ruotare i registri in base alle dimensioni del registro

Se si desidera utilizzare il metodo di rotazione del log predefinito e la dimensione del log predefinita, non è necessario configurare alcun parametro specifico per la rotazione del log. La dimensione predefinita del registro è 100 MB.

Se non si desidera utilizzare la dimensione predefinita del registro, è possibile configurare `-rotate-size` parametro per specificare una dimensione di log personalizzata.

Se si desidera ripristinare la rotazione solo in base alle dimensioni del log, utilizzare il comando seguente per annullare l'impostazione di `-rotate-schedule-minute` parametro:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

### Ruotare i registri in base a una pianificazione

Se si sceglie di ruotare i registri di controllo in base a una pianificazione, è possibile pianificare la rotazione dei registri utilizzando i parametri di rotazione basati sul tempo in qualsiasi combinazione.

- Se si utilizza la rotazione basata sul tempo, il `-rotate-schedule-minute` il parametro è obbligatorio.
- Tutti gli altri parametri di rotazione basati sul tempo sono opzionali.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- Il programma di rotazione viene calcolato utilizzando tutti i valori relativi al tempo. Ad esempio, se si specifica solo il `-rotate-schedule-minute` i file di log di audit vengono ruotati in base ai minuti specificati in tutti i giorni della settimana, durante tutte le ore in tutti i mesi dell'anno.
- Se si specificano solo uno o due parametri di rotazione basati sul tempo (ad esempio, `-rotate-schedule-month` e `-rotate-schedule-minutes`), i file di log vengono ruotati in base ai valori dei minuti specificati in tutti i giorni della settimana, durante tutte le ore, ma solo durante i mesi specificati.

Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato durante i mesi di gennaio, marzo e agosto tutti i lunedì, mercoledì e sabato alle 10:30

- Se si specificano i valori per entrambi `-rotate-schedule-dayofweek` e `-rotate-schedule-day`, sono considerati indipendenti.

Ad esempio, se si specifica `-rotate-schedule-dayofweek` Come venerdì e `-rotate-schedule-day` Come 13, i registri di audit verrebbero ruotati ogni venerdì e il 13° giorno del mese specificato, non solo ogni venerdì 13.

- Se si desidera ripristinare la rotazione solo in base a una pianificazione, utilizzare il comando seguente per annullare l'impostazione di `-rotate-size` parameter:

```
vserver audit modify -vserver svm_name -destination / -rotate-size -
```

### Rotazione dei registri in base alle dimensioni e alla pianificazione dei registri

È possibile scegliere di ruotare i file di log in base alle dimensioni del log e a una pianificazione impostando sia il parametro `-rotate-size` che i parametri di rotazione basati sul tempo in qualsiasi combinazione. Ad esempio: Se `-rotate-size` È impostato su 10 MB e `-rotate-schedule-minute` È impostato su 15, i file di log ruotano quando le dimensioni del file di log raggiungono i 10 MB o al 15° minuto di ogni ora (a seconda dell'evento che si verifica per primo).

## Creare e abilitare una configurazione di controllo S3

Per implementare il controllo S3, creare prima una configurazione di controllo dell'archivio di oggetti persistente su una SVM abilitata per S3, quindi attivare la configurazione.

### Di cosa hai bisogno

- Una SVM abilitata per S3.
- Spazio sufficiente per lo staging dei volumi nell'aggregato.

### A proposito di questa attività

Per ogni SVM contenente i bucket S3 che si desidera controllare è necessaria una configurazione di controllo. È possibile attivare il controllo S3 su server S3 nuovi o esistenti. Le configurazioni di controllo persistono in un ambiente S3 fino a quando non vengono rimosse dal comando **`vserver object-store-server audit delete`**.

La configurazione di controllo S3 si applica a tutti i bucket della SVM selezionati per il controllo. Una SVM abilitata all'audit può contenere bucket controllati e non verificati.

Si consiglia di configurare il controllo S3 per la rotazione automatica del log, determinata dalle dimensioni del log o da una pianificazione. Se non si configura la rotazione automatica del log, tutti i file di log vengono conservati per impostazione predefinita. È inoltre possibile ruotare manualmente i file di log S3 utilizzando il comando **`vserver object-store-server audit rotate-log`**.

Se SVM è un'origine di disaster recovery SVM, il percorso di destinazione non può trovarsi sul volume root.

### Procedura

1. Creare la configurazione di controllo per ruotare i registri di controllo in base alle dimensioni del registro o a una pianificazione.

Se si desidera ruotare i registri di audit di...	Inserisci...
Dimensione del log	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer]   [- retention-duration [integer_d] [_integer_h][_integer_m][_integers]]] [-rotate-size {integer[KB MB GB TB PB]}]</pre>
Un calendario	<pre>vserver object-store-server audit create -vserver svm_name -destination path [[-events] {data management}, ...] [[-rotate-limit integer]   [- retention-duration [integerd][integerh] [integerm ][_integers]] ] [-rotate-schedule-month chron_month] [-rotate-schedule-dayofweek chron_dayofweek] [- rotate-schedule-day chron_dayofmonth] [-rotate- schedule-hour chron_hour] -rotate-schedule-minute chron_minute</pre> <p>Il -rotate-schedule-minute il parametro è obbligatorio se si configura la rotazione del log di audit basata sul tempo.</p>

## 2. Abilita controllo S3:

```
vserver object-store-server audit enable -vserver svm_name
```

### Esempi

Nell'esempio seguente viene creata una configurazione di controllo che controlla tutti gli eventi S3 (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. I registri vengono memorizzati nella directory /audit\_log. Il limite delle dimensioni del file di log è di 200 MB. I log vengono ruotati quando raggiungono le dimensioni di 200 MB.

```
cluster1:> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla tutti gli eventi S3 (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il limite delle dimensioni del file di registro è di 100 MB (impostazione predefinita) e i registri vengono conservati per 5 giorni prima di essere cancellati.

```
cluster1:> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla gli eventi di gestione S3 e gli eventi di staging dei criteri di accesso centrale utilizzando la rotazione basata sul tempo. I registri di audit vengono ruotati mensilmente alle 12:30 tutti i giorni della settimana. Il limite di rotazione del log è 5.

```
cluster1:> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```



## Selezionare i bucket per il controllo S3

È necessario specificare quali bucket eseguire il controllo in una SVM abilitata per l'audit.

### Di cosa hai bisogno

- SVM abilitato per il controllo S3.

### A proposito di questa attività

Le configurazioni di controllo S3 sono abilitate per SVM, ma è necessario selezionare i bucket nelle SVM che sono abilitati per l'audit. Se si aggiungono bucket alla SVM e si desidera che i nuovi bucket vengano controllati, è necessario selezionarli con questa procedura. È inoltre possibile avere bucket non controllati in una SVM abilitata per il controllo S3.

Le configurazioni di controllo persistono per i bucket fino a quando non vengono rimosse da `vserver object-store-server audit object-select delete` comando.

### Procedura

Seleziona un bucket per l'audit S3:

```
vserver object-store-server audit event-selector create -vserver svm_name -bucket bucket_name [[-access] {read-only|write-only|all}] [[-permission] {allow-only|deny-only|all}]
```

- `-access` - specifica il tipo di accesso all'evento da sottoporre a verifica: `read-only`, `write-only` oppure `all` (il valore predefinito è `all`).
- `-permission` - specifica il tipo di autorizzazione all'evento da sottoporre a verifica: `allow-only`, `deny-only` oppure `all` (il valore predefinito è `all`).

### Esempio

Nell'esempio seguente viene creata una configurazione di controllo del bucket che registra solo gli eventi consentiti con accesso in sola lettura:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1 -bucket test-bucket -access read-only -permission allow-only
```

## Modificare una configurazione di controllo S3

È possibile modificare i parametri di controllo dei singoli bucket o la configurazione di controllo di tutti i bucket selezionati per l'audit nella SVM.

Se si desidera modificare la configurazione dell'audit per...	Inserisci...
Bucket individuali	<code>vserver object-store-server audit event-selector modify -vserver svm_name [-bucket bucket_name] [parameters to modify]</code>
Tutti i bucket di SVM	<code>vserver object-store-server audit modify -vserver svm_name [parameters to modify]</code>

### Esempi

Nell'esempio seguente viene modificata una singola configurazione di controllo del bucket per controllare solo gli eventi di accesso di sola scrittura:

```
cluster1:> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

Nell'esempio riportato di seguito viene modificata la configurazione di controllo di tutti i bucket di SVM per modificare il limite delle dimensioni dei log a 10 MB e conservare 3 file di log prima della rotazione.

```
cluster1:> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

## Mostrare le configurazioni di controllo S3

Una volta completata la configurazione di controllo, è possibile verificare che il controllo sia configurato correttamente e sia attivato. È inoltre possibile visualizzare informazioni su tutte le configurazioni di controllo dell'archivio di oggetti nel cluster.

### A proposito di questa attività

È possibile visualizzare informazioni sulle configurazioni di controllo bucket e SVM.

- **Bucket** – utilizzare `vserver object-store-server audit event-selector show` comando

Senza alcun parametro, il comando visualizza le seguenti informazioni sui bucket in tutte le SVM del cluster con configurazioni di controllo degli archivi di oggetti:

- Nome SVM
- Nome bucket
- Valori di accesso e autorizzazione

- **SVM**: Utilizzare `vserver object-store-server audit show` comando

Senza alcun parametro, il comando visualizza le seguenti informazioni su tutte le SVM nel cluster con configurazioni di controllo degli archivi di oggetti:

- Nome SVM
- Stato di audit
- Directory di destinazione

È possibile specificare `-fields` parametro per specificare le informazioni di configurazione di controllo da visualizzare.

### Procedura

Mostra informazioni sulle configurazioni di controllo S3:

Se si desidera modificare la configurazione per...	Inserisci...
Bucket	<code>vserver object-store-server audit event-selector show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>
SVM	<code>vserver object-store-server audit show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>

## Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a un singolo bucket:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
```

Vserver	Bucket	Access	Permission
-----	-----	-----	-----
vs1	bucket1	read-only	allow-only

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative a tutti i bucket di una SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1
```

Vserver	:vs1
Bucket	:test-bucket
Access	:all
Permission	:all

Nell'esempio riportato di seguito vengono visualizzati il nome, lo stato di controllo, i tipi di evento, il formato del registro e la directory di destinazione di tutte le SVM.

```
cluster1::> vserver object-store-server audit show
```

Vserver	State	Event Types	Log Format	Target Directory
-----	-----	-----	-----	-----
vs1	false	data	json	/audit_log

Nell'esempio seguente vengono visualizzati i nomi e i dettagli SVM relativi al registro di controllo per tutte le SVM.

```
cluster1::> vserver object-store-server audit show -log-save-details
```

Vserver	Rotation File Size	Rotation Schedule	Rotation Limit
vs1	100MB	-	0

Nell'esempio riportato di seguito vengono visualizzate tutte le informazioni di configurazione dell'audit relative a tutte le SVM.

```
cluster1::> vserver object-store-server audit show -instance
```

```

    Vserver: vs1
    Auditing state: true
    Log Destination Path: /audit_log
    Categories of Events to Audit: data
    Log Format: json
    Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
    Log Rotation Schedule: Day of Week: -
    Log Rotation Schedule: Day: -
    Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
    Rotation Schedules: -
    Log Files Rotation Limit: 0
    Log Retention Time: 0s
```

# Autenticazione e controllo dell'accesso

## Panoramica dell'autenticazione e del controllo degli accessi

Puoi gestire l'autenticazione del cluster ONTAP e il controllo dell'accesso ai servizi web ONTAP.

Con System Manager o la CLI puoi controllare e proteggere l'accesso client e amministratore al cluster e allo storage.

Se si utilizza la gestione di sistema classica (disponibile solo in ONTAP 9.7 e versioni precedenti), fare riferimento a. "[System Manager Classic \(ONTAP da 9.0 a 9.7\)](#)"

### Autenticazione e autorizzazione del client

ONTAP autentica un computer client e un utente verificando la propria identità con un'origine attendibile.

ONTAP autorizza un utente ad accedere a un file o a una directory confrontando le credenziali dell'utente con le autorizzazioni configurate nel file o nella directory.

### Autenticazione amministratore e RBAC

Gli amministratori utilizzano account di accesso locali o remoti per autenticarsi sulla VM del cluster e dello storage. RBAC (Role-Based Access Control) determina i comandi a cui un amministratore ha accesso.

## Gestire l'autenticazione dell'amministratore e RBAC

### Panoramica dell'autenticazione dell'amministratore e RBAC con la CLI

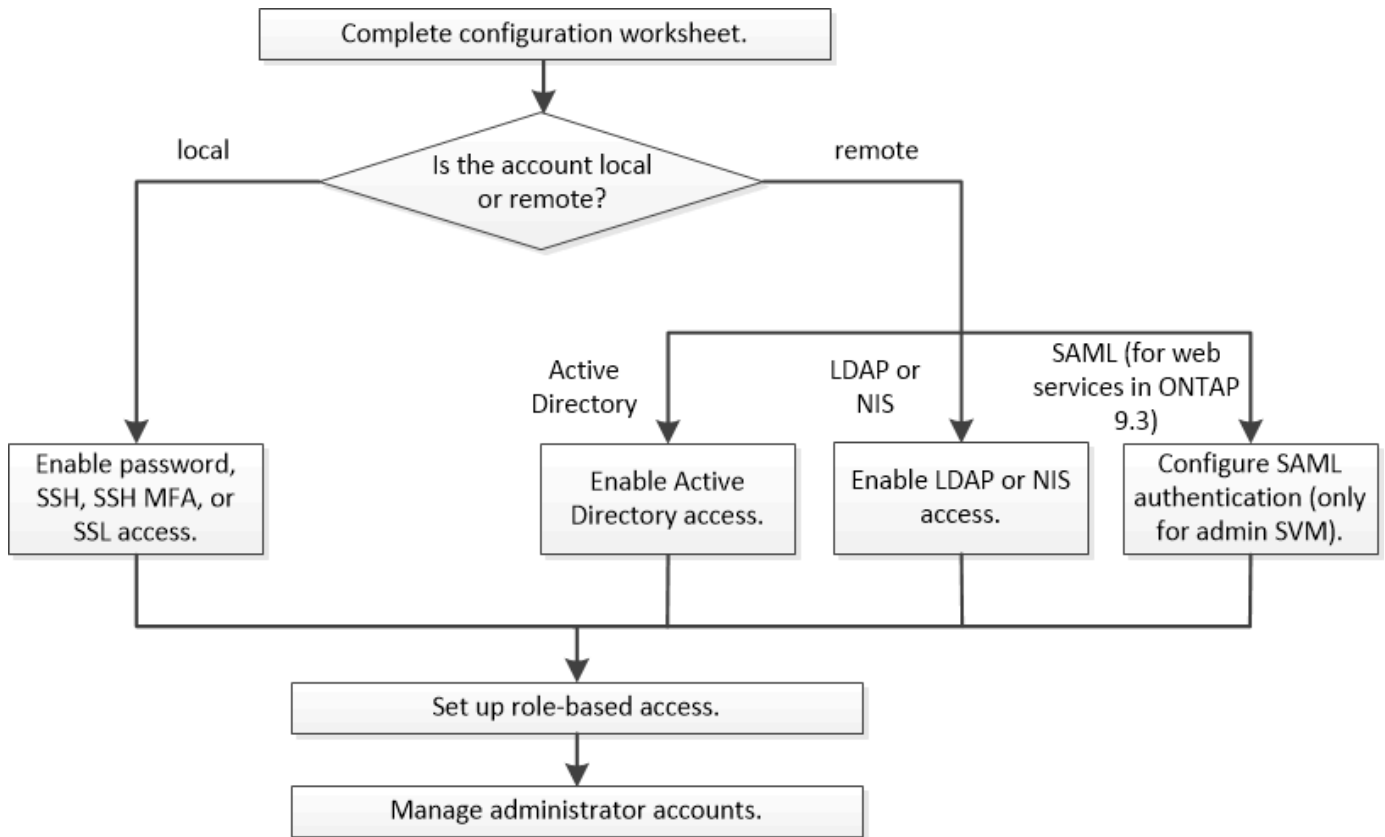
È possibile abilitare gli account di accesso per gli amministratori del cluster ONTAP e per gli amministratori delle macchine virtuali di storage (SVM). È inoltre possibile utilizzare RBAC (role-based access control) per definire le funzionalità degli amministratori.

È possibile abilitare gli account di accesso e RBAC nei seguenti modi:

- Si desidera utilizzare l'interfaccia della riga di comando (CLI) di ONTAP, non Gestione di sistema o uno strumento di scripting automatico.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Non si utilizza SNMP per raccogliere informazioni sul cluster.

### Autenticazione dell'amministratore e workflow RBAC

È possibile attivare l'autenticazione per gli account amministratore locali o per gli account amministratore remoti. Le informazioni dell'account per un account locale risiedono nel sistema di storage e le informazioni dell'account per un account remoto risiedono altrove. Ogni account può avere un ruolo predefinito o personalizzato.



È possibile consentire agli account amministratore locali di accedere a una SVM (Storage Virtual Machine) o a una SVM dati con i seguenti tipi di autenticazione:

- Password
- Chiave pubblica SSH
- Certificato SSL
- Autenticazione multifattore SSH (MFA)

A partire da ONTAP 9.3, è supportata l'autenticazione con password e chiave pubblica.

È possibile consentire agli account amministratore remoto di accedere a una SVM amministrativa o a una SVM dati con i seguenti tipi di autenticazione:

- Active Directory
- Autenticazione SAML (solo per SVM admin)

A partire da ONTAP 9.3, l'autenticazione SAML (Security Assertion Markup Language) può essere utilizzata per accedere alla SVM amministrativa utilizzando uno dei seguenti servizi Web: Infrastruttura del processore di servizi, API ONTAP o Gestore di sistema.

- A partire da ONTAP 9.4, SSH MFA può essere utilizzato per utenti remoti su server LDAP o NIS. È supportata l'autenticazione con nsswitch e chiave pubblica.

## Fogli di lavoro per l'autenticazione dell'amministratore e la configurazione RBAC

Prima di creare account di accesso e impostare RBAC (role-based access control), è necessario raccogliere informazioni per ciascun elemento nei fogli di lavoro di

configurazione.

### Creare o modificare gli account di accesso

Questi valori vengono forniti con `security login create` Comando quando abiliti gli account di accesso per accedere a una VM di storage. Vengono forniti gli stessi valori con `security login modify` Comando quando si modifica il modo in cui un account accede a una VM storage.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della VM di storage a cui accede l'account. Il valore predefinito è il nome della VM storage di amministrazione per il cluster.	
<code>-user-or-group-name</code>	Il nome utente o il nome del gruppo dell'account. Specificando un nome di gruppo, è possibile accedere a ciascun utente del gruppo. È possibile associare un nome utente o un nome di gruppo a più applicazioni.	
<code>-application</code>	Applicazione utilizzata per accedere alla VM di storage: <ul style="list-style-type: none"><li>• <code>http</code></li><li>• <code>ontapi</code></li><li>• <code>snmp</code></li><li>• <code>ssh</code></li></ul>	

-authmethod	<p>Il metodo utilizzato per autenticare l'account:</p> <ul style="list-style-type: none"> <li>• <code>cert</code> Per l'autenticazione del certificato SSL</li> <li>• <code>domain</code> Per l'autenticazione di Active Directory</li> <li>• <code>nsswitch</code> Per l'autenticazione LDAP o NIS</li> <li>• <code>password</code> per l'autenticazione della password dell'utente</li> <li>• <code>publickey</code> per l'autenticazione a chiave pubblica</li> <li>• <code>community</code> Per le stringhe di comunità SNMP</li> <li>• <code>usm</code> Per il modello di sicurezza dell'utente SNMP</li> <li>• <code>saml</code> Per l'autenticazione SAML (Security Assertion Markup Language)</li> </ul>	
-remote-switch-ipaddress	<p>L'indirizzo IP dello switch remoto. Lo switch remoto può essere uno switch del cluster monitorato dal monitor di stato dello switch del cluster (CSHM) o uno switch Fibre Channel (FC) monitorato dal monitor di stato MetroCluster (MCC-HM). Questa opzione è applicabile solo quando l'applicazione è <code>snmp</code> e il metodo di autenticazione è <code>usm</code>.</p>	
-role	<p>Il ruolo di controllo degli accessi assegnato all'account:</p> <ul style="list-style-type: none"> <li>• Per il cluster (la VM di storage di amministrazione), il valore predefinito è <code>admin</code>.</li> <li>• Per una macchina virtuale per lo storage dei dati, il valore predefinito è <code>vsadmin</code>.</li> </ul>	
-comment	<p>(Facoltativo) testo descrittivo per l'account. Racchiudere il testo tra virgolette doppie (").</p>	



-is-ns-switch-group	Se l'account è un account di gruppo LDAP o NIS (yes oppure no).	
-second-authentication-method	<p>Secondo metodo di autenticazione in caso di autenticazione multifattore:</p> <ul style="list-style-type: none"> <li>• none se non si utilizza l'autenticazione a più fattori, valore predefinito</li> <li>• publickey per l'autenticazione a chiave pubblica quando authmethod è password o nsswitch</li> <li>• password per l'autenticazione della password utente quando authmethod è chiave pubblica</li> <li>• nsswitch per l'autenticazione della password utente quando il metodo authmethod è publickey</li> </ul> <p>L'ordine di autenticazione è sempre la chiave pubblica seguita dalla password.</p>	
-is-ldap-fastbind	<p>A partire da ONTAP 9.11.1, se impostato su true, attiva il binding rapido LDAP per l'autenticazione nsswitch; l'impostazione predefinita è false. Per utilizzare l'associazione rapida LDAP, il -authentication-method il valore deve essere impostato su nsswitch. <a href="#">"Scopri di più su LDAP fastbind per l'autenticazione nsswitch."</a></p>	

## Configurare le informazioni di protezione di Cisco Duo

Questi valori vengono forniti con `security login duo create` Comando quando si attiva l'autenticazione a due fattori Cisco Duo con gli accessi SSH per una VM di storage.

Campo	Descrizione	Il tuo valore
-------	-------------	---------------

-vserver	La VM di storage (denominata vserver nell'interfaccia CLI di ONTAP) a cui si applicano le impostazioni di autenticazione Duo.	
-integration-key	La chiave di integrazione, ottenuta durante la registrazione dell'applicazione SSH con Duo.	
-secret-key	La chiave segreta, ottenuta durante la registrazione dell'applicazione SSH con Duo.	
-api-host	<p>Il nome host API, ottenuto durante la registrazione dell'applicazione SSH con Duo. Ad esempio:</p> <pre>api- &lt;HOSTNAME&gt;.duosecurity.com</pre>	
-fail-mode	In caso di errori di configurazione o di servizio che impediscono l'autenticazione Duo, non viene eseguita correttamente <code>safe</code> (consentire l'accesso) o <code>secure</code> (negare l'accesso). L'impostazione predefinita è <code>safe</code> , il che significa che l'autenticazione Duo viene ignorata se non riesce a causa di errori quali il server Duo API non è accessibile.	
-http-proxy	<p>Utilizzare il proxy HTTP specificato. Se il proxy HTTP richiede l'autenticazione, includere le credenziali nell'URL del proxy. Ad esempio:</p> <pre>http- proxy=http://username :password@proxy.example.org:8080</pre>	

-autopush	<p>Entrambi <code>true</code> oppure <code>false</code>. Il valore predefinito è <code>false</code>. Se <code>true</code>, Duo invia automaticamente una richiesta di accesso push al telefono dell'utente, tornando a una chiamata telefonica se non è disponibile il push. Si noti che in questo modo l'autenticazione con codice di accesso viene disattivata. Se <code>false</code>, all'utente viene richiesto di scegliere un metodo di autenticazione.</p> <p>Se configurato con <code>autopush = true</code>, si consiglia l'impostazione <code>max-prompts = 1</code>.</p>	
-max-prompts	<p>Se un utente non riesce ad autenticarsi con un secondo fattore, Duo richiede all'utente di eseguire nuovamente l'autenticazione. Questa opzione consente di impostare il numero massimo di richieste visualizzate da Duo prima di negare l'accesso. Deve essere 1, 2, o 3. Il valore predefinito è 1.</p> <p>Ad esempio, quando <code>max-prompts = 1</code>, l'utente deve eseguire correttamente l'autenticazione al primo prompt, mentre se <code>max-prompts = 2</code>, se l'utente immette informazioni errate al prompt iniziale, gli verrà richiesto di eseguire nuovamente l'autenticazione.</p> <p>Se configurato con <code>autopush = true</code>, si consiglia l'impostazione <code>max-prompts = 1</code>.</p> <p>Per una migliore esperienza, un utente con solo autenticazione a chiave pubblica avrà sempre <code>max-prompts</code> impostare su 1.</p>	

-enabled	Attiva l'autenticazione a due fattori Duo. Impostare su <code>true</code> per impostazione predefinita. Quando questa opzione è attivata, l'autenticazione Duo a due fattori viene applicata durante il login SSH in base ai parametri configurati. Quando Duo è disattivato (impostato su <code>false</code> ), l'autenticazione Duo viene ignorata.	
----------	---	--

## Definire ruoli personalizzati

Questi valori vengono forniti con `security login role create` quando si definisce un ruolo personalizzato.

Campo	Descrizione	Il tuo valore
-vserver	(Opzionale) il nome della VM di storage (chiamato vserver nella CLI di ONTAP) associata al ruolo.	
-role	Il nome del ruolo.	
-cmddirname	La directory di comando a cui il ruolo dà accesso. I nomi delle sottodirectory dei comandi devono essere racimati tra virgolette doppie ("). Ad esempio, " <code>volume snapshot</code> ". È necessario immettere <code>DEFAULT</code> per specificare tutte le directory dei comandi.	

-access	<p>(Facoltativo) il livello di accesso per il ruolo. Per le directory dei comandi:</p> <ul style="list-style-type: none"> <li>• none (il valore predefinito per i ruoli personalizzati) nega l'accesso ai comandi nella directory dei comandi</li> <li>• readonly concede l'accesso a show comandi nella directory dei comandi e nelle relative sottodirectory</li> <li>• all concede l'accesso a tutti i comandi nella directory dei comandi e alle relative sottodirectory</li> </ul> <p>Per <i>comandi non intrinseci</i> (comandi che non finiscono in create, modify, delete, o. show):</p> <ul style="list-style-type: none"> <li>• none (il valore predefinito per i ruoli personalizzati) nega l'accesso al comando</li> <li>• readonly non applicabile</li> <li>• all concede l'accesso al comando</li> </ul> <p>Per concedere o negare l'accesso ai comandi intrinseci, è necessario specificare la directory dei comandi.</p>	
-query	<p>(Facoltativo) oggetto query utilizzato per filtrare il livello di accesso, specificato sotto forma di un'opzione valida per il comando o per un comando nella directory dei comandi. Racchiudere l'oggetto di query tra virgolette doppie ("). Ad esempio, se la directory dei comandi è volume, l'oggetto query "-aggr aggr0" consentirebbe l'accesso a aggr0 solo aggregato.</p>	

### Associare una chiave pubblica a un account utente

Questi valori vengono forniti con `security login publickey create` Quando si associa una chiave pubblica SSH a un account utente.

Campo	Descrizione	Il tuo valore
-vserver	(Facoltativo) il nome della VM di storage a cui l'account accede.	
-username	Il nome utente dell'account. Il valore predefinito, <code>admin</code> , che è il nome predefinito dell'amministratore del cluster.	
-index	Il numero di indice della chiave pubblica. Il valore predefinito è 0 se la chiave è la prima chiave creata per l'account; in caso contrario, il valore predefinito è uno più del numero di indice più alto esistente per l'account.	
-publickey	La chiave pubblica OpenSSH. Racchiudere la chiave tra virgolette doppie (").	
-role	Il ruolo di controllo degli accessi assegnato all'account.	
-comment	(Facoltativo) testo descrittivo per la chiave pubblica. Racchiudere il testo tra virgolette doppie (").	

-x509-certificate	<p>(Facoltativo) a partire da ONTAP 9.13.1, consente di gestire l'associazione del certificato X.509 con la chiave pubblica SSH.</p> <p>Quando si associa un certificato X.509 alla chiave pubblica SSH, ONTAP verifica la validità del certificato al momento dell'accesso SSH. Se è scaduto o è stato revocato, l'accesso non è consentito e la chiave pubblica SSH associata è disattivata. Valori possibili:</p> <ul style="list-style-type: none"> <li>• <code>install</code>: Installare il certificato X.509 con codifica PEM specificato e associarlo alla chiave pubblica SSH. Includere il testo completo del certificato che si desidera installare.</li> <li>• <code>modify</code>: Aggiornare il certificato X.509 con codifica PEM esistente con il certificato specificato e associarlo alla chiave pubblica SSH. Includere il testo completo del nuovo certificato.</li> <li>• <code>delete</code>: Rimuovere l'associazione esistente del certificato X.509 con la chiave pubblica SSH.</li> </ul>	
-------------------	---	--

## Installare un certificato digitale del server firmato dalla CA

Questi valori vengono forniti con `security certificate generate-csr` Comando quando si genera una richiesta di firma digitale del certificato (CSR) da utilizzare per l'autenticazione di una VM di storage come server SSL.

Campo	Descrizione	Il tuo valore
-common-name	Il nome del certificato, ovvero un nome di dominio completo (FQDN) o un nome comune personalizzato.	

-size	Il numero di bit nella chiave privata. Maggiore è il valore, maggiore sarà la sicurezza della chiave. Il valore predefinito è 2048. I valori possibili sono 512, 1024, 1536, e. 2048.	
-country	Il paese della macchina virtuale di archiviazione, in un codice di due lettere. Il valore predefinito è US. Consultare le pagine man per un elenco di codici.	
-state	Lo stato o la provincia della macchina virtuale di storage.	
-locality	La località della macchina virtuale storage.	
-organization	L'organizzazione della macchina virtuale di storage.	
-unit	L'unità nell'organizzazione della VM di storage.	
-email-addr	L'indirizzo e-mail dell'amministratore del contatto per la VM di storage.	
-hash-function	Funzione di hashing crittografico per la firma del certificato. Il valore predefinito è SHA256. I valori possibili sono SHA1, SHA256, e. MD5.	

Questi valori vengono forniti con `security certificate install` Comando quando si installa un certificato digitale con firma CA da utilizzare per l'autenticazione del cluster o della VM di storage come server SSL. Nella tabella seguente sono riportate solo le opzioni relative alla configurazione dell'account.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della VM di archiviazione su cui deve essere installato il certificato.	



-type	<p>Il tipo di certificato:</p> <ul style="list-style-type: none"> <li>• <code>server</code> per i certificati server e intermedi</li> <li>• <code>client-ca</code> Per il certificato a chiave pubblica della CA principale del client SSL</li> <li>• <code>server-ca</code> Per il certificato a chiave pubblica della CA principale del server SSL di cui ONTAP è un client</li> <li>• <code>client</code> Per un certificato digitale autofirmato o firmato da CA e una chiave privata per ONTAP come client SSL</li> </ul>	
-------	--	--

### Configurare l'accesso al controller di dominio Active Directory

Questi valori vengono forniti con `security login domain-tunnel create` Comando quando è già stato configurato un server SMB per una macchina virtuale per lo storage dei dati e si desidera configurare la macchina virtuale per lo storage come gateway o *tunnel* per l'accesso al cluster da parte del controller di dominio Active Directory.

Campo	Descrizione	Il tuo valore
-vserver	Nome della VM di storage per cui è stato configurato il server SMB.	

Questi valori vengono forniti con `vserver active-directory create` Comando quando non è stato configurato un server SMB e si desidera creare un account di un computer VM di archiviazione nel dominio Active Directory.


Campo	Descrizione	Il tuo valore
-vserver	Il nome della VM di storage per cui si desidera creare un account di computer Active Directory.	
-account-name	Il nome NetBIOS dell'account del computer.	
-domain	Il nome di dominio completo (FQDN).	

-ou	L'unità organizzativa nel dominio. Il valore predefinito è CN=Computers. ONTAP aggiunge questo valore al nome di dominio per produrre il nome distinto di Active Directory.	
-----	---	--

## Configurare l'accesso al server LDAP o NIS

Questi valori vengono forniti con `vserver services name-service ldap client create` Comando quando si crea una configurazione del client LDAP per la VM di storage.

Nella seguente tabella sono riportate solo le opzioni relative alla configurazione dell'account:

Campo	Descrizione	Il tuo valore
-vserver	Nome della VM di storage per la configurazione client.	
-client-config	Il nome della configurazione del client.	
-ldap-servers	Elenco separato da virgole di indirizzi IP e nomi host per i server LDAP a cui si connette il client.	
-schema	Lo schema utilizzato dal client per eseguire query LDAP.	
-use-start-tls	<p>Se il client utilizza Start TLS per crittografare la comunicazione con il server LDAP (<code>true</code> oppure <code>false</code>).</p> <div>  <p>Start TLS è supportato solo per l'accesso alle macchine virtuali storage dei dati. Non è supportato per l'accesso alle VM di amministrazione dello storage.</p> </div>	

Questi valori vengono forniti con `vserver services name-service ldap create` Comando quando si associa una configurazione client LDAP alla VM di storage.

Campo	Descrizione	Il tuo valore
-------	-------------	---------------

<code>-vserver</code>	Nome della VM di storage a cui deve essere associata la configurazione client.	
<code>-client-config</code>	Il nome della configurazione del client.	
<code>-client-enabled</code>	Se la VM di storage può utilizzare la configurazione del client LDAP (true oppure false).	

Questi valori vengono forniti con `vserver services name-service nis-domain create` Quando crei una configurazione di dominio NIS su una VM di storage.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Nome della VM di storage su cui deve essere creata la configurazione del dominio.	
<code>-domain</code>	Il nome del dominio.	
<code>-active</code>	Se il dominio è attivo (true oppure false).	
<code>-servers</code>	<b>ONTAP 9.0, 9.1:</b> Un elenco separato da virgole di indirizzi IP per i server NIS utilizzati dalla configurazione del dominio.	
<code>-nis-servers</code>	Elenco separato da virgole di indirizzi IP e nomi host per i server NIS utilizzati dalla configurazione di dominio.	

Questi valori vengono forniti con `vserver services name-service ns-switch create` quando si specifica l'ordine di ricerca per le origini del servizio nome.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della VM di storage su cui deve essere configurato l'ordine di ricerca del servizio dei nomi.	

-database	<p>Il database name service:</p> <ul style="list-style-type: none"> <li>• <code>hosts</code> Per file e servizi di nomi DNS</li> <li>• <code>group</code> Per file, LDAP e NIS name service</li> <li>• <code>passwd</code> Per file, LDAP e NIS name service</li> <li>• <code>netgroup</code> Per file, LDAP e NIS name service</li> <li>• <code>namemap</code> Per file e servizi di nomi LDAP</li> </ul>	
-sources	<p>L'ordine in cui cercare le origini del servizio dei nomi (in un elenco separato da virgole):</p> <ul style="list-style-type: none"> <li>• <code>files</code></li> <li>• <code>dns</code></li> <li>• <code>ldap</code></li> <li>• <code>nis</code></li> </ul>	

## Configurare l'accesso SAML

A partire da ONTAP 9.3, si forniscono questi valori con `security saml-sp create` Comando per configurare l'autenticazione SAML.

Campo	Descrizione	Il tuo valore
-idp-uri	L'indirizzo FTP o HTTP dell'host IdP (Identity Provider) da cui è possibile scaricare i metadati IdP.	
-sp-host	Il nome host o l'indirizzo IP dell'host del provider di servizi SAML (sistema ONTAP). Per impostazione predefinita, viene utilizzato l'indirizzo IP della LIF di gestione del cluster.	

<code>-cert-ca e. -cert-serial, o. -cert-common-name</code>	I dettagli del certificato del server dell'host del provider di servizi (sistema ONTAP). È possibile immettere l'autorità di certificazione (CA) di emissione del certificato del provider di servizi e il numero di serie del certificato oppure il nome comune del certificato del server.	
<code>-verify-metadata-server</code>	Se l'identità del server di metadati IdP deve essere convalidata <code>true</code> oppure <code>false</code> ). La procedura consigliata consiste nell'impostare sempre questo valore su <code>true</code> .	

## Creare account di accesso

### Panoramica sulla creazione degli account di accesso

È possibile attivare gli account di amministratore SVM e cluster locali o remoti. Un account locale è un account in cui le informazioni sull'account, la chiave pubblica o il certificato di protezione risiedono nel sistema di storage. Le informazioni sull'account AD vengono memorizzate in un controller di dominio. Gli account LDAP e NIS risiedono sui server LDAP e NIS.

#### Amministratori di cluster e SVM

Un *amministratore del cluster* accede alla SVM amministrativa per il cluster. La SVM amministrativa e un amministratore del cluster con il nome riservato `admin` vengono creati automaticamente quando viene configurato il cluster.

Un amministratore del cluster con l'impostazione predefinita `admin` il ruolo può amministrare l'intero cluster e le relative risorse. L'amministratore del cluster può creare ulteriori amministratori del cluster con ruoli diversi in base alle esigenze.

Un *amministratore SVM* accede a una SVM di dati. L'amministratore del cluster crea gli amministratori SVM e SVM dei dati in base alle necessità.

Agli amministratori di SVM viene assegnato il `vsadmin` ruolo per impostazione predefinita. L'amministratore del cluster può assegnare ruoli diversi agli amministratori SVM in base alle esigenze.

### Convenzioni di naming

I seguenti nomi generici non possono essere utilizzati per gli account di amministratori di cluster remoti e SVM:

- "adm"
- "contenitore"
- "cli"
- "demone"

- "ftp"
- "giochi"
- "arresta"
- "lp"
- "e-mail"
- "uomo"
- "naroot"
- "NetApp"
- "notizie"
- "nessuno"
- "operatore"
- "radice"
- "arresto"
- "sshd"
- "sincronizza"
- "sis"
- "uucp"
- "www"

## Ruoli Uniti

Se si abilitano più account remoti per lo stesso utente, all'utente viene assegnata l'Unione di tutti i ruoli specificati per gli account. Ovvero, se viene assegnato un account LDAP o NIS `vsadmin` E all'account di gruppo `ad` per lo stesso utente viene assegnato il `vsadmin-volume` Ruolo, l'utente ad effettua l'accesso con il più inclusivo `vsadmin` funzionalità. Si dice che i ruoli siano *merged*.

## Abilitare l'accesso all'account locale

### Attiva la panoramica dell'accesso all'account locale

Un account locale è un account in cui le informazioni sull'account, la chiave pubblica o il certificato di protezione risiedono nel sistema di storage. È possibile utilizzare `security login create` Comando per consentire agli account locali di accedere a un amministratore o a una SVM di dati.

### Abilitare l'accesso all'account password

È possibile utilizzare `security login create` Comando per consentire agli account amministratore di accedere a un SVM di amministrazione o dati con una password. La password viene richiesta dopo aver immesso il comando.

### A proposito di questa attività

Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare `security login modify` per aggiungere il ruolo in un secondo momento.

**Prima di iniziare**

Per eseguire questa attività, è necessario essere un amministratore del cluster.

**Fase**

- 1. Abilitare gli account dell'amministratore locale per accedere a una SVM utilizzando una password:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

Per la sintassi completa dei comandi, vedere "foglio di lavoro".

Il seguente comando attiva l'account amministratore del cluster admin1 con il predefinito backup Ruolo di accesso alla SVM amministrativaengCluster utilizzo di una password. La password viene richiesta dopo aver immesso il comando.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
admin1 -application ssh -authmethod password -role backup
```

**Abilitare gli account a chiave pubblica SSH**

È possibile utilizzare security login create Comando per consentire agli account amministratore di accedere a una SVM amministrativa o di dati con una chiave pubblica SSH.

**A proposito di questa attività**

- Prima che l'account possa accedere a SVM, è necessario associare la chiave pubblica all'account.

[Associazione di una chiave pubblica a un account utente](#)

È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare security login modify per aggiungere il ruolo in un secondo momento.

Se si desidera attivare la modalità FIPS sul cluster, gli account a chiave pubblica SSH esistenti senza gli algoritmi a chiave supportati devono essere riconfigurati con un tipo di chiave supportato. Gli account devono essere riconfigurati prima di attivare FIPS, altrimenti l'autenticazione dell'amministratore non avrà esito positivo.

La seguente tabella indica gli algoritmi del tipo di chiave host supportati per le connessioni SSH ONTAP. Questi tipi di chiave non si applicano alla configurazione dell'autenticazione pubblica SSH.

Release di ONTAP	Tipi di chiave supportati in modalità FIPS	Tipi di chiave supportati in modalità non FIPS
9.11.1 e versioni successive	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 + rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa

9.10.1 e versioni precedenti	ecdsa-sha2-nistp256 + ssh-ed25519	ecdsa-sha2-nistp256 + ssh-ed25519 + ssh-dss + ssh-rsa
------------------------------	-----------------------------------	---



Il supporto per l'algoritmo della chiave host ssh-ed25519 viene rimosso a partire da ONTAP 9.11.1.

Per ulteriori informazioni, vedere ["Configurare la sicurezza di rete utilizzando FIPS"](#).

## Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

## Fase

1. Abilitare gli account dell'amministratore locale per accedere a una SVM utilizzando una chiave pubblica SSH:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

Il seguente comando attiva l'account amministratore SVM `svmadmin1` con il predefinito `vsadmin-volume` Ruolo per accedere a `SVMengData1` Utilizzando una chiave pubblica SSH:

```
cluster1::>security login create -vserver engData1 -user-or-group-name
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

## Al termine

Se non è stata associata una chiave pubblica all'account amministratore, è necessario farlo prima che l'account possa accedere a SVM.

## Associazione di una chiave pubblica a un account utente

### Abilitare gli account MFA (Multiple Factor Authentication)

## Panoramica dell'autenticazione a più fattori

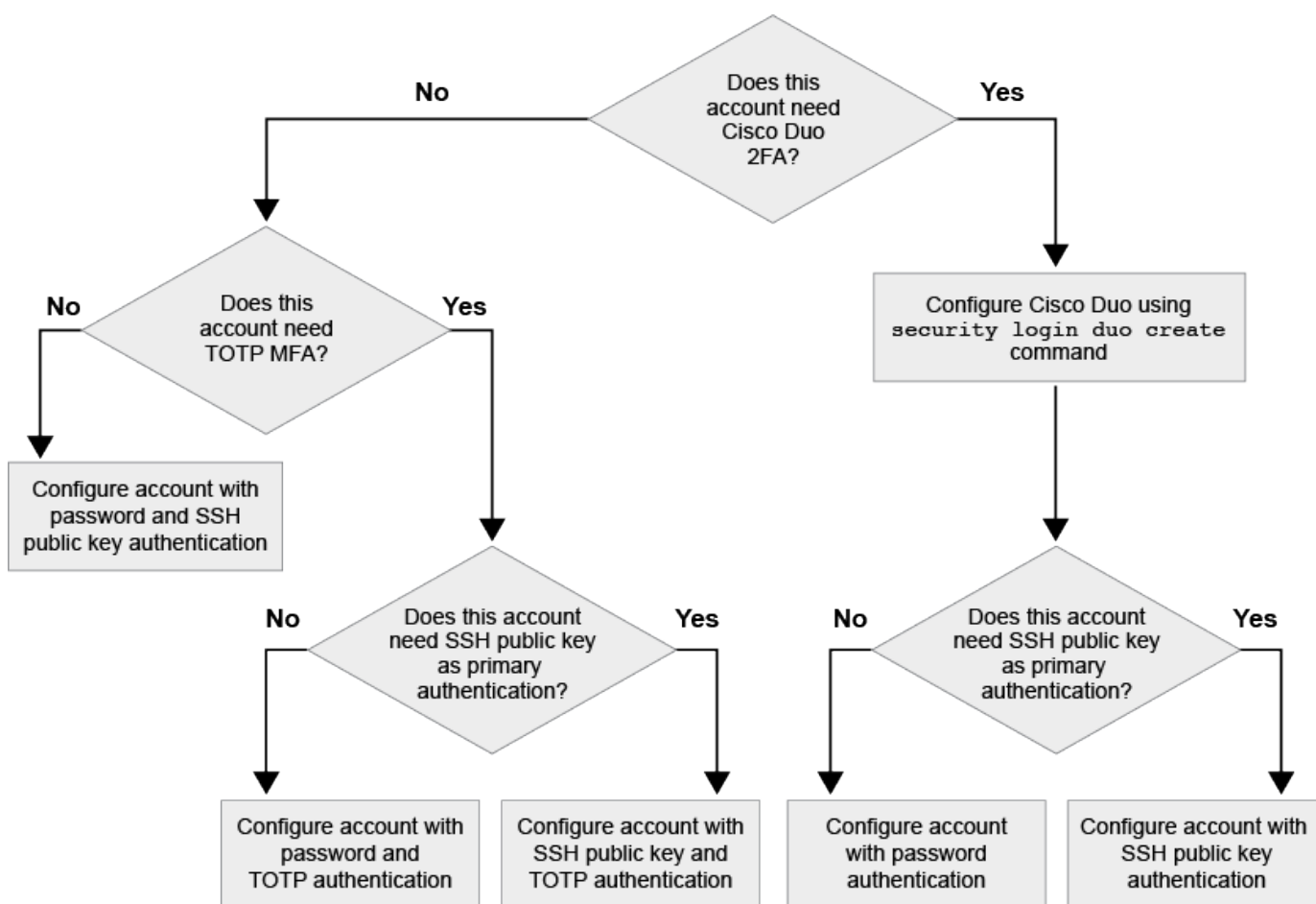
La Multifactor Authentication (MFA) consente di migliorare la sicurezza richiedendo agli utenti di fornire due metodi di autenticazione per l'accesso a una VM di amministrazione o per lo storage dei dati.

A seconda della versione di ONTAP in uso, è possibile utilizzare una combinazione di chiave pubblica SSH, una password utente e una password monouso (TOTP) basata sul tempo per l'autenticazione multifattore. Quando si attiva e si configura Cisco Duo (ONTAP 9.14.1 e versioni successive), questo metodo funge da metodo di autenticazione aggiuntivo, che integra i metodi esistenti per tutti gli utenti.



Disponibile a partire da...	Primo metodo di autenticazione	Secondo metodo di autenticazione
ONTAP 9.14.1	Chiave pubblica SSH	TTP
	User Password (Password utente)	TTP
	Chiave pubblica SSH	Cisco Duo
	Password utente	Cisco Duo
ONTAP 9.13.1	Chiave pubblica SSH	TTP
	Password utente	TTP
ONTAP 9.3	Chiave pubblica SSH	Password utente

Se MFA è configurato, l'amministratore del cluster deve prima abilitare l'account utente locale, quindi l'account deve essere configurato dall'utente locale.



### Abilitare l'autenticazione a più fattori

L'autenticazione a più fattori (MFA) consente di migliorare la sicurezza richiedendo agli utenti di fornire due metodi di autenticazione per accedere a un'SVM amministrativa o di dati.

### A proposito di questa attività

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare `security login modify` per aggiungere il ruolo in un secondo momento.

#### "Modifica del ruolo assegnato a un amministratore"

- Se si utilizza una chiave pubblica per l'autenticazione, è necessario associare la chiave pubblica all'account prima che l'account possa accedere a SVM.

#### "Associare una chiave pubblica a un account utente"

È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- A partire da ONTAP 9.12.1, è possibile utilizzare i dispositivi di autenticazione hardware di Yubikey per l'autenticazione MFA del client SSH utilizzando gli standard di autenticazione FIDO2 (Fast Identity Online) o Personal Identity Verification (PIV).

### Abilitare MFA con chiave pubblica SSH e password utente

A partire da ONTAP 9.3, un amministratore del cluster può configurare account utente locali per l'accesso con MFA utilizzando una chiave pubblica SSH e una password utente.

1. Abilitare MFA sull'account utente locale con chiave pubblica SSH e password utente:

```
security login create -vserver <svm_name> -user-or-group-name
<user_name> -application ssh -authentication-method <password|publickey>
-role admin -second-authentication-method <password|publickey>
```

Il seguente comando richiede l'account amministratore SVM `admin2` con il predefinito `admin` Ruolo di accesso a `SVMengData1` Con una chiave pubblica SSH e una password utente:

```
cluster-1::> security login create -vserver engData1 -user-or-group-name
admin2 -application ssh -authentication-method publickey -role admin
-second-authentication-method password
```

Please enter a password for user 'admin2':

Please enter it again:

Warning: To use public-key authentication, you must create a public key for user "admin2".

### Abilitare MFA con TOTP

A partire da ONTAP 9.13.1, è possibile migliorare la sicurezza richiedendo agli utenti locali di accedere a un server di amministrazione o a una SVM di dati con una chiave pubblica SSH o una password utente e una password monouso (TOTP) basata sul tempo. Una volta abilitato l'account MFA con TOTP, l'utente locale deve effettuare l'accesso a. ["completare la configurazione"](#).

TOTP è un algoritmo per computer che utilizza l'ora corrente per generare una password monouso. Se si

utilizza il protocollo TOTP, si tratta sempre della seconda forma di autenticazione dopo la chiave pubblica SSH o la password dell'utente.

### **Prima di iniziare**

Per eseguire queste attività, è necessario essere un amministratore dello storage.

### **Fasi**

È possibile impostare MFA su con una password utente o una chiave pubblica SSH come primo metodo di autenticazione e TOTP come secondo metodo di autenticazione.

## Abilitare MFA con password utente e TOTP

1. Abilitare un account utente per l'autenticazione a più fattori con una password utente e TOTP.

### Per nuovi account utente

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

### Per gli account utente esistenti

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
password -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Verificare che MFA con TOTP sia attivato:

```
security login show
```

## Abilitare MFA con chiave pubblica SSH e TOTP

1. Abilitare un account utente per l'autenticazione a più fattori con una chiave pubblica SSH e TOTP.

### Per nuovi account utente

```
security login create -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

### Per gli account utente esistenti

```
security login modify -vserver <svm_name> -user-or-group-name  
<user_or_group_name> -application ssh -authentication-method  
publickey -second-authentication-method totp -role <role> -comment  
<comment>
```

2. Verificare che MFA con TOTP sia attivato:

```
security login show
```

### Al termine

- Se non è stata associata una chiave pubblica all'account amministratore, è necessario farlo prima che l'account possa accedere a SVM.

["Associazione di una chiave pubblica a un account utente"](#)

- L'utente locale deve effettuare l'accesso per completare la configurazione MFA con TOTP.

["Configurare l'account utente locale per MFA con TOTP"](#)

### Informazioni correlate

Scopri di più ["Autenticazione multifattore in ONTAP 9 \(TR-4647\)"](#).

### Configurare l'account utente locale per MFA con TOTP

A partire da ONTAP 9.13.1, gli account utente possono essere configurati con autenticazione multifattore (MFA) utilizzando una password monouso (TTP) basata sul tempo.

### Prima di iniziare

- L'amministratore dello storage deve ["Abilitare MFA con TOTP"](#) come secondo metodo di autenticazione per l'account utente.
- Il metodo di autenticazione dell'account utente principale deve essere una password utente o una chiave SSH pubblica.
- È necessario configurare l'applicazione TOTP per il funzionamento con lo smartphone e creare la chiave segreta TOTP.

TOTP è supportato da diverse applicazioni di autenticazione come Google Authenticator.

### Fasi

1. Accedere all'account utente con il metodo di autenticazione corrente.

Il metodo di autenticazione corrente deve essere una password utente o una chiave pubblica SSH.

2. Creare la configurazione TOTP sull'account:

```
security login totp create -vserver "<svm_name>" -username  
"<account_username >"
```

3. Verificare che la configurazione TOTP sia attivata sull'account:

```
security login totp show -vserver "<svm_name>" -username  
"<account_username>"
```

### Reimpostare la chiave segreta TOTP

Per proteggere la sicurezza del tuo account, se la tua chiave segreta TOTP viene compromessa o persa, devi disattivarla e crearne una nuova.

### Reimpostare il TOTP se la chiave viene compromessa

Se la chiave segreta TOTP è compromessa, ma si dispone ancora dell'accesso, è possibile rimuovere la chiave compromessa e crearne una nuova.

1. Accedere all'account utente con la password utente o la chiave pubblica SSH e la chiave segreta TOTP compromessa.
2. Rimuovere la chiave segreta TOTP compromessa:

```
security login totp delete -vserver <svm_name> -username  
<account_username>
```

3. Creare una nuova chiave segreta TOTP:

```
security login totp create -vserver <svm_name> -username  
<account_username>
```

4. Verificare che la configurazione TOTP sia attivata sull'account:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

### Ripristinare il TOTP se la chiave viene persa

Se la chiave segreta TOTP viene persa, contattare l'amministratore dello storage per ["disattivare la chiave"](#). Una volta disattivata la chiave, è possibile utilizzare il primo metodo di autenticazione per accedere e configurare un nuovo TOTP.

### Prima di iniziare

La chiave segreta TOTP deve essere disattivata da un amministratore dello storage. Se non si dispone di un account amministratore dello storage, contattare l'amministratore dello storage per disattivare la chiave.

### Fasi

1. Una volta disattivato il segreto TOTP da un amministratore dello storage, utilizzare il metodo di autenticazione principale per accedere all'account locale.

## 2. Creare una nuova chiave segreta TOTP:

```
security login totp create -vserver <svm_name> -username  
<account_username >
```

## 3. Verificare che la configurazione TOTP sia attivata sull'account:

```
security login totp show -vserver <svm_name> -username  
<account_username>
```

### Disattiva la chiave segreta TOTP per l'account locale

Se la chiave segreta TOTP (Time-Based One-Time Password) di un utente locale viene persa, la chiave persa deve essere disattivata da un amministratore dello storage prima che l'utente possa creare una nuova chiave segreta TOTP.

#### A proposito di questa attività

Questa attività può essere eseguita solo da un account amministratore del cluster.

#### Fase

### 1. Disattivare la chiave segreta TOTP:

```
security login totp delete -vserver "<svm_name>" -username  
"<account_username>"
```

### Abilitare gli account dei certificati SSL

È possibile utilizzare `security login create` Comando per consentire agli account amministratore di accedere a un SVM di amministrazione o dati con un certificato SSL.

#### A proposito di questa attività

- È necessario installare un certificato digitale del server firmato dalla CA prima che l'account possa accedere alla SVM.

#### [Creazione e installazione di un certificato server firmato dalla CA](#)

È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile aggiungerlo successivamente con `security login modify` comando.

#### [Modifica del ruolo assegnato a un amministratore](#)



Per gli account degli amministratori del cluster, l'autenticazione del certificato è supportata con `http`, `ontapi`, e. `rest` applicazioni. Per gli account amministratore SVM, l'autenticazione del certificato è supportata solo con `ontapi` e. `rest` applicazioni.

## Fase

1. Abilitare gli account dell'amministratore locale per accedere a una SVM utilizzando un certificato SSL:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Per la sintassi completa dei comandi, vedere ["Man page di ONTAP per release"](#).

Il seguente comando attiva l'account amministratore SVM `svmadmin2` con l'impostazione predefinita `vsadmin` Ruolo per accedere a `SVMengData2` Utilizzando un certificato digitale SSL.

```
cluster1::>security login create -vserver engData2 -user-or-group-name  
svmadmin2 -application ontapi -authmethod cert
```

## Al termine

Se non è stato installato un certificato digitale del server firmato dalla CA, è necessario farlo prima che l'account possa accedere alla SVM.

[Creazione e installazione di un certificato server firmato dalla CA](#)

## Abilitare l'accesso all'account Active Directory

È possibile utilizzare `security login create` Comando per abilitare gli account utente o di gruppo Active Directory (ad) per accedere a un SVM di amministrazione o dati. Qualsiasi utente del gruppo ad può accedere a SVM con il ruolo assegnato al gruppo.

### A proposito di questa attività

- È necessario configurare l'accesso del controller di dominio ad al cluster o alla SVM prima che l'account possa accedere alla SVM.

#### [Configurazione dell'accesso al controller di dominio Active Directory](#)

È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- A partire da ONTAP 9.13.1, è possibile utilizzare una chiave pubblica SSH come metodo di autenticazione primario o secondario con una password utente ad.

Se si sceglie di utilizzare una chiave pubblica SSH come autenticazione principale, non viene eseguita alcuna autenticazione ad.

- A partire da ONTAP 9.11.1, è possibile utilizzare ["LDAP fast bind per l'autenticazione nsswitch"](#) Se supportato dal server LDAP ad.
- Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è



possibile utilizzare `security login modify` per aggiungere il ruolo in un secondo momento.

### Modifica del ruolo assegnato a un amministratore



L'accesso all'account DEL GRUPPO DI ANNUNCI è supportato solo con SSH, ontapi, e. rest applicazioni. I gruppi DI ANNUNCI NON sono supportati con l'autenticazione a chiave pubblica SSH, comunemente utilizzata per l'autenticazione a più fattori.

#### Prima di iniziare

- Il tempo del cluster deve essere sincronizzato entro cinque minuti dal tempo sul controller di dominio ad.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

#### Fase

1. Abilitare gli account amministratore di gruppo o utente ad per accedere a una SVM:

##### Per utenti ad:

Versione di ONTAP	Autenticazione primaria	Autenticazione secondaria	Comando
9.13.1 e versioni successive	Chiave pubblica	Nessuno	<pre>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application ssh -authentication-method publickey -role &lt;role&gt;</pre>

Versione di ONTAP	Autenticazione primaria	Autenticazione secondaria	Comando
9.13.1 e versioni successive	Dominio	Chiave pubblica	<p><b>Per un nuovo utente</b></p> <pre>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application ssh -authentication-method domain -second -authentication-method publickey -role &lt;role&gt;</pre> <p><b>Per un utente esistente</b></p> <pre>security login modify -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application ssh -authentication-method domain -second -authentication-method publickey -role &lt;role&gt;</pre>
9.0 e versioni successive	Dominio	Nessuno	<pre>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application &lt;application&gt; -authentication-method domain -role &lt;role&gt; -comment &lt;comment&gt; [-is-ldap- fastbind true]</pre>

**Per gruppi ad:**

Versione di ONTAP	Autenticazione primaria	Autenticazione secondaria	Comando
9.0 e versioni successive	Dominio	Nessuno	<pre>security login create -vserver &lt;svm_name&gt; -user-or-group-name &lt;user_name&gt; -application &lt;application&gt; -authentication-method domain -role &lt;role&gt; -comment &lt;comment&gt; [-is-ldap- fastbind true]</pre>

Per la sintassi completa dei comandi, vedere ["Fogli di lavoro per l'autenticazione dell'amministratore e la configurazione RBAC"](#)

## Al termine

Se non è stato configurato l'accesso del controller di dominio ad al cluster o alla SVM, è necessario farlo prima che l'account possa accedere alla SVM.

### [Configurazione dell'accesso al controller di dominio Active Directory](#)

## Abilitare l'accesso all'account LDAP o NIS

È possibile utilizzare `security login create` Comando per abilitare gli account utente LDAP o NIS per accedere a un SVM di amministrazione o dati. Se non è stato configurato l'accesso al server LDAP o NIS alla SVM, è necessario farlo prima che l'account possa accedere alla SVM.

### A proposito di questa attività

- Gli account di gruppo non sono supportati.
- È necessario configurare l'accesso al server LDAP o NIS alla SVM prima che l'account possa accedere alla SVM.

### [Configurazione dell'accesso al server LDAP o NIS](#)

È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare `security login modify` per aggiungere il ruolo in un secondo momento.

### [Modifica del ruolo assegnato a un amministratore](#)

- A partire da ONTAP 9.4, l'autenticazione multifattore (MFA) è supportata per gli utenti remoti su server LDAP o NIS.
- A partire da ONTAP 9.11.1, è possibile utilizzare ["LDAP fast bind per l'autenticazione nsswitch"](#) Se supportato dal server LDAP.
- A causa di un problema LDAP noto, non utilizzare ' : ' (Due punti) carattere in qualsiasi campo delle informazioni dell'account utente LDAP (ad esempio, `gecos`, ``userPassword`` e così via). In caso contrario, l'operazione di ricerca non riuscirà per quell'utente.

## Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

## Fasi

1. Abilitare gli account utente o gruppo LDAP o NIS per accedere a una SVM:

```
security login create -vserver SVM_name -user-or-group-name user_name
-application application -authmethod nsswitch -role role -comment comment -is
-ns-switch-group yes|no [-is-ldap-fastbind true]
```

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

### ["Creazione o modifica degli account di accesso"](#)

Il seguente comando attiva l'account amministratore del cluster LDAP o NIS `quest2` con il predefinito backup Ruolo di accesso alla SVM amministrativa `engCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
quest2 -application ssh -authmethod nsswitch -role backup
```

## 2. Abilitare l'accesso MFA per gli utenti LDAP o NIS:

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

Il metodo di autenticazione può essere specificato come `publickey` e secondo metodo di autenticazione `as nsswitch`.

L'esempio seguente mostra l'attivazione dell'autenticazione MFA:

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

### Al termine

Se non è stato configurato l'accesso al server LDAP o NIS alla SVM, è necessario farlo prima che l'account possa accedere alla SVM.

### [Configurazione dell'accesso al server LDAP o NIS](#)

## Gestire i ruoli di controllo degli accessi

### Panoramica sui ruoli di controllo degli accessi

Il ruolo assegnato a un amministratore determina i comandi a cui l'amministratore ha accesso. Il ruolo viene assegnato quando si crea l'account per l'amministratore. È possibile assegnare un ruolo diverso o definire ruoli personalizzati in base alle esigenze.

### Modificare il ruolo assegnato a un amministratore

È possibile utilizzare `security login modify` Comando per modificare il ruolo di un account di amministratore di cluster o SVM. È possibile assegnare un ruolo predefinito o personalizzato.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

### Fase

1. Modificare il ruolo di un amministratore di cluster o SVM:

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

### "Creazione o modifica degli account di accesso"

Il seguente comando modifica il ruolo dell'account amministratore del cluster ad DOMAIN1\guest1 al predefinito readonly ruolo.

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

Il seguente comando modifica il ruolo degli account amministratore SVM nell'account di gruppo ad DOMAIN1\adgroup al personalizzato vol\_role ruolo.

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

## Definire ruoli personalizzati

È possibile utilizzare `security login role create` per definire un ruolo personalizzato. È possibile eseguire il comando tutte le volte necessarie per ottenere la combinazione esatta di funzionalità che si desidera associare al ruolo.

### A proposito di questa attività

- Un ruolo, predefinito o personalizzato, concede o nega l'accesso ai comandi ONTAP o alle directory dei comandi.

Una directory di comandi (`volume`, ad esempio) è un gruppo di sottodirectory di comandi e comandi correlati. Ad eccezione di quanto descritto in questa procedura, la concessione o il rifiuto dell'accesso a una directory di comandi concede o nega l'accesso a ciascun comando nella directory e nelle relative sottodirectory.

- L'accesso a comandi o sottodirectory specifici sovrascrive l'accesso alla directory principale.

Se un ruolo viene definito con una directory di comandi e quindi viene definito nuovamente con un livello di accesso diverso per un comando specifico o per una sottodirectory della directory principale, il livello di accesso specificato per il comando o la sottodirectory sovrascrive quello della directory principale.



Non è possibile assegnare a un amministratore SVM un ruolo che dia accesso a una directory di comandi o comandi disponibile solo per `admin` amministratore del cluster, ad esempio `security directory dei comandi`.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

**Fase**

1. Definire un ruolo personalizzato:

```
security login role create -vserver SVM_name -role role -cmddirname
command_or_directory_name -access access_level -query query
```

Per la sintassi completa dei comandi, vedere "foglio di lavoro".

I seguenti comandi assegnano a vol\_role accesso completo ai comandi in volume directory dei comandi e accesso in sola lettura ai comandi in volume snapshot sottodirectory.

```
cluster1::>security login role create -role vol_role -cmddirname
"volume" -access all

cluster1::>security login role create -role vol_role -cmddirname "volume
snapshot" -access readonly
```

I seguenti comandi assegnano a SVM\_storage accesso in sola lettura ai comandi in storage directory dei comandi, nessun accesso ai comandi in storage encryption sottodirectory e accesso completo a storage aggregate plex offline comando non intrinseco.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

**Ruoli predefiniti per gli amministratori del cluster**

I ruoli predefiniti per gli amministratori dei cluster devono soddisfare la maggior parte delle esigenze. È possibile creare ruoli personalizzati in base alle necessità. Per impostazione predefinita, a un amministratore del cluster viene assegnato il valore predefinito admin ruolo.

La seguente tabella elenca i ruoli predefiniti per gli amministratori del cluster:

Questo ruolo...	Dispone di questo livello di accesso...	Alle seguenti directory di comandi o comandi
amministratore	tutto	Tutte le directory dei comandi (DEFAULT)

admin-no-fsa (disponibile a partire da ONTAP 9.12.1)	Lettura/scrittura	<ul style="list-style-type: none"> <li>• Tutte le directory dei comandi (DEFAULT)</li> <li>• security login rest-role</li> <li>• security login role</li> </ul>
Di sola lettura	<ul style="list-style-type: none"> <li>• security login rest-role create</li> <li>• security login rest-role delete</li> <li>• security login rest-role modify</li> <li>• security login rest-role show</li> <li>• security login role create</li> <li>• security login role create</li> <li>• security login role delete</li> <li>• security login role modify</li> <li>• security login role show</li> <li>• volume activity-tracking</li> <li>• volume analytics</li> </ul>	Nessuno
volume file show-disk-usage	AutoSupport	tutto
<ul style="list-style-type: none"> <li>• set</li> <li>• system node autosupport</li> </ul>	nessuno	Tutte le altre directory di comando (DEFAULT)
backup	tutto	vserver services ndmp
readonly	volume	nessuno
Tutte le altre directory di comando (DEFAULT)	readonly	tutto

<ul style="list-style-type: none"> <li>• <code>security login password</code></li> </ul> <p>Solo per la gestione della password locale del proprio account utente e delle informazioni sulle chiavi</p> <ul style="list-style-type: none"> <li>• <code>set</code></li> </ul>	nessuno	security
readonly	Tutte le altre directory di comando (DEFAULT)	nessuno



Il `autosupport` il ruolo viene assegnato al predefinito `autosupport` Account, utilizzato da AutoSupport OnDemand. ONTAP impedisce di modificare o eliminare `autosupport` account. ONTAP impedisce inoltre l'assegnazione di `autosupport` ruolo per altri account utente.

### Ruoli predefiniti per gli amministratori SVM

I ruoli predefiniti per gli amministratori SVM devono soddisfare la maggior parte delle esigenze. È possibile creare ruoli personalizzati in base alle necessità. Per impostazione predefinita, a un amministratore SVM viene assegnato il valore predefinito `vsadmin` ruolo.

La seguente tabella elenca i ruoli predefiniti per gli amministratori SVM:

Nome del ruolo	Funzionalità
vsadmin	<ul style="list-style-type: none"> <li>• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente</li> <li>• Gestione dei volumi, ad eccezione degli spostamenti dei volumi</li> <li>• Gestione di quote, <code>qtree</code>, copie Snapshot e file</li> <li>• Gestione delle LUN</li> <li>• Esecuzione delle operazioni SnapLock, ad eccezione dell'eliminazione con privilegi</li> <li>• Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP</li> <li>• Configurazione dei servizi: DNS, LDAP e NIS</li> <li>• Monitoraggio dei lavori</li> <li>• Monitoraggio delle connessioni di rete e dell'interfaccia di rete</li> <li>• Monitoraggio dello stato di salute di SVM</li> </ul>



volume vsadmin	<ul style="list-style-type: none"> <li>• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente</li> <li>• Gestione dei volumi, compresi gli spostamenti dei volumi</li> <li>• Gestione di quote, qtree, copie Snapshot e file</li> <li>• Gestione delle LUN</li> <li>• Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP</li> <li>• Configurazione dei servizi: DNS, LDAP e NIS</li> <li>• Interfaccia di rete di monitoraggio</li> <li>• Monitoraggio dello stato di salute di SVM</li> </ul>
protocollo vsadmin	<ul style="list-style-type: none"> <li>• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente</li> <li>• Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP</li> <li>• Configurazione dei servizi: DNS, LDAP e NIS</li> <li>• Gestione delle LUN</li> <li>• Interfaccia di rete di monitoraggio</li> <li>• Monitoraggio dello stato di salute di SVM</li> </ul>
vsadmin-backup	<ul style="list-style-type: none"> <li>• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente</li> <li>• Gestione delle operazioni NDMP</li> <li>• Creazione di un volume ripristinato in lettura/scrittura</li> <li>• Gestione delle relazioni SnapMirror e delle copie Snapshot</li> <li>• Visualizzazione di volumi e informazioni di rete</li> </ul>

vsadmin-snaplock	<ul style="list-style-type: none"> <li>• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente</li> <li>• Gestione dei volumi, ad eccezione degli spostamenti dei volumi</li> <li>• Gestione di quote, qtree, copie Snapshot e file</li> <li>• Esecuzione di operazioni SnapLock, inclusa l'eliminazione con privilegi</li> <li>• Configurazione dei protocolli: NFS e SMB</li> <li>• Configurazione dei servizi: DNS, LDAP e NIS</li> <li>• Monitoraggio dei lavori</li> <li>• Monitoraggio delle connessioni di rete e dell'interfaccia di rete</li> </ul>
vsadmin-readonly	<ul style="list-style-type: none"> <li>• Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente</li> <li>• Monitoraggio dello stato di salute di SVM</li> <li>• Interfaccia di rete di monitoraggio</li> <li>• Visualizzazione di volumi e LUN</li> <li>• Visualizzazione di servizi e protocolli</li> </ul>

### Controllare l'accesso dell'amministratore

Il ruolo assegnato a un amministratore determina le funzioni che l'amministratore può eseguire con System Manager. System Manager fornisce ruoli predefiniti per gli amministratori dei cluster e gli amministratori delle macchine virtuali dello storage. Il ruolo viene assegnato quando si crea l'account dell'amministratore oppure è possibile assegnarlo in un secondo momento.

A seconda di come è stato attivato l'accesso all'account, potrebbe essere necessario eseguire una delle seguenti operazioni:

- Associare una chiave pubblica a un account locale.
- Installare un certificato digitale del server firmato dalla CA.
- Configurare l'accesso ad, LDAP o NIS.

È possibile eseguire queste attività prima o dopo aver attivato l'accesso all'account.

### Assegnazione di un ruolo a un amministratore

Assegnare un ruolo a un amministratore, come indicato di seguito:

#### Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare ➔ Accanto a **utenti e ruoli**.

3. Selezionare **+ Add** Sotto **utenti**.
4. Specificare un nome utente e selezionare un ruolo nel menu a discesa per **ruolo**.
5. Specificare un metodo di accesso e una password per l'utente.

#### Modifica del ruolo di amministratore

Modificare il ruolo di amministratore, come segue:

##### Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Selezionare il nome dell'utente di cui si desidera modificare il ruolo, quindi fare clic su **:** visualizzato accanto al nome utente.
3. Fare clic su **Edit** (Modifica).
4. Selezionare un ruolo nel menu a discesa per **ruolo**.

## Gestire gli account amministratore

#### Panoramica sulla gestione degli account amministratore

A seconda di come è stato attivato l'accesso all'account, potrebbe essere necessario associare una chiave pubblica a un account locale, installare un certificato digitale del server firmato dalla CA o configurare l'accesso ad, LDAP o NIS. È possibile eseguire tutte queste attività prima o dopo aver attivato l'accesso all'account.

#### Associare una chiave pubblica a un account amministratore

Per l'autenticazione a chiave pubblica SSH, è necessario associare la chiave pubblica a un account amministratore prima che l'account possa accedere a SVM. È possibile utilizzare `security login publickey create` comando per associare una chiave a un account amministratore.

##### A proposito di questa attività

Se si autentica un account su SSH con una password e una chiave pubblica SSH, l'account viene autenticato prima con la chiave pubblica.

##### Prima di iniziare

- È necessario aver generato la chiave SSH.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

##### Fasi

1. Associare una chiave pubblica a un account amministratore:

```
security login publickey create -vserver SVM_name -username user_name -index  
index -publickey certificate -comment comment
```

Per la sintassi completa dei comandi, vedere il riferimento al foglio di lavoro per "[Associazione di una chiave pubblica a un account utente](#)".

## 2. Verificare la modifica visualizzando la chiave pubblica:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

### Esempio

Il seguente comando associa una chiave pubblica all'account amministratore di SVM svmadmin1 Per SVM engData1. Alla chiave pubblica viene assegnato il numero di indice 5.

```
cluster1::> security login publickey create -vserver engData1 -username  
svmadmin1 -index 5 -publickey  
"<key text>"
```

## Gestire le chiavi pubbliche SSH e i certificati X.509 per un account amministratore

Per una maggiore sicurezza di autenticazione SSH con gli account amministratore, è possibile utilizzare `security login publickey` Set di comandi per gestire la chiave pubblica SSH e la sua associazione con i certificati X.509.

### Associare una chiave pubblica e un certificato X.509 a un account amministratore

A partire da ONTAP 9.13.1, è possibile associare un certificato X.509 alla chiave pubblica associata all'account amministratore. In questo modo si ottiene la sicurezza aggiuntiva dei controlli di scadenza o revoca del certificato al momento dell'accesso SSH per quell'account.

### A proposito di questa attività

Se si autentica un account su SSH con una chiave pubblica SSH e un certificato X.509, ONTAP verifica la validità del certificato X.509 prima di autenticarsi con la chiave pubblica SSH. L'accesso SSH verrà rifiutato se il certificato è scaduto o revocato e la chiave pubblica verrà disattivata automaticamente.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- È necessario aver generato la chiave SSH.
- Se è necessario controllare solo la scadenza del certificato X.509, è possibile utilizzare un certificato autofirmato.
- Se è necessario controllare la scadenza e la revoca del certificato X.509:
  - È necessario aver ricevuto il certificato da un'autorità di certificazione (CA).
  - È necessario installare la catena di certificati (certificati CA intermedi e principali) utilizzando `security certificate install` comandi.
  - Devi attivare OCSP per SSH. Fare riferimento a ["Verificare che i certificati digitali siano validi utilizzando OCSP"](#) per istruzioni.

### Fasi

#### 1. Associare una chiave pubblica e un certificato X.509 a un account amministratore:

```
security login publickey create -vserver SVM_name -username user_name -index  
index -publickey certificate -x509-certificate install
```

Per la sintassi completa dei comandi, vedere il riferimento al foglio di lavoro per ["Associazione di una chiave pubblica a un account utente"](#).

2. Verificare la modifica visualizzando la chiave pubblica:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

### Esempio

Il seguente comando associa una chiave pubblica e un certificato X.509 all'account amministratore SVM svmin2 Per SVM engData2. Alla chiave pubblica viene assegnato il numero di indice 6.

```
cluster1::> security login publickey create -vserver engData2 -username svmin2 -index 6 -publickey "<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

### Rimuovere l'associazione del certificato dalla chiave pubblica SSH per un account amministratore

È possibile rimuovere l'associazione del certificato corrente dalla chiave pubblica SSH dell'account, mantenendo la chiave pubblica.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

1. Rimuovere l'associazione del certificato X.509 da un account amministratore e conservare la chiave pubblica SSH esistente:

```
security login publickey modify -vserver SVM_name -username user_name -index index -x509-certificate delete
```

2. Verificare la modifica visualizzando la chiave pubblica:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

### Esempio

Il comando seguente rimuove l'associazione del certificato X.509 dall'account amministratore SVM svmin2 Per SVM engData2 al numero di indice 6.

```
cluster1::> security login publickey modify -vserver engData2 -username svmin2 -index 6 -x509-certificate delete
```

## Rimuovere la chiave pubblica e l'associazione del certificato da un account amministratore

È possibile rimuovere la chiave pubblica corrente e la configurazione del certificato da un account.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

1. Rimuovere la chiave pubblica e un'associazione di certificati X.509 da un account amministratore:

```
security login publickey delete -vserver SVM_name -username user_name -index index
```

2. Verificare la modifica visualizzando la chiave pubblica:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

### Esempio

Il comando seguente rimuove una chiave pubblica e un certificato X.509 dall'account amministratore SVM svmadmin3 Per SVM engData3 al numero di indice 7.

```
cluster1::> security login publickey delete -vserver engData3 -username svmadmin3 -index 7
```

## Configurare Cisco Duo 2FA per gli accessi SSH

A partire da ONTAP 9.14.1, è possibile configurare ONTAP in modo che utilizzi Cisco Duo per l'autenticazione a due fattori (2FA) durante gli accessi SSH. Duo viene configurato a livello di cluster e si applica a tutti gli account utente per impostazione predefinita. In alternativa, è possibile configurare Duo al livello della VM di storage (precedentemente denominata vserver), nel qual caso si applica solo agli utenti della VM di storage. Se abiliti e configuri Duo, serve come metodo di autenticazione aggiuntivo, che integra i metodi esistenti per tutti gli utenti.

Se si abilita l'autenticazione Duo per gli accessi SSH, gli utenti dovranno registrare un dispositivo al successivo accesso tramite SSH. Per informazioni sulla registrazione, fare riferimento a Cisco Duo ["documentazione di iscrizione"](#).

È possibile utilizzare l'interfaccia della riga di comando di ONTAP per eseguire le seguenti operazioni con Cisco Duo:

- [Configurare Cisco Duo](#)
- [Modificare la configurazione di Cisco Duo](#)
- [Rimuovere la configurazione di Cisco Duo](#)
- [Visualizzare la configurazione di Cisco Duo](#)
- [Rimuovere un gruppo Duo](#)

- [Visualizza i gruppi Duo](#)
- [Ignora autenticazione Duo per gli utenti](#)

## Configurare Cisco Duo

Puoi creare una configurazione di Cisco Duo per l'intero cluster o per una macchina virtuale storage specifica (denominata vserver nell'interfaccia a riga di comando di ONTAP) utilizzando il `security login duo create` comando. A tale scopo, Cisco Duo è abilitato per gli accessi SSH per il cluster o per la VM di storage.

### Fasi

1. Accedere al pannello di amministrazione di Cisco Duo.
2. Andare a **applicazioni > applicazioni UNIX**.
3. Registrare la chiave di integrazione, la chiave segreta e il nome host API.
4. Accedere al proprio account ONTAP utilizzando SSH.
5. Abilitare l'autenticazione Cisco Duo per questa VM di storage, sostituendo le informazioni dell'ambiente ai valori tra parentesi:

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

Per ulteriori informazioni sui parametri richiesti e facoltativi per questo comando, fare riferimento a ["Fogli di lavoro per l'autenticazione dell'amministratore e la configurazione RBAC"](#).

## Modificare la configurazione di Cisco Duo

È possibile modificare il modo in cui Cisco Duo autentica gli utenti (ad esempio, il numero di richieste di autenticazione o il proxy HTTP utilizzato). Se è necessario modificare la configurazione di Cisco Duo per una macchina virtuale di storage (nota come vserver nell'interfaccia CLI di ONTAP), è possibile utilizzare `security login duo modify` comando.

### Fasi

1. Accedere al pannello di amministrazione di Cisco Duo.
2. Andare a **applicazioni > applicazioni UNIX**.
3. Registrare la chiave di integrazione, la chiave segreta e il nome host API.
4. Accedere al proprio account ONTAP utilizzando SSH.
5. Modificare la configurazione di Cisco Duo per questa VM di archiviazione, sostituendo le informazioni aggiornate dell'ambiente ai valori tra parentesi:

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-is-enabled true|false \
-fail-mode safe|secure
```

### Rimuovere la configurazione di Cisco Duo

È possibile rimuovere la configurazione di Cisco Duo, che elimina la necessità per gli utenti SSH di eseguire l'autenticazione utilizzando Duo al momento dell'accesso. Per rimuovere la configurazione di Cisco Duo per una VM di storage (nota come server virtuale nell'interfaccia CLI di ONTAP), è possibile utilizzare `security login duo delete` comando.

#### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Rimuovere la configurazione Cisco Duo per questa VM di archiviazione, sostituendo il nome della VM di archiviazione con `<STORAGE_VM_NAME>`:

```
security login duo delete -vserver <STORAGE_VM_NAME>
```

In questo modo viene eliminata in modo permanente la configurazione di Cisco Duo per questa VM di storage.

### Visualizzare la configurazione di Cisco Duo

È possibile visualizzare la configurazione di Cisco Duo esistente di una macchina virtuale di storage (definita `vserver` nell'interfaccia CLI di ONTAP) utilizzando il `security login duo show` comando.

#### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Mostrare la configurazione di Cisco Duo per questa VM di storage. In alternativa, è possibile utilizzare `vserver` Parametro per specificare una VM di storage, sostituendo il nome della VM di storage con `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

L'output dovrebbe essere simile a quanto segue:



```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

### Creare un gruppo Duo

È possibile richiedere a Cisco Duo di includere solo gli utenti di un determinato Active Directory, LDAP o gruppo di utenti locali nel processo di autenticazione Duo. Se si crea un gruppo Duo, viene richiesta l'autenticazione Duo solo agli utenti del gruppo. È possibile creare un gruppo Duo utilizzando `security login duo group create` comando. Quando si crea un gruppo, è possibile escludere dal processo di autenticazione Duo utenti specifici di tale gruppo.

#### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Creare il gruppo Duo, sostituendo le informazioni del proprio ambiente ai valori tra parentesi. Se si omette `-vserver` il gruppo viene creato a livello di cluster:

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Il nome del gruppo Duo deve corrispondere a un gruppo Active Directory, LDAP o locale. Gli utenti specificati con l'opzione `-exclude-users` Il parametro non verrà incluso nel processo di autenticazione Duo.

### Visualizza i gruppi Duo

È possibile visualizzare le voci di gruppo Cisco Duo esistenti utilizzando `security login duo group show` comando.

#### Fasi

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Mostrare le voci del gruppo Duo, sostituendo le informazioni dell'ambiente con i valori tra parentesi. Se si omette `-vserver` il gruppo viene visualizzato a livello del cluster:

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Il nome del gruppo Duo deve corrispondere a un gruppo Active Directory, LDAP o locale. Gli utenti specificati con l'opzione `-exclude-users` il parametro non viene visualizzato.

### **Rimuovere un gruppo Duo**

È possibile rimuovere una voce di gruppo Duo utilizzando `security login duo group delete` comando. Se si rimuove un gruppo, gli utenti del gruppo non saranno più inclusi nel processo di autenticazione Duo.

#### **Fasi**

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Rimuovere la voce del gruppo Duo, sostituendo le informazioni presenti nell'ambiente in uso con i valori tra parentesi. Se si omette `-vserver` il gruppo viene rimosso a livello di cluster:

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME>
```

Il nome del gruppo Duo deve corrispondere a un gruppo Active Directory, LDAP o locale.

### **Ignora autenticazione Duo per gli utenti**

È possibile escludere tutti gli utenti o utenti specifici dal processo di autenticazione SSH Duo.

### **Escludere tutti gli utenti Duo**

È possibile disattivare l'autenticazione SSH di Cisco Duo per tutti gli utenti.

#### **Fasi**

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Disattiva l'autenticazione Cisco Duo per gli utenti SSH, sostituendo il nome del Vserver con `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled=false
```

### **Escludere gli utenti del gruppo Duo**

È possibile escludere alcuni utenti che fanno parte di un gruppo Duo dal processo di autenticazione SSH Duo.

#### **Fasi**

1. Accedere al proprio account ONTAP utilizzando SSH.
2. Disattivare l'autenticazione Cisco Duo per utenti specifici di un gruppo. Sostituire il nome del gruppo e l'elenco degli utenti da escludere per i valori tra parentesi:

```
security login group modify -group-name <GROUP_NAME> -exclude-users  
<USER1, USER2>
```

Il nome del gruppo Duo deve corrispondere a un gruppo Active Directory, LDAP o locale. Utenti specificati con `-exclude-users` Il parametro non verrà incluso nel processo di autenticazione Duo.

## Escludere gli utenti Duo locali

È possibile escludere utenti locali specifici dall'uso dell'autenticazione Duo utilizzando il pannello di amministrazione di Cisco Duo. Per istruzioni, fare riferimento a. "[Documentazione di Cisco Duo](#)".

## Generare e installare una panoramica del certificato server firmato dalla CA

Nei sistemi di produzione, è consigliabile installare un certificato digitale con firma CA da utilizzare per l'autenticazione del cluster o SVM come server SSL. È possibile utilizzare `security certificate generate-csr` Per generare una richiesta di firma del certificato (CSR) e il `security certificate install` per installare il certificato ricevuto dall'autorità di certificazione.

### Generare una richiesta di firma del certificato

È possibile utilizzare `security certificate generate-csr` Comando per generare una richiesta di firma del certificato (CSR). Una volta elaborata la richiesta, l'autorità di certificazione (CA) invia il certificato digitale firmato.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

#### 1. Generare una CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size  
512|1024|1536|2048 -country country -state state -locality locality  
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

Il seguente comando crea una CSR con una chiave privata a 2048 bit generata dalla funzione di hash "SHA256" per l'utilizzo da parte del gruppo "Software" nel reparto "IT" di una società il cui nome comune personalizzato è "server1.companyname.com", con sede a Sunnyvale, California, USA. L'indirizzo e-mail dell'amministratore del contatto della SVM è "[web@example.com](#)". Il sistema visualizza la CSR e la chiave privata nell'output.

## Esempio di creazione di una CSR

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
```

Certificate Signing Request :

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBcWUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

-----BEGIN RSA PRIVATE KEY-----

```
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

Note: Please keep a copy of your certificate request and private key for future reference.

2. Copiare la richiesta di certificato dall'output CSR e inviarla in formato elettronico (ad esempio tramite e-mail) a una CA di terze parti attendibile per la firma.

Una volta elaborata la richiesta, la CA invia il certificato digitale firmato. Conservare una copia della chiave privata e del certificato digitale firmato dalla CA.

### Installare un certificato server firmato dalla CA

È possibile utilizzare `security certificate install` Comando per installare un certificato server firmato da CA su una SVM. ONTAP richiede i certificati principali e intermedi dell'autorità di certificazione (CA) che formano la catena di certificati del certificato del server.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

## Fase

1. Installare un certificato server firmato dalla CA:

```
security certificate install -vserver SVM_name -type certificate_type
```

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).



ONTAP richiede i certificati CA principali e intermedi che formano la catena di certificati del certificato del server. La catena inizia con il certificato della CA che ha emesso il certificato del server e può arrivare fino al certificato root della CA. Eventuali certificati intermedi mancanti causano un errore nell'installazione del certificato del server.

Il seguente comando installa il certificato del server firmato dalla CA e i certificati intermedi su SVM `"engData2"`.

## Esempio di installazione di certificati intermedi di un certificato server con firma CA

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTAADEJMAcGA1UECzMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTAADEJMAcGA1UECzM
AMQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C6lX2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG7lUyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----
```

Do you want to continue entering root and/or intermediate  
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSGAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECzMOR28gRGFkZkhkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate  
certificates {y|n}: y

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACGTG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEExodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACGTG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEExodHRw
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate  
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital  
certificate for future reference.

## Gestire i certificati con System Manager

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per gestire autorità di certificazione attendibili, certificati client/server e autorità di certificazione locali (integrate).

Con System Manager, è possibile gestire i certificati ricevuti da altre applicazioni in modo da autenticare le comunicazioni da tali applicazioni. È inoltre possibile gestire i propri certificati che identificano il sistema in altre applicazioni.

### Visualizzare le informazioni sul certificato

System Manager consente di visualizzare le autorità di certificazione attendibili, i certificati client/server e le autorità di certificazione locali memorizzati nel cluster.

### Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Scorrere fino all'area **Security** (sicurezza). Nella sezione **certificati** vengono visualizzati i seguenti dettagli:
  - Il numero di autorità di certificazione attendibili memorizzate.
  - Il numero di certificati client/server memorizzati.
  - Il numero di autorità di certificazione locali memorizzate.
3. Selezionare un numero qualsiasi per visualizzare i dettagli relativi a una categoria di certificati oppure scegliere ➔ Consente di aprire la pagina **certificati**, che contiene informazioni su tutte le categorie. L'elenco visualizza le informazioni relative all'intero cluster. Se si desidera visualizzare le informazioni solo per una specifica macchina virtuale di storage, attenersi alla seguente procedura:
  - a. Selezionare **Storage > Storage VM**.
  - b. Selezionare la VM di storage.

- c. Passare alla scheda **Impostazioni**.
- d. Selezionare un numero visualizzato nella sezione **certificato**.

### Cosa fare in seguito

- Dalla pagina **certificati**, è possibile [Generare una richiesta di firma del certificato](#).
- Le informazioni sul certificato sono suddivise in tre schede, una per ciascuna categoria. È possibile eseguire le seguenti attività da ciascuna scheda:

In questa scheda...	È possibile eseguire queste procedure...
<b>Autorità di certificazione attendibili</b>	<ul style="list-style-type: none"> <li>• <a href="#">[install-trusted-cert]</a></li> <li>• <a href="#">Eliminare un'autorità di certificazione attendibile</a></li> <li>• <a href="#">Rinnovare un'autorità di certificazione attendibile</a></li> </ul>
<b>Certificati client/server</b>	<ul style="list-style-type: none"> <li>• <a href="#">[install-cs-cert]</a></li> <li>• <a href="#">[gen-cs-cert]</a></li> <li>• <a href="#">[delete-cs-cert]</a></li> <li>• <a href="#">[renew-cs-cert]</a></li> </ul>
<b>Autorità locali di certificazione</b>	<ul style="list-style-type: none"> <li>• <a href="#">Creare una nuova autorità di certificazione locale</a></li> <li>• <a href="#">Firmare un certificato utilizzando un'autorità di certificazione locale</a></li> <li>• <a href="#">Eliminare un'autorità di certificazione locale</a></li> <li>• <a href="#">Rinnovare un'autorità di certificazione locale</a></li> </ul>

### Generare una richiesta di firma del certificato

È possibile generare una richiesta di firma del certificato (CSR) con System Manager da qualsiasi scheda della pagina **certificati**. Vengono generate una chiave privata e una CSR corrispondente, che possono essere firmate utilizzando un'autorità di certificazione per generare un certificato pubblico.

### Fasi


1. Visualizzare la pagina **certificati**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare **+genera CSR**.
3. Inserire le informazioni relative al nome del soggetto:
  - a. Immettere un **nome comune**.
  - b. Selezionare un **paese**.
  - c. Inserire un'organizzazione \*.
  - d. Inserire un'unità organizzativa\*.
4. Se si desidera ignorare le impostazioni predefinite, selezionare **altre opzioni** e fornire ulteriori informazioni.

### Installare (aggiungere) un'autorità di certificazione attendibile

È possibile installare altre autorità di certificazione attendibili in System Manager.

### Fasi



1. Visualizzare la scheda **autorità di certificazione attendibili**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare .
3. Nella finestra **Aggiungi autorità di certificazione attendibile**, eseguire le seguenti operazioni:
  - Immettere un **nome**.
  - Per il campo **scope**, selezionare una VM di storage.
  - Immettere un **nome comune**.
  - Selezionare un **tipo**.
  - Immettere o importare **dati del certificato**.


#### Eliminare un'autorità di certificazione attendibile

System Manager consente di eliminare un'autorità di certificazione attendibile.



Non è possibile eliminare le autorità di certificazione attendibili preinstallate con ONTAP.


#### Fasi

1. Visualizzare la scheda **autorità di certificazione attendibili**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione attendibile.
3. Selezionare  Accanto al nome, selezionare **Elimina**.

#### Rinnovare un'autorità di certificazione attendibile

System Manager consente di rinnovare un'autorità di certificazione attendibile scaduta o in scadenza.

#### Fasi

1. Visualizzare la scheda **autorità di certificazione attendibili**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione attendibile.
3. Selezionare  Accanto al nome del certificato, quindi **Rinnova**.

#### Installare (aggiungere) un certificato client/server

Con System Manager, è possibile installare certificati client/server aggiuntivi.

#### Fasi

1. Visualizzare la scheda **certificati client/server**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare .
3. Nel pannello **Aggiungi certificato client/server**, eseguire le seguenti operazioni:
  - Immettere un **nome del certificato**.
  - Per il campo **scope**, selezionare una VM di storage.
  - Immettere un **nome comune**.
  - Selezionare un **tipo**.

- Immettere o importare **dati del certificato**. È possibile scrivere o copiare e incollare i dettagli del certificato da un file di testo oppure importare il testo da un file di certificato facendo clic su **Importa**.
- Immettere la **chiave privata**.  
È possibile scrivere o copiare e incollare la chiave privata da un file di testo oppure importare il testo da un file di chiave privata facendo clic su **Importa**.

### Generare (aggiungere) un certificato client/server autofirmato

Con System Manager, è possibile generare certificati client/server autofirmati aggiuntivi.


#### Fasi

1. Visualizzare la scheda **certificati client/server**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare **+genera certificato autofirmato**.
3. Nel pannello **genera certificato autofirmato**, eseguire le seguenti operazioni:
  - Immettere un **nome del certificato**.
  - Per il campo **scope**, selezionare una VM di storage.
  - Immettere un **nome comune**.
  - Selezionare un **tipo**.
  - Selezionare una funzione **hash**.
  - Selezionare una **dimensione chiave**.
  - Selezionare una **VM di storage**.

### Eliminare un certificato client/server

Con System Manager, è possibile eliminare i certificati client/server.


#### Fasi

1. Visualizzare la scheda **certificati client/server**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome del certificato client/server.
3. Selezionare  Accanto al nome, quindi fare clic su **Delete** (Elimina).

### Rinnovare un certificato client/server

System Manager consente di rinnovare un certificato client/server scaduto o in scadenza.

#### Fasi

1. Visualizzare la scheda **certificati client/server**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome del certificato client/server.
3. Selezionare  Accanto al nome, quindi fare clic su **Rinnova**.

### Creare una nuova autorità di certificazione locale

Con System Manager, è possibile creare una nuova autorità di certificazione locale.

#### Fasi

1. Visualizzare la scheda **autorità locali dei certificati**. Vedere [Visualizzare le informazioni sul certificato](#).
- 2.


Selezionare  **Add** .

3. Nel pannello **Add Local Certificate Authority** (Aggiungi autorità di certificazione locale), eseguire le seguenti operazioni:
  - Immettere un **nome**.
  - Per il campo **scope**, selezionare una VM di storage.
  - Immettere un **nome comune**.
4. Se si desidera ignorare le impostazioni predefinite, selezionare **altre opzioni** e fornire ulteriori informazioni.

#### Firmare un certificato utilizzando un'autorità di certificazione locale

In System Manager, è possibile utilizzare un'autorità di certificazione locale per firmare un certificato.


##### Fasi

1. Visualizzare la scheda **autorità locali dei certificati**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione locale.
3. Selezionare  Accanto al nome, quindi **Firma un certificato**.
4. Compilare il modulo **Sign a Certificate Signing Request** (Firma una richiesta di firma certificato).
  - È possibile incollare il contenuto della firma del certificato o importare un file di richiesta della firma del certificato facendo clic su **Importa**.
  - Specificare il numero di giorni per i quali il certificato sarà valido.

#### Eliminare un'autorità di certificazione locale

Con System Manager, è possibile eliminare un'autorità di certificazione locale.


##### Fasi

1. Visualizzare la scheda **autorità di certificazione locale**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione locale.
3. Selezionare  Accanto al nome, quindi **Elimina**.

#### Rinnovare un'autorità di certificazione locale

Con System Manager, è possibile rinnovare un'autorità di certificazione locale scaduta o in scadenza.

##### Fasi

1. Visualizzare la scheda **autorità di certificazione locale**. Vedere [Visualizzare le informazioni sul certificato](#).
2. Selezionare il nome dell'autorità di certificazione locale.
3. Selezionare  Accanto al nome, quindi fare clic su **Rinnova**.

#### Panoramica sull'accesso al controller di dominio di Active Directory

È necessario configurare l'accesso del controller di dominio ad al cluster o alla SVM prima che un account ad possa accedere alla SVM. Se è già stato configurato un server SMB per una SVM di dati, è possibile configurare la SVM come gateway, o *tunnel*, per l'accesso ad al cluster. Se non è stato configurato un server SMB, è possibile creare un account di computer per SVM nel dominio ad.

ONTAP supporta i seguenti servizi di autenticazione dei controller di dominio:

- Kerberos
- LDAP
- Netlogon
- Autorità di sicurezza locale (LSA)

ONTAP supporta i seguenti algoritmi delle chiavi di sessione per connessioni di accesso alla rete sicure:

Algoritmo della chiave di sessione	Disponibile a partire da...
HMAC-SHA256, basato su Advanced Encryption Standard (AES)  Se il cluster esegue ONTAP 9.9.1 o versione precedente e il controller di dominio applica AES per i servizi di Netlogon protetti, la connessione non riesce. In questo caso, è necessario riconfigurare il controller di dominio per accettare connessioni con chiave forte con ONTAP.	ONTAP 9.10.1
DES e HMAC-MD5 (quando è impostato il tasto forte)	Tutte le release di ONTAP 9

Se si desidera utilizzare le chiavi di sessione AES durante la creazione del canale protetto Netlogon, è necessario verificare che AES sia attivato nella SVM.

- A partire da ONTAP 9.14.1, l'AES viene attivato per impostazione predefinita quando si crea una SVM e non è necessario modificare le impostazioni di sicurezza della SVM per utilizzare le chiavi di sessione AES durante la creazione del canale protetto Netlogon.
- Negli ONTAP da 9.10.1 a 9.13.1, quando si crea una SVM, il sistema AES è disattivato per impostazione predefinita. È necessario attivare AES utilizzando il seguente comando:

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```



L'upgrade a ONTAP 9.14.1 o versione successiva non cambia automaticamente le impostazioni AES per le SVM esistenti create con le release precedenti di ONTAP. È comunque necessario aggiornare il valore di questa impostazione per attivare AES su queste SVM.

### Configurare un tunnel di autenticazione

Se è già stato configurato un server SMB per una SVM dati, è possibile utilizzare `security login domain-tunnel create` Comando per configurare la SVM come gateway, o *tunnel*, per l'accesso ad al cluster.

### Prima di iniziare

- È necessario aver configurato un server SMB per una SVM dati.
- Per accedere alla SVM amministrativa per il cluster, è necessario aver attivato un account utente di dominio ad.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

A partire da ONTAP 9.10.1, se si dispone di un gateway SVM (tunnel di dominio) per l'accesso ad, è possibile utilizzare Kerberos per l'autenticazione dell'amministratore se NTLM è stato disattivato nel dominio ad. Nelle versioni precedenti, Kerberos non era supportato con l'autenticazione admin per i gateway SVM. Questa funzionalità è disponibile per impostazione predefinita; non è richiesta alcuna configurazione.



L'autenticazione Kerberos viene sempre tentata per prima. In caso di errore, viene quindi tentata l'autenticazione NTLM.

## Fase

1. Configurare una SVM di dati abilitata per SMB come tunnel di autenticazione per l'accesso del controller di dominio ad al cluster:

```
security login domain-tunnel create -vserver svm_name
```

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).



Affinché l'utente possa essere autenticato, SVM deve essere in esecuzione.

Il seguente comando configura la SVM dei dati con abilitazione SMB `"engData"` come tunnel di autenticazione.

```
cluster1::>security login domain-tunnel create -vserver engData
```

## Creare un account di computer SVM sul dominio

Se non è stato configurato un server SMB per una SVM dati, è possibile utilizzare `vserver active-directory create` Per creare un account di computer per la SVM nel dominio.

### A proposito di questa attività

Dopo aver inserito `vserver active-directory create` Viene richiesto di fornire le credenziali per un account utente ad con privilegi sufficienti per aggiungere computer all'unità organizzativa specificata nel dominio. La password dell'account non può essere vuota.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

## Fase

1. Creare un account di computer per una SVM nel dominio ad:

```
vserver active-directory create -vserver SVM_name -account-name  
NetBIOS_account_name -domain domain -ou organizational_unit
```

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

Il seguente comando crea un account di computer denominato `"ADSERVER1"` nel dominio `"example.com"` per SVM `"engData"`. Dopo aver immesso il comando, viene richiesto di immettere le credenziali dell'account utente ad.

```
cluster1::>vserver active-directory create -vserver engData -account  
-name ADSERVER1 -domain example.com
```

In order to create an Active Directory machine account, you must supply the name and password of a Windows account with sufficient privileges to add computers to the "CN=Computers" container within the "example.com" domain.

Enter the user name: Administrator

Enter the password:

## Configurare la panoramica dell'accesso al server LDAP o NIS

È necessario configurare l'accesso al server LDAP o NIS a una SVM prima che gli account LDAP o NIS possano accedere alla SVM. La funzione di switch consente di utilizzare LDAP o NIS come origini alternative del servizio di nomi.

### Configurare l'accesso al server LDAP

È necessario configurare l'accesso del server LDAP a una SVM prima che gli account LDAP possano accedere alla SVM. È possibile utilizzare `vserver services name-service ldap client create` Per creare una configurazione del client LDAP su SVM. È quindi possibile utilizzare `vserver services name-service ldap create` Comando per associare la configurazione del client LDAP a SVM.

### A proposito di questa attività

La maggior parte dei server LDAP può utilizzare gli schemi predefiniti forniti da ONTAP:

- MS-ad-BIS (lo schema preferito per la maggior parte dei server ad Windows 2012 e successivi)
- AD-IDMU (server AD Windows 2008, Windows 2016 e versioni successive)
- AD-SFU (server ad Windows 2003 e precedenti)
- RFC-2307 (SERVER LDAP UNIX)

Si consiglia di utilizzare gli schemi predefiniti, a meno che non vi sia un requisito diverso. In tal caso, è possibile creare uno schema personalizzato copiando uno schema predefinito e modificando la copia. Per ulteriori informazioni, consulta:

- ["Configurazione NFS"](#)
- ["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#)

### Prima di iniziare

- È necessario aver installato un ["Certificato digitale del server firmato CA"](#) Su SVM.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

1. Creare una configurazione del client LDAP su una SVM:

```
vserver services name-service ldap client create -vserver SVM_name -client
-config client_configuration -servers LDAP_server_IPs -schema schema -use
-start-tls true|false
```



Start TLS è supportato solo per l'accesso ai dati SVM. Non è supportato per l'accesso alle SVM amministrative.

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

Il seguente comando crea una configurazione del client LDAP denominata "corp" su SVM "engData". Il client crea un'associazione anonima ai server LDAP con gli indirizzi IP 172.160.0.100 e 172.16.0.101. Il client utilizza lo schema RFC-2307 per eseguire query LDAP. La comunicazione tra il client e il server viene crittografata mediante Start TLS.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```



A partire da ONTAP 9.2, il campo `-ldap-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server LDAP.

2. Associare la configurazione del client LDAP a SVM: `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

Il seguente comando associa la configurazione del client LDAP corp Con SVM `engData` E attiva il client LDAP su SVM.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```



A partire da ONTAP 9.2, la `vserver services name-service ldap create` Il comando esegue una convalida automatica della configurazione e segnala un messaggio di errore se ONTAP non è in grado di contattare il server dei nomi.

3. Convalidare lo stato dei server dei nomi utilizzando il comando di controllo `ldap name-service` dei servizi `vserver`.

Il seguente comando convalida i server LDAP su SVM vs0.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server |
| "10.11.12.13". |
```

Il comando name service check è disponibile a partire da ONTAP 9.2.

### Configurare l'accesso al server NIS

È necessario configurare l'accesso del server NIS a una SVM prima che gli account NIS possano accedere alla SVM. È possibile utilizzare `vserver services name-service nis-domain create` Per creare una configurazione di dominio NIS su una SVM.

#### A proposito di questa attività

È possibile creare più domini NIS. È possibile impostare un solo dominio NIS su `active` alla volta.

#### Prima di iniziare

- Tutti i server configurati devono essere disponibili e accessibili prima di configurare il dominio NIS sulla SVM.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

#### Fase

1. Creare una configurazione di dominio NIS su una SVM:

```
vserver services name-service nis-domain create -vserver SVM_name -domain
client_configuration -active true|false -nis-servers NIS_server_IPs
```

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).



A partire da ONTAP 9.2, il campo `-nis-servers` sostituisce il campo `-servers`. Questo nuovo campo può includere un nome host o un indirizzo IP per il server NIS.

Il seguente comando crea una configurazione di dominio NIS su SVM `"engData"`. Il dominio NIS `nisdomain` È attivo alla creazione e comunica con un server NIS con l'indirizzo IP `192.0.2.180`.

```
cluster1::>vserver services name-service nis-domain create
-vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
```

### Creare un name service switch

La funzione di switch del name service consente di utilizzare LDAP o NIS come origini alternative del name service. È possibile utilizzare `vserver services name-service ns-switch modify` per specificare l'ordine di ricerca delle origini del servizio nome.



## Prima di iniziare

- È necessario aver configurato l'accesso al server LDAP e NIS.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

## Fase

1. Specificare l'ordine di ricerca per le origini del servizio nome:

```
vserver services name-service ns-switch modify -vserver SVM_name -database  
name_service_switch_database -sources name_service_source_order
```

Per la sintassi completa dei comandi, vedere ["foglio di lavoro"](#).

Il seguente comando specifica l'ordine di ricerca delle origini del servizio nomi LDAP e NIS per il database "passwd" su SVM "engData".

```
cluster1::>vserver services name-service ns-switch  
modify -vserver engData -database passwd -source files ldap,nis
```

## Modificare la password dell'amministratore

È necessario modificare la password iniziale subito dopo aver effettuato l'accesso al sistema per la prima volta. Gli amministratori di SVM possono utilizzare `security login password` per modificare la password. Gli amministratori del cluster possono utilizzare `security login password` per modificare la password dell'amministratore.

### A proposito di questa attività

La nuova password deve rispettare le seguenti regole:

- Non può contenere il nome utente
- La lunghezza deve essere di almeno otto caratteri
- Deve contenere almeno una lettera e un numero
- Non può essere uguale alle ultime sei password



È possibile utilizzare `security login role config modify` comando per modificare le regole delle password per gli account associati a un determinato ruolo. Per ulteriori informazioni, consultare ["riferimento al comando"](#).

## Prima di iniziare

- Per modificare la password, è necessario essere un amministratore del cluster o di SVM.
- Per modificare la password di un altro amministratore, è necessario essere un amministratore del cluster.

## Fase

1. Modifica della password di amministratore: `security login password -vserver svm_name -username user_name`

Il seguente comando modifica la password dell'amministratore `admin1` Per `SVMvs1.example.com`. Viene richiesto di inserire la password corrente, quindi di inserire e immettere nuovamente la nuova

password.

```
vs1.example.com::>security login password -vserver engData -username  
admin1  
Please enter your current password:  
Please enter a new password:  
Please enter it again:
```

## Bloccare e sbloccare un account amministratore

È possibile utilizzare `security login lock` per bloccare un account amministratore e `security login unlock` per sbloccare l'account.

### Prima di iniziare

Per eseguire queste attività, è necessario essere un amministratore del cluster.

### Fasi

1. Blocco di un account amministratore:

```
security login lock -vserver SVM_name -username user_name
```

Il seguente comando blocca l'account amministratore `admin1` Per SVM `vs1.example.com`:

```
cluster1::>security login lock -vserver engData -username admin1
```

2. Sbloccare un account amministratore:

```
security login unlock -vserver SVM_name -username user_name
```

Il seguente comando sblocca l'account amministratore `admin1` Per SVM `vs1.example.com`:

```
cluster1::>security login unlock -vserver engData -username admin1
```

## Gestire i tentativi di accesso non riusciti

Tentativi ripetuti di accesso non riusciti indicano talvolta che un intruso sta tentando di accedere al sistema di storage. È possibile eseguire una serie di operazioni per evitare l'intrusione.

### Come saprai che i tentativi di accesso non sono riusciti

Il sistema di gestione degli eventi (EMS) notifica ogni ora i tentativi di accesso non riusciti. È possibile trovare un record dei tentativi di accesso non riusciti in `audit.log` file.

## Cosa fare se i tentativi di accesso ripetuti non riescono

A breve termine, è possibile adottare una serie di misure per prevenire un'intrusione:

- Richiedere che le password siano composte da un numero minimo di caratteri maiuscoli, minuscoli, caratteri speciali e/o cifre
- Imporre un ritardo dopo un tentativo di accesso non riuscito
- Limitare il numero di tentativi di accesso non riusciti consentiti e bloccare gli utenti dopo il numero specificato di tentativi non riusciti
- Scade e blocca gli account inattivi per un determinato numero di giorni

È possibile utilizzare `security login role config modify` per eseguire queste attività.

A lungo termine, è possibile eseguire le seguenti operazioni aggiuntive:

- Utilizzare `security ssh modify` Comando per limitare il numero di tentativi di accesso non riusciti per tutte le SVM appena create.
- Migrare gli account dell'algoritmo MD5 esistenti sull'algoritmo SHA-512 più sicuro richiedendo agli utenti di modificare le password.

## Applicare SHA-2 sulle password dell'account amministratore

Gli account amministratore creati prima di ONTAP 9.0 continuano a utilizzare le password MD5 dopo l'aggiornamento, fino a quando le password non vengono modificate manualmente. MD5 è meno sicuro di SHA-2. Pertanto, dopo l'aggiornamento, è necessario richiedere agli utenti degli account MD5 di modificare le password per utilizzare la funzione hash SHA-512 predefinita.

### A proposito di questa attività

La funzionalità di hash delle password consente di effettuare le seguenti operazioni:

- Visualizza gli account utente che corrispondono alla funzione hash specificata.
- Gli account con scadenza che utilizzano una funzione hash specificata (ad esempio MD5), costringendo gli utenti a modificare le password nel successivo accesso.
- Bloccare gli account le cui password utilizzano la funzione hash specificata.
- Quando si torna a una release precedente a ONTAP 9, reimpostare la password dell'amministratore del cluster affinché sia compatibile con la funzione hash (MD5) supportata dalla release precedente.

ONTAP accetta password SHA-2 pre-hash solo utilizzando l'SDK di gestione NetApp (`security-login-create` e `security-login-modify-password`).

### Fasi

1. Migrare gli account amministratore MD5 alla funzione hash della password SHA-512:

- a. Scadenza di tutti gli account amministratore MD5: `security login expire-password -vserver * -username * -hash-function md5`

In questo modo, gli utenti degli account MD5 devono modificare le password al successivo accesso.

- b. Chiedere agli utenti degli account MD5 di effettuare l'accesso tramite una console o una sessione


SSH.

Il sistema rileva che gli account sono scaduti e richiede agli utenti di modificare le password. SHA-512 viene utilizzato per impostazione predefinita per le password modificate.


2. Per gli account MD5 i cui utenti non effettuano l'accesso per modificare le password entro un determinato periodo di tempo, forzare la migrazione dell'account:
  - a. Bloccare gli account che utilizzano ancora la funzione hash MD5 (livello di privilegio avanzato):  
`security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`  
  
Dopo il numero di giorni specificato da `-lock-after`, Gli utenti non possono accedere ai propri account MD5.
  - b. Sbloccare gli account quando gli utenti sono pronti a modificare le proprie password: `security login unlock -vserver svm_name -username user_name`
  - c. Chiedere agli utenti di accedere ai propri account tramite una console o una sessione SSH e modificare le password quando richiesto dal sistema.

## Diagnosticare e correggere i problemi di accesso ai file

### Fasi

1. In System Manager, selezionare **Storage > Storage VM**.
2. Selezionare la VM di storage su cui si desidera eseguire una traccia.
3. Fare clic su  **Altro**.
4. Fare clic su **accesso al file di traccia**.
5. Fornire il nome utente e l'indirizzo IP del client, quindi fare clic su **Avvia traccia**.

I risultati della traccia vengono visualizzati in una tabella. La colonna **motivi** indica il motivo per cui non è stato possibile accedere a un file.

6. Fare clic su  nella colonna sinistra della tabella dei risultati per visualizzare le autorizzazioni di accesso al file.

## Gestire la verifica multi-admin

### Panoramica sulla verifica multi-admin

A partire da ONTAP 9.11.1, è possibile utilizzare la verifica multi-admin (MAV) per garantire che determinate operazioni, come l'eliminazione di volumi o copie Snapshot, possano essere eseguite solo dopo l'approvazione da parte degli amministratori designati. In questo modo si evita che gli amministratori compromessi, dannosi o inesperti apportino modifiche indesiderate o eliminino dati.

La configurazione della verifica multi-admin comprende:

- ["Creazione di uno o più gruppi di approvazione dell'amministratore."](#)
- ["Abilitazione della funzionalità di verifica multi-admin."](#)
- ["Aggiunta o modifica di regole."](#)

Dopo la configurazione iniziale, questi elementi possono essere modificati solo dagli amministratori di un gruppo di approvazione MAV (amministratori MAV).

Quando la verifica multi-admin è attivata, il completamento di ogni operazione protetta richiede tre passaggi:

- Quando un utente avvia l'operazione, un ["la richiesta viene generata."](#)
- Prima che possa essere eseguito, almeno uno ["L'amministratore MAV deve approvare."](#)
- Dopo l'approvazione, l'utente completa l'operazione.

La verifica multi-admin non è prevista per l'utilizzo con volumi o flussi di lavoro che comportano un'elevata automazione, perché ogni attività automatizzata richiederebbe l'approvazione prima che l'operazione possa essere completata. Se si desidera utilizzare l'automazione e MAV insieme, si consiglia di utilizzare le query per specifiche operazioni MAV. Ad esempio, è possibile fare domanda `volume delete`. Le regole MAV si applicano solo ai volumi in cui l'automazione non è coinvolta ed è possibile designare tali volumi con uno schema di denominazione specifico.



Se è necessario disattivare la funzionalità di verifica multi-admin senza l'approvazione dell'amministratore MAV, contattare il supporto NetApp e citare il seguente articolo della Knowledge base: ["Come disattivare la verifica multi-amministratore se MAV admin non è disponibile"](#).

### Come funziona la verifica multi-admin

La verifica multi-admin consiste in:

- Un gruppo di uno o più amministratori con poteri di approvazione e veto.
- Un insieme di operazioni o comandi protetti in una *tabella di regole*.
- Un *motore di regole* per identificare e controllare l'esecuzione di operazioni protette.

Le regole MAV vengono valutate in base alle regole RBAC (role-based access control). Pertanto, gli amministratori che eseguono o approvano operazioni protette devono già disporre dei privilegi RBAC minimi per tali operazioni. ["Scopri di più su RBAC."](#)

### Regole definite dal sistema

Quando la verifica multi-admin è attivata, le regole definite dal sistema (note anche come regole *guard-rail*) stabiliscono un insieme di operazioni MAV per contenere il rischio di aggirare il processo MAV stesso. Queste operazioni non possono essere rimosse dalla tabella delle regole. Una volta abilitato MAV, le operazioni contrassegnate da un asterisco ( \* ) devono essere approvate da uno o più amministratori prima dell'esecuzione, ad eccezione dei comandi **show**.

- `security multi-admin-verify modify funzionamento*`

Controlla la configurazione della funzionalità di verifica multi-admin.

- `security multi-admin-verify approval-group operazioni*`

Controlla l'appartenenza all'insieme di amministratori con credenziali di verifica multi-admin.

- `security multi-admin-verify rule operazioni*`

Controlla il set di comandi che richiedono la verifica multi-admin.

- `security multi-admin-verify request` operazioni

Controllare il processo di approvazione.

## Comandi protetti da regole

Oltre ai comandi definiti dal sistema, i seguenti comandi sono protetti per impostazione predefinita quando è attivata la verifica multi-admin, ma è possibile modificare le regole per rimuovere la protezione per questi comandi.

- `security login password`
- `security login unlock`
- `set`

I seguenti comandi possono essere protetti in ONTAP 9.11.1 e versioni successive.

<code>cluster peer delete</code>	<code>volume snapshot autodelete modify</code>
<code>event config modify</code>	<code>volume snapshot delete</code>
<code>security login create</code>	<code>volume snapshot policy add-schedule</code>
<code>security login delete</code>	<code>volume snapshot policy create</code>
<code>security login modify</code>	<code>volume snapshot policy delete</code>
<code>system node run</code>	<code>volume snapshot policy modify</code>
<code>system node systemshell</code>	<code>volume snapshot policy modify-schedule</code>
<code>volume delete</code>	<code>volume snapshot policy remove-schedule</code>
<code>volume flexcache delete</code>	<code>volume snapshot restore</code>
	<code>vserver peer delete</code>

I seguenti comandi possono essere protetti a partire da ONTAP 9.13.1:

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

I seguenti comandi possono essere protetti a partire da ONTAP 9.14.1:

- `volume recovery-queue modify`
- `volume recovery-queue purge`

- `volume recovery-queue purge-all`
- `vserver modify`

### Come funziona l'approvazione multi-admin

Ogni volta che un'operazione protetta viene inserita in un cluster protetto da MAV, una richiesta di esecuzione dell'operazione viene inviata al gruppo di amministratori MAV designato.

È possibile configurare:

- I nomi, le informazioni di contatto e il numero di amministratori nel gruppo MAV.

Un amministratore MAV deve avere un ruolo RBAC con privilegi di amministratore del cluster.

- Il numero di gruppi di amministratori MAV.
  - Viene assegnato un gruppo MAV per ogni regola operativa protetta.
  - Per più gruppi MAV, è possibile configurare quale gruppo MAV approva una data regola.
- Il numero di approvazioni MAV richieste per eseguire un'operazione protetta.
- Un periodo di *scadenza dell'approvazione* entro il quale un amministratore MAV deve rispondere a una richiesta di approvazione.
- Un periodo di *scadenza dell'esecuzione* entro il quale l'amministratore richiedente deve completare l'operazione.

Una volta configurati questi parametri, è necessaria l'approvazione MAV per modificarli.

Gli amministratori MAV non possono approvare le proprie richieste di esecuzione di operazioni protette. Pertanto:

- MAV non deve essere abilitato sui cluster con un solo amministratore.
- Se nel gruppo MAV è presente una sola persona, l'amministratore MAV non può inserire operazioni protette; gli amministratori regolari devono inserirle e l'amministratore MAV può solo approvarle.
- Se si desidera che gli amministratori MAV siano in grado di eseguire operazioni protette, il numero di amministratori MAV deve essere maggiore di uno rispetto al numero di approvazioni richieste. Ad esempio, se sono necessarie due approvazioni per un'operazione protetta e si desidera che gli amministratori MAV le eseguano, devono essere presenti tre persone nel gruppo di amministratori MAV.

Gli amministratori MAV possono ricevere richieste di approvazione in avvisi e-mail (tramite EMS) oppure interrogare la coda delle richieste. Quando ricevono una richiesta, possono intraprendere una delle tre azioni seguenti:

- Approvare
- Rifiuto (veto)
- Ignora (nessuna azione)

Le notifiche e-mail vengono inviate a tutti i responsabili dell'approvazione associati a una regola MAV quando:

- Viene creata una richiesta.
- Una richiesta viene approvata o vetoata.
- Viene eseguita una richiesta approvata.

Se il richiedente si trova nello stesso gruppo di approvazione per l'operazione, riceverà un'e-mail quando la richiesta verrà approvata.

**Nota:** Un richiedente non può approvare le proprie richieste, anche se si trova nel gruppo di approvazione. Ma possono ricevere le notifiche via email. I richiedenti che non fanno parte di gruppi di approvazione (vale a dire, che non sono amministratori MAV) non ricevono notifiche via email.

#### Come funziona l'esecuzione di operazioni protette

Se l'esecuzione viene approvata per un'operazione protetta, l'utente richiedente continua con l'operazione quando richiesto. Se l'operazione è vetoed, l'utente richiedente deve eliminare la richiesta prima di procedere.

Le regole MAV vengono valutate dopo le autorizzazioni RBAC. Di conseguenza, un utente senza autorizzazioni RBAC sufficienti per l'esecuzione dell'operazione non può avviare il processo di richiesta MAV.

#### Gestire i gruppi di approvazione degli amministratori

Prima di attivare la verifica multi-amministratore (MAV), è necessario creare un gruppo di approvazione amministratore contenente uno o più amministratori a cui concedere l'autorizzazione di approvazione o veto. Una volta attivata la verifica multi-admin, qualsiasi modifica all'appartenenza al gruppo di approvazione richiede l'approvazione di uno degli amministratori qualificati esistenti.

#### A proposito di questa attività

È possibile aggiungere amministratori esistenti a un gruppo MAV o creare nuovi amministratori.

La funzionalità MAV rispetta le impostazioni RBAC (role-based access control) esistenti. I potenziali amministratori MAV devono disporre di privilegi sufficienti per eseguire operazioni protette prima di aggiungerli ai gruppi di amministratori MAV. ["Scopri di più su RBAC."](#)

È possibile configurare MAV per avvisare gli amministratori MAV che le richieste di approvazione sono in sospeso. A tale scopo, è necessario configurare le notifiche e-mail, in particolare i `Mail From` e `Mail Server` parametri—oppure è possibile cancellare questi parametri per disattivare la notifica. Senza avvisi via email, gli amministratori MAV devono controllare manualmente la coda di approvazione.

#### Procedura di System Manager

Se si desidera creare un gruppo di approvazione MAV per la prima volta, consultare la procedura di System Manager in ["attiva la verifica multi-admin."](#)

Per modificare un gruppo di approvazione esistente o creare un gruppo di approvazione aggiuntivo:


1. Identificare gli amministratori per ricevere la verifica multi-admin.
  - a. Fare clic su **Cluster > Settings**.
  - b. Fare clic su ➔ Accanto a **utenti e ruoli**.
  - c. Fare clic su + **Add** Sotto **utenti**.
  - d. Modificare il registro in base alle esigenze.

Per ulteriori informazioni, vedere ["Controllare l'accesso dell'amministratore."](#)

2. Creare o modificare il gruppo di approvazione MAV:



a. Fare clic su **Cluster > Settings**.

b. Fare clic su → Accanto a **approvazione multi-amministratore** nella sezione **sicurezza**. (Viene visualizzata la  Se MAV non è ancora configurato).

- Name (Nome): Immettere un nome di gruppo.
- Responsabili dell'approvazione: Selezionare i responsabili dell'approvazione da un elenco di utenti.
- Email address (Indirizzo email): Inserire gli indirizzi email.
- Default group (Gruppo predefinito): Selezionare un gruppo.

L'approvazione MAV è necessaria per modificare una configurazione esistente una volta abilitato MAV.

#### Procedura CLI

1. Verificare che siano stati impostati i valori per Mail From e Mail Server parametri. Inserire:

```
event config show
```

Il display dovrebbe essere simile a quanto segue:

```
cluster01::> event config show
                        Mail From:  admin@localhost
                        Mail Server: localhost
                        Proxy URL:   -
                        Proxy User:  -
                        Publish/Subscribe Messaging Enabled: true
```

Per configurare questi parametri, immettere:

```
event config modify -mail-from email_address -mail-server server_name
```

2. Identificare gli amministratori per ricevere la verifica multi-admin

Se si desidera...	Immettere questo comando
Visualizza gli amministratori correnti	<code>security login show</code>
Modificare le credenziali degli amministratori correnti	<code>security login modify &lt;parameters&gt;</code>
Creare nuovi account amministratore	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

3. Creare il gruppo di approvazione MAV:

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2...] [[-email address1], address1...]
```

- -vserver - Solo la SVM amministrativa è supportata in questa versione.

- `-name` - Il nome del gruppo MAV, composto da un massimo di 64 caratteri.
- `-approvers` - L'elenco di uno o più responsabili dell'approvazione.
- `-email` - Uno o più indirizzi e-mail che vengono notificati quando una richiesta viene creata, approvata, sottoposta a veto o eseguita.

**Esempio:** il seguente comando crea un gruppo MAV con due membri e indirizzi e-mail associati.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

#### 4. Verificare la creazione e l'appartenenza del gruppo:

```
security multi-admin-verify approval-group show
```

**Esempio:**

```
cluster-1::> security multi-admin-verify approval-group show
Vserver   Name           Approvers      Email
-----
svm-1     mav-grp1      pavan,julia    email
pavan@myfirm.com,julia@myfirm.com
```

Utilizzare questi comandi per modificare la configurazione iniziale del gruppo MAV.

**Nota:** tutti richiedono l'approvazione dell'amministratore MAV prima dell'esecuzione.

Se si desidera...	Immettere questo comando
Modificare le caratteristiche del gruppo o le informazioni sui membri esistenti	<code>security multi-admin-verify approval-group modify [parameters]</code>
Aggiungere o rimuovere membri	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[, approver2...]] [-approvers-to-remove approver1[, approver2...]]</code>
Eliminare un gruppo	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

#### Attiva e disattiva la verifica multi-admin

La verifica multi-admin (MAV) deve essere attivata esplicitamente. Una volta attivata la

verifica multi-admin, l'approvazione da parte degli amministratori di un gruppo di approvazione MAV (amministratori MAV) è necessaria per eliminarla.

### A proposito di questa attività

Una volta attivato MAV, la modifica o la disattivazione di MAV richiede l'approvazione dell'amministratore MAV.



Se è necessario disattivare la funzionalità di verifica multi-admin senza l'approvazione dell'amministratore MAV, contattare il supporto NetApp e citare il seguente articolo della Knowledge base: "[Come disattivare la verifica multi-amministratore se MAV admin non è disponibile](#)".

Quando si attiva MAV, è possibile specificare globalmente i seguenti parametri.

### Gruppi di approvazione

Un elenco di gruppi di approvazione globali. Per abilitare la funzionalità MAV è necessario almeno un gruppo.



Se si utilizza MAV con la protezione ransomware autonoma (ARP), definire un gruppo di approvazione nuovo o esistente responsabile dell'approvazione della pausa, della disattivazione e dell'eliminazione delle richieste sospette di ARP.

### Responsabili dell'approvazione richiesti

Il numero di responsabili dell'approvazione necessari per eseguire un'operazione protetta. Il numero predefinito e minimo è 1.



Il numero richiesto di responsabili dell'approvazione deve essere inferiore al numero totale di responsabili dell'approvazione univoci nei gruppi di approvazione predefiniti.

### Scadenza approvazione (ore, minuti, secondi)

Periodo entro il quale un amministratore MAV deve rispondere a una richiesta di approvazione. Il valore predefinito è un'ora (1h), il valore minimo supportato è un secondo (1s) e il valore massimo supportato è 14 giorni (14d).

### Scadenza dell'esecuzione (ore, minuti, secondi)

Il periodo entro il quale l'amministratore richiedente deve completare l'operazione:: Il valore predefinito è un'ora (1h), il valore minimo supportato è un secondo (1s) e il valore massimo supportato è 14 giorni (14d).

È inoltre possibile eseguire l'override di uno qualsiasi di questi parametri per specifici "[regole operative](#)."



### Procedura di System Manager

1. Identificare gli amministratori per ricevere la verifica multi-admin.
  - a. Fare clic su **Cluster > Settings**.
  - b. Fare clic su ➔ Accanto a **utenti e ruoli**.
  - c. Fare clic su ➕ **Add** Sotto **utenti**.
  - d. Modificare il registro in base alle esigenze.

Per ulteriori informazioni, vedere "[Controllare l'accesso dell'amministratore](#)."

2. Abilitare la verifica multi-admin creando almeno un gruppo di approvazione e aggiungendo almeno una


regola.

- a. Fare clic su **Cluster > Settings**.
- b. Fare clic su  Accanto a **approvazione multi-amministratore** nella sezione **sicurezza**.
- c. Fare clic su  **Add** per aggiungere almeno un gruppo di approvazione.
  - Name (Nome): Immettere il nome di un gruppo.
  - Responsabili dell'approvazione: Selezionare i responsabili dell'approvazione da un elenco di utenti.
  - Email address (Indirizzo e-mail) – inserire gli indirizzi e-mail.
  - Default group (Gruppo predefinito) – selezionare un gruppo.
- d. Aggiungere almeno una regola.
  - Operation (funzionamento) – selezionare un comando supportato dall'elenco.
  - Query - immettere le opzioni e i valori dei comandi desiderati.
  - Parametri facoltativi; lasciare vuoto per applicare le impostazioni globali o assegnare un valore diverso per regole specifiche per sostituire le impostazioni globali.
    - Numero richiesto di responsabili dell'approvazione
    - Gruppi di approvazione
- e. Fare clic su **Advanced Settings** (Impostazioni avanzate) per visualizzare o modificare le impostazioni predefinite.
  - Numero richiesto di responsabili dell'approvazione (impostazione predefinita: 1)
  - Scadenza richiesta di esecuzione (impostazione predefinita: 1 ora)
  - Scadenza richiesta di approvazione (impostazione predefinita: 1 ora)
  - Server di posta\*
  - Da indirizzo email\*


\*Questi aggiornano le impostazioni e-mail gestite in "Gestione notifiche". Se non sono ancora stati configurati, viene richiesto di impostarli.
- f. Fare clic su **Enable** (attiva) per completare la configurazione iniziale MAV.

Dopo la configurazione iniziale, lo stato MAV corrente viene visualizzato nel riquadro **Multi-Admin Approval**.

- Stato (attivato o meno)
- Operazioni attive per le quali sono richieste approvazioni
- Numero di richieste aperte in stato di attesa

È possibile visualizzare una configurazione esistente facendo clic su . L'approvazione MAV è necessaria per modificare una configurazione esistente.

Per disattivare la verifica multi-admin:

1. Fare clic su **Cluster > Settings**.
2. Fare clic su  Accanto a **approvazione multi-amministratore** nella sezione **sicurezza**.
3. Fare clic sul pulsante di attivazione/disattivazione.

Per completare questa operazione è richiesta l'approvazione MAV.

Procedura CLI

Prima di attivare la funzionalità MAV nella CLI, almeno una "Gruppo di amministratori MAV" deve essere stato creato.

Se si desidera...	Immettere questo comando
Abilitare la funzionalità MAV	<div>security multi-admin-verify modify -approval-groups <i>group1[,group2...]</i> [- required-approvers <i>nn</i> ] -enabled true [ -execution-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]] [ -approval-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]]</div> <div><b>Esempio:</b> Il seguente comando abilita MAV con 1 gruppo di approvazione, 2 responsabili dell'approvazione richiesti e periodi di scadenza predefiniti.</div> <div><pre>cluster-1::&gt; security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre></div> <div>Completare la configurazione iniziale aggiungendone almeno una "regola operativa."</div>
Modifica di una configurazione MAV (richiede l'approvazione MAV)	<div>security multi-admin-verify approval- group modify [-approval-groups <i>group1</i> [,<i>group2...</i>]] [-required-approvers <i>nn</i> ] [ -execution-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]] [ -approval-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]]</div>
Verificare la funzionalità MAV	<div>security multi-admin-verify show</div> <div><b>Esempio:</b></div> <div><pre>cluster-1::&gt; security multi-admin- verify show Is      Required  Execution Approval Approval Enabled Approvers Expiry    Expiry Groups ----- true    2          1h      1h mav-grp1</pre></div>

Se si desidera...	Immettere questo comando
Disattivare la funzionalità MAV (richiede l'approvazione MAV)	<code>security multi-admin-verify modify -enabled false</code>

### Gestire le regole operative protette

Si creano regole di verifica multi-amministratore (MAV) per designare le operazioni che richiedono l'approvazione. Ogni volta che viene avviata un'operazione, le operazioni protette vengono intercettate e viene generata una richiesta di approvazione.

Le regole possono essere create prima di abilitare MAV da qualsiasi amministratore con funzionalità RBAC appropriate, ma una volta attivata la MAV, qualsiasi modifica al set di regole richiede l'approvazione MAV.

È possibile creare una sola regola MAV per operazione; ad esempio, non è possibile creare più regole `volume-snapshot-delete` regole. Tutti i vincoli di regola desiderati devono essere contenuti all'interno di una regola.

### Comandi protetti da regole

È possibile creare regole per proteggere i seguenti comandi, a partire da ONTAP 9.11.1.

<code>cluster peer delete</code>	<code>volume snapshot autodelete modify</code>
<code>event config modify</code>	<code>volume snapshot delete</code>
<code>security login create</code>	<code>volume snapshot policy add-schedule</code>
<code>security login delete</code>	<code>volume snapshot policy create</code>
<code>security login modify</code>	<code>volume snapshot policy delete</code>
<code>system node run</code>	<code>volume snapshot policy modify</code>
<code>system node systemshell</code>	<code>volume snapshot policy modify-schedule</code>
<code>volume delete</code>	<code>volume snapshot policy remove-schedule</code>
<code>volume flexcache delete</code>	<code>volume snapshot restore</code>
	<code>vserver peer delete</code>

È possibile creare regole per proteggere i seguenti comandi a partire da ONTAP 9.13.1:

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

È possibile creare regole per proteggere i seguenti comandi a partire da ONTAP 9.14.1:

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

Le regole per i comandi MAV di default del sistema, il `security multi-admin-verify` "comandi", non può essere modificato.

Oltre ai comandi definiti dal sistema, i seguenti comandi sono protetti per impostazione predefinita quando è attivata la verifica multi-admin, ma è possibile modificare le regole per rimuovere la protezione per questi comandi.

- `security login password`
- `security login unlock`
- `set`

#### Vincoli della regola

Quando si crea una regola, è possibile specificare il `-query` opzione per limitare la richiesta a un sottoinsieme della funzionalità del comando. Il `-query` Può essere utilizzata anche per limitare gli elementi di configurazione, come SVM, volume e nomi delle Snapshot.

Ad esempio, in `volume snapshot delete` comando, `-query` può essere impostato su `-snapshot !hourly*,!daily*,!weekly*`, Ovvero, le istantanee del volume con attributi orari, giornalieri o settimanali sono escluse dalle protezioni MAV.

```
smci-vs1m20::> security multi-admin-verify rule show
```

		Required	Approval
Vserver	Operation	Approvers	Groups
vs01	volume snapshot delete	-	-
	Query: -snapshot !hourly*,!daily*,!weekly*		



Tutti gli elementi di configurazione esclusi non sono protetti da MAV e qualsiasi amministratore può eliminarli o rinominarli.

Per impostazione predefinita, le regole specificano un corrispondente `security multi-admin-verify request create` "protected operation" il comando viene generato automaticamente quando si inserisce un'operazione protetta. È possibile modificare questa impostazione predefinita in modo che richieda `request create` il comando deve essere immesso separatamente.

Per impostazione predefinita, le regole ereditano le seguenti impostazioni MAV globali, anche se è possibile specificare eccezioni specifiche della regola:



- Numero richiesto di approvatori

- Gruppi di approvazione
- Periodo di scadenza dell'approvazione
- Periodo di scadenza dell'esecuzione

### Procedura di System Manager

Se si desidera aggiungere una regola operativa protetta per la prima volta, consultare la procedura di System Manager in ["attiva la verifica multi-admin."](#)

Per modificare il set di regole esistente:

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare  Accanto a **approvazione multi-amministratore** nella sezione **sicurezza**.
3. Selezionare  **Add** per aggiungere almeno una regola, è anche possibile modificare o eliminare le regole esistenti.
  - Operation (funzionamento) – selezionare un comando supportato dall'elenco.
  - Query - immettere le opzioni e i valori dei comandi desiderati.
  - Parametri facoltativi: Lasciare vuoto per applicare le impostazioni globali o assegnare un valore diverso per regole specifiche per sostituire le impostazioni globali.
    - Numero richiesto di responsabili dell'approvazione
    - Gruppi di approvazione

### Procedura CLI



Tutto `security multi-admin-verify rule` I comandi richiedono l'approvazione dell'amministratore MAV prima dell'esecuzione tranne `security multi-admin-verify rule show`.

Se si desidera...	Immettere questo comando
Creare una regola	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>
Modificare le credenziali degli amministratori correnti	<code>security login modify &lt;parameters&gt;</code>  <b>Esempio:</b> La seguente regola richiede l'approvazione per eliminare il volume root.  <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code>
Modificare una regola	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>



Se si desidera...	Immettere questo comando
Eliminare una regola	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
Mostra regole	<code>security multi-admin-verify rule show</code>

Per informazioni dettagliate sulla sintassi dei comandi, vedere `security multi-admin-verify rule` pagine man.

### Richiedere l'esecuzione di operazioni protette

Quando si avvia un'operazione o un comando protetto su un cluster abilitato per la verifica multi-admin (MAV), ONTAP intercetta automaticamente l'operazione e chiede di generare una richiesta, che deve essere approvata da uno o più amministratori in un gruppo di approvazione MAV (amministratori MAV). In alternativa, è possibile creare una richiesta MAV senza la finestra di dialogo.

Se approvata, è necessario rispondere alla richiesta per completare l'operazione entro il periodo di scadenza della richiesta. In caso di veto o di superamento dei termini di richiesta o scadenza, è necessario eliminare la richiesta e reinviarla.

La funzionalità MAV rispetta le impostazioni RBAC esistenti. In altri termini, il ruolo di amministratore deve disporre di privilegi sufficienti per eseguire un'operazione protetta, indipendentemente dalle impostazioni MAV. ["Scopri di più su RBAC"](#).

Se sei un amministratore MAV, le tue richieste di eseguire operazioni protette devono essere approvate anche da un amministratore MAV.

### Procedura di System Manager

Quando un utente fa clic su una voce di menu per avviare un'operazione e l'operazione è protetta, viene generata una richiesta di approvazione e l'utente riceve una notifica simile a quanto segue:

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

La finestra **Richieste multi-amministratore** è disponibile quando MAV è attivato, mostrando le richieste in sospeso in base all'ID di accesso dell'utente e al ruolo MAV (approvatore o meno). Per ogni richiesta in sospeso, vengono visualizzati i seguenti campi:

- Operazione
- Indice (numero)
- Stato (in sospeso, approvato, rifiutato, eseguito o scaduto)

Se una richiesta viene respinta da un responsabile dell'approvazione, non sono possibili ulteriori azioni.

- Query (qualsiasi parametro o valore per l'operazione richiesta)

- Utente richiedente
- La richiesta scade il
- (Numero di) approvatori in sospenso
- (Numero di) potenziali responsabili dell'approvazione

Una volta approvata la richiesta, l'utente richiedente può riprovare l'operazione entro il periodo di scadenza.

Se l'utente tenta di eseguire nuovamente l'operazione senza approvazione, viene visualizzata una notifica simile alla seguente:

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

### Procedura CLI

1. Inserire l'operazione protetta direttamente o utilizzando il comando di richiesta MAV.

**Esempi – per eliminare un volume, immettere uno dei seguenti comandi:**

° volume delete

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
      verification request use "security multi-admin-verify
request
      create".

      Would you like to create a request for this operation?
      {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
      auto-generated and requires approval.
```

° security multi-admin-verify request create "volume delete"

```
Error: command failed: The security multi-admin-verify request (index
3)
      requires approval.
```

2. Controllare lo stato della richiesta e rispondere all'avviso MAV.

- a. Se la richiesta viene approvata, rispondere al messaggio CLI per completare l'operazione.

**Esempio:**

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll1
    State: approved
Required Approvers: 1
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: admin2
    User Vetoed: -
      Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

Info: Volume "voll1" in Vserver "vs0" will be marked as deleted and placed in the volume recovery queue. The space used by the volume will be recovered only after the retention period of 12 hours has completed. To recover the space immediately, get the volume name using (privilege:advanced) "volume recovery-queue show voll1\_\*" and then "volume recovery-queue purge -vserver vs0 -volume <volume\_name>" command. To recover the volume use the (privilege:advanced) "volume recovery-queue recover -vserver vs0 -volume <volume\_name>" command.

Warning: Are you sure you want to delete volume "voll1" in Vserver "vs0" ?  
{y|n}: y

- b. Se la richiesta è stata vetoata o il periodo di scadenza è scaduto, eliminarla e reinviarla o contattare l'amministratore MAV.

**Esempio:**

```
cluster-1::> security multi-admin-verify request show 3
```

```
    Request Index: 3
      Operation: volume delete
        Query: -vserver vs0 -volume voll1
        State: vetoed
Required Approvers: 1
Pending Approvers: 1
  Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
    Approvals: -
      User Vetoed: admin2
      Vserver: cluster-1
  User Requested: admin
    Time Created: 2/25/2022 13:38:47
    Time Approved: -
      Comment: -
  Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

```
Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

## Gestire le richieste di operazioni protette

Quando gli amministratori di un gruppo di approvazione MAV (amministratori MAV) ricevono una notifica di una richiesta di esecuzione dell'operazione in sospeso, devono rispondere con un messaggio di approvazione o veto entro un periodo di tempo fisso (scadenza dell'approvazione). Se non si riceve un numero sufficiente di approvazioni, il richiedente deve eliminare la richiesta ed effettuare un'altra.

### A proposito di questa attività

Le richieste di approvazione sono identificate con numeri di indice, inclusi nei messaggi e-mail e nelle visualizzazioni della coda di richiesta.

È possibile visualizzare le seguenti informazioni dalla coda di richiesta:

### Operazione

Operazione protetta per la quale viene creata la richiesta.

### Query

Oggetto (o oggetti) su cui l'utente desidera applicare l'operazione.

## **Stato**

Lo stato corrente della richiesta: In sospeso, approvato, rifiutato, scaduto, eseguito. Se una richiesta viene respinta da un responsabile dell'approvazione, non sono possibili ulteriori azioni.

## **Responsabili dell'approvazione richiesti**

Il numero di amministratori MAV necessari per approvare la richiesta. Un utente può impostare il parametro `required-approvers` per la regola dell'operazione. Se un utente non imposta i responsabili dell'approvazione richiesti sulla regola, vengono applicati i responsabili dell'approvazione richiesti dall'impostazione globale.

## **Responsabili dell'approvazione in sospeso**

Il numero di amministratori MAV che sono ancora necessari per approvare la richiesta per essere contrassegnati come approvati.

## **Scadenza approvazione**

Periodo entro il quale un amministratore MAV deve rispondere a una richiesta di approvazione. Qualsiasi utente autorizzato può impostare la scadenza dell'approvazione per una regola dell'operazione. Se la regola non è impostata su approvazione-scadenza, viene applicata l'approvazione-scadenza dall'impostazione globale.

## **Scadenza dell'esecuzione**

Il periodo entro il quale l'amministratore richiedente deve completare l'operazione. Qualsiasi utente autorizzato può impostare la scadenza dell'esecuzione per una regola dell'operazione. Se la regola non è impostata su `execution-expiry`, viene applicata l'impostazione di `execution-expiry` dall'impostazione globale.

## **Approvati dagli utenti**

Gli amministratori MAV che hanno approvato la richiesta.

## **Veto dell'utente**

Gli amministratori MAV che hanno posto il veto alla richiesta.

## **Storage VM (vserver)**

SVM a cui è associata la richiesta. Solo la SVM amministrativa è supportata in questa release.

## **Richiesto dall'utente**

Il nome utente dell'utente che ha creato la richiesta.

## **Ora di creazione**

L'ora in cui viene creata la richiesta.

## **Tempo approvato**

L'ora in cui lo stato della richiesta è cambiato in approvato.

## **Commento**

Eventuali commenti associati alla richiesta.

## **Utenti consentiti**

L'elenco degli utenti autorizzati a eseguire l'operazione protetta per cui la richiesta è approvata. Se `users-permitted` è vuoto, quindi qualsiasi utente con autorizzazioni appropriate può eseguire l'operazione.

Tutte le richieste scadute o eseguite vengono eliminate quando viene raggiunto un limite di 1000 richieste o quando il tempo di scadenza è superiore a 8 ore per le richieste scadute. Le richieste vetoed vengono

eliminate una volta contrassegnate come scadute.

### Procedura di System Manager

Gli amministratori MAV ricevono messaggi e-mail con i dettagli della richiesta di approvazione, il periodo di scadenza della richiesta e un link per approvare o rifiutare la richiesta. È possibile accedere a una finestra di dialogo di approvazione facendo clic sul collegamento nell'e-mail o accedendo a **Eventi e lavori> Richieste** in System Manager.

La finestra **Requests** (Richieste) è disponibile quando è attivata la verifica multi-admin, mostrando le richieste in sospeso in base all'ID di accesso dell'utente e al ruolo MAV (approvatore o meno).

- Operazione
- Indice (numero)
- Stato (in sospeso, approvato, rifiutato, eseguito o scaduto)

Se una richiesta viene respinta da un responsabile dell'approvazione, non sono possibili ulteriori azioni.

- Query (qualsiasi parametro o valore per l'operazione richiesta)
- Utente richiedente
- La richiesta scade il
- (Numero di) approvatori in sospeso
- (Numero di) potenziali responsabili dell'approvazione

Gli amministratori MAV dispongono di controlli aggiuntivi in questa finestra; possono approvare, rifiutare o eliminare singole operazioni o gruppi di operazioni selezionati. Tuttavia, se l'amministratore MAV è l'utente richiedente, non può approvare, rifiutare o eliminare le proprie richieste.

### Procedura CLI

1. Quando viene inviata una notifica via email delle richieste in sospeso, annotare il numero di indice della richiesta e il periodo di scadenza dell'approvazione. Il numero dell'indice può essere visualizzato anche utilizzando le opzioni **show** o **show-pending** indicate di seguito.
2. Approvare o veto la richiesta.

Se si desidera...	Immettere questo comando
Approvare una richiesta	<code>security multi-admin-verify request approve nn</code>
Veto di una richiesta	<code>security multi-admin-verify request veto nn</code>
Mostra tutte le richieste, le richieste in sospeso o una singola richiesta	<code>`security multi-admin-verify request { show</code>

Se si desidera...	Immettere questo comando
show-pending } [nn] { -fields <i>field1</i> [, <i>field2</i> ...]	[-instance ] }`  È possibile visualizzare tutte le richieste nella coda o solo quelle in sospeso. Se si inserisce il numero di indice, vengono visualizzate solo le informazioni relative a tale valore. È possibile visualizzare informazioni su campi specifici utilizzando -fields o su tutti i campi (utilizzando il -instance parametro).
Eliminare una richiesta	security multi-admin-verify request delete nn

### Esempio:

La seguente sequenza approva una richiesta dopo che l'amministratore MAV ha ricevuto l'email di richiesta con il numero di indice 3, che ha già un'approvazione.

```

cluster1::> security multi-admin-verify request show-pending
                                Pending
Index Operation      Query State  Approvers Requestor
-----
   3 volume delete  -    pending 1      julia

cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
  Operation: volume delete
    Query: -
    State: approved
Required Approvers: 2
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
    Approvals: mav-admin2
    User Vetoed: -
      Vserver: cluster-1
User Requested: julia
  Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -

```

### Esempio:

La seguente sequenza veto una richiesta dopo che l'amministratore MAV ha ricevuto l'email di richiesta con il numero di indice 3, che ha già un'approvazione.

```
cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete    -      pending 1      pavan

cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
  Operation: volume delete
    Query: -
    State: vetoed
Required Approvers: 2
Pending Approvers: 0
Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
  Approvals: mav-admin1
  User Vetoed: mav-admin2
    Vserver: cluster-1
User Requested: pavan
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -
```

## Autenticazione e autorizzazione utilizzando OAuth 2,0

### Panoramica dell'implementazione di ONTAP OAuth 2,0

A partire da ONTAP 9,14, puoi controllare l'accesso ai tuoi cluster ONTAP utilizzando il framework Open Authorization (OAuth 2,0). Puoi configurare questa funzionalità utilizzando qualsiasi interfaccia amministrativa di ONTAP, inclusi l'interfaccia a riga di comando di ONTAP, System Manager e l'API REST. Tuttavia, le decisioni relative all'autorizzazione e al controllo dell'accesso OAuth 2,0 possono essere applicate solo quando un client accede a ONTAP utilizzando l'API REST.





Il supporto di OAuth 2,0 è stato introdotto per la prima volta con ONTAP 9.14.0, pertanto la sua disponibilità dipende dalla versione di ONTAP in uso. Vedere ["Note di rilascio di ONTAP"](#) per ulteriori informazioni.

## Caratteristiche e vantaggi

Di seguito sono descritte le principali caratteristiche e i vantaggi dell'utilizzo di OAuth 2,0 con ONTAP.

### Supporto per lo standard OAuth 2,0

OAuth 2,0 è il quadro di autorizzazione standard del settore. Viene utilizzato per limitare e controllare l'accesso alle risorse protette utilizzando token di accesso firmati. L'utilizzo di OAuth 2,0 offre diversi vantaggi:

- Molte opzioni per la configurazione dell'autorizzazione
- Non rivelare mai le credenziali del client, incluse le password
- I token possono essere impostati in modo che scadano in base alla configurazione
- Ideale per l'uso con API REST

### Testato con diversi server di autorizzazione più diffusi

L'implementazione di ONTAP è progettata per essere compatibile con qualsiasi server di autorizzazione conforme a OAuth 2,0. È stato testato con i seguenti server o servizi comuni, tra cui:

- Auth0
- Active Directory Federation Service (ADFS)
- Keycloak

### Supporto per più server di autorizzazione simultanei

È possibile definire fino a otto server di autorizzazione per un singolo cluster ONTAP. Ciò offre la flessibilità necessaria per soddisfare le esigenze dei diversi ambienti di sicurezza.

### Integrazione con i ruoli REST

Le decisioni di autorizzazione ONTAP si basano in ultima analisi sui ruoli REST assegnati a utenti o gruppi. Questi ruoli vengono riportati nel token di accesso come ambiti indipendenti o in base alle definizioni ONTAP locali insieme ai gruppi Active Directory o LDAP.

### Opzione per utilizzare token di accesso con restrizioni del mittente

È possibile configurare ONTAP e i server di autorizzazione per utilizzare Mutual Transport Layer Security (mTLS) che rafforza l'autenticazione client. Garantisce che i token di accesso OAuth 2,0 siano utilizzati solo dai client ai quali sono stati originariamente rilasciati. Questa funzionalità supporta e si allinea con diverse raccomandazioni di protezione note, incluse quelle stabilite da FAPI e MITER.

## Implementazione e configurazione

A un livello elevato, ci sono diversi aspetti di un'implementazione e configurazione di OAuth 2,0 che è necessario considerare quando si inizia.

### OAuth 2,0 entità all'interno di ONTAP

Il framework di autorizzazione OAuth 2,0 definisce diverse entità che possono essere mappate ad elementi reali o virtuali all'interno del data center o della rete. Le entità OAuth 2,0 e il loro adattamento a ONTAP sono presentati nella tabella seguente.

Entità OAuth 2,0	Descrizione
Risorsa	Gli endpoint delle API REST che forniscono accesso alle risorse ONTAP tramite comandi ONTAP interni.
Proprietario della risorsa	L'utente del cluster ONTAP che ha creato la risorsa protetta o la possiede per impostazione predefinita.
Server delle risorse	L'host per le risorse protette, ovvero il cluster ONTAP.
Client	Un'applicazione che richiede l'accesso a un endpoint API REST per conto o con l'autorizzazione del proprietario della risorsa.
Server di autorizzazione	In genere, un server dedicato responsabile dell'emissione dei token di accesso e dell'applicazione dei criteri amministrativi.

### Configurazione core ONTAP

È necessario configurare il cluster ONTAP per abilitare e utilizzare OAuth 2,0. Ciò include la creazione di una connessione al server di autorizzazione e la definizione della configurazione di autorizzazione ONTAP richiesta. È possibile eseguire questa configurazione utilizzando una qualsiasi delle interfacce amministrative, tra cui:

- Interfaccia a riga di comando di ONTAP
- System Manager
- API REST di ONTAP

### Ambiente e servizi di supporto

Oltre alle definizioni di ONTAP, è necessario configurare anche i server di autorizzazione. Se si utilizza la mappatura da gruppo a ruolo, è necessario configurare anche i gruppi Active Directory o l'equivalente LDAP.

### Client ONTAP supportati

A partire da ONTAP 9,14, un client API REST può accedere a ONTAP utilizzando OAuth 2,0. Prima di eseguire una chiamata API REST, è necessario ottenere un token di accesso dal server di autorizzazione. Il client passa quindi questo token al cluster ONTAP come *bearer token* utilizzando l'intestazione della richiesta di autorizzazione HTTP. A seconda del livello di protezione necessario, è anche possibile creare e installare un certificato nel client per utilizzare token con vincoli di mittente basati su mTLS.

### Terminologia selezionata

Quando si inizia a esaminare la distribuzione di OAuth 2,0 con ONTAP, è utile acquisire familiarità con alcune parti della terminologia. Vedere ["Risorse aggiuntive"](#) Per collegamenti a ulteriori informazioni su OAuth 2,0.

### Token di accesso

Token emesso da un server di autorizzazione e utilizzato da un'applicazione client OAuth 2,0 per effettuare richieste di accesso alle risorse protette.

### Token Web JSON

Lo standard utilizzato per formattare i token di accesso. JSON viene utilizzato per rappresentare le rivendicazioni OAuth 2,0 in formato compatto con le rivendicazioni disposte in tre sezioni principali.

### Token di accesso vincolato dal mittente

Funzione opzionale basata sul protocollo mTLS (Mutual Transport Layer Security). Utilizzando un'ulteriore richiesta di conferma nel token, questo garantisce che il token di accesso venga utilizzato solo dal client al quale è stato originariamente emesso.

## Set di chiavi Web JSON

Un JWKS è un insieme di chiavi pubbliche utilizzate da ONTAP per verificare i token JWT presentati dai clienti. I set di chiavi sono generalmente disponibili sul server di autorizzazione tramite un URI dedicato.

## Scopo

Gli ambiti forniscono un modo per limitare o controllare l'accesso di un'applicazione alle risorse protette come l'API REST ONTAP. Sono rappresentate come stringhe nel token di accesso.

## Ruolo REST di ONTAP

I ruoli REST sono stati introdotti con ONTAP 9,6 e costituiscono una parte fondamentale del framework RBAC di ONTAP. Questi ruoli sono diversi dai ruoli tradizionali precedenti che sono ancora supportati da ONTAP. L'implementazione di OAuth 2,0 in ONTAP supporta solo i ruoli REST.

## Intestazione autorizzazione HTTP

Intestazione inclusa nella richiesta HTTP per identificare il client e le autorizzazioni associate come parte di una chiamata API REST. Sono disponibili diverse varianti o implementazioni a seconda della modalità di autenticazione e autorizzazione. Quando si presenta un token di accesso OAuth 2,0 a ONTAP, il token viene identificato come *token bearer*.

## Autenticazione di base HTTP

Una tecnica di autenticazione HTTP avanzata ancora supportata da ONTAP. Le credenziali in testo normale (nome utente e password) sono concatenate con due punti e codificate in base64. La stringa viene inserita nell'intestazione della richiesta di autorizzazione e inviata al server.

## FAPI

Un gruppo di lavoro della OpenID Foundation che fornisce protocolli, schemi di dati e raccomandazioni sulla sicurezza per il settore finanziario. L'API era originariamente nota come API di livello finanziario.

## MITRA

Un'azienda privata senza scopo di lucro che fornisce una guida tecnica e di sicurezza all'aeronautica militare degli Stati Uniti e al governo degli Stati Uniti.

## Risorse aggiuntive

Di seguito sono riportate diverse risorse aggiuntive. Dovreste rivedere questi luoghi per ottenere più informazioni su OAuth 2,0 e sugli standard relativi.

### Protocolli e standard

- ["RFC 6749: Framework di autorizzazione OAuth 2,0"](#)
- ["RFC 7519: Token Web JSON \(JWT\)"](#)
- ["RFC 7523: Profilo JSON Web Token \(JWT\) per l'autenticazione client OAuth 2,0 e le concessioni di autorizzazione"](#)
- ["RFC 7662: Introspezione token OAuth 2,0"](#)
- ["RFC 7800: Chiave di prova del possesso per JWT"](#)
- ["RFC 8705: Autenticazione client OAuth 2,0 Mutual-TLS e token di accesso con associazione a certificati"](#)

### Governativi

- ["Fondazione OpenID"](#)
- ["Gruppo di lavoro FAPI"](#)

- ["MITRA"](#)
- ["IANA - JWT"](#)

## Prodotti e servizi

- ["Auth0"](#)
- ["Panoramica di ADFS"](#)
- ["Keycloak"](#)

## Strumenti e utilità aggiuntivi

- ["JWT entro il Auth0"](#)
- ["OpenSSL"](#)

## Documentazione e risorse di NetApp

- ["Automazione ONTAP"](#) documentazione

## Concetti

### Server di autorizzazione e token di accesso

I server di autorizzazione svolgono diverse funzioni importanti come componente centrale all'interno del framework OAuth 2,0 Authorization.

#### Server di autorizzazione OAuth 2,0

I server di autorizzazione sono principalmente responsabili della creazione e della firma dei token di accesso. Questi token contengono informazioni di identità e autorizzazione che consentono a un'applicazione client di accedere in modo selettivo alle risorse protette. I server sono generalmente isolati l'uno dall'altro e possono essere implementati in diversi modi, incluso come server dedicato standalone o come parte di un prodotto di gestione delle identità e degli accessi più ampio.



A volte è possibile utilizzare una terminologia diversa per un server di autorizzazione, specialmente quando la funzionalità OAuth 2,0 è inclusa in un prodotto o una soluzione di gestione delle identità e degli accessi più ampia. Ad esempio, il termine **provider di identità (IdP)** viene spesso utilizzato in modo intercambiabile con **server di autorizzazione**.

## Amministrazione

Oltre all'emissione di token di accesso, i server di autorizzazione forniscono anche servizi amministrativi correlati, in genere tramite un'interfaccia utente Web. Ad esempio, è possibile definire e amministrare:

- Autenticazione degli utenti e degli utenti
- Ambiti
- Segregazione amministrativa attraverso locatari e regni
- Applicazione delle policy
- Collegamento a vari servizi esterni
- Supporto per altri protocolli di identità (come SAML)

ONTAP è compatibile con i server di autorizzazione conformi allo standard OAuth 2,0.

## Definizione di ONTAP

È necessario definire uno o più server di autorizzazione in ONTAP. ONTAP comunica in modo sicuro con ciascun server per verificare i token ed eseguire altre attività correlate a supporto delle applicazioni client.

Di seguito sono illustrati gli aspetti principali della configurazione di ONTAP. Vedere anche ["Scenari di distribuzione di OAuth 2,0"](#) per ulteriori informazioni.

### Come e dove vengono convalidati i token di accesso

Sono disponibili due opzioni per la convalida dei token di accesso.

- Convalida locale

ONTAP può convalidare i token di accesso localmente in base alle informazioni fornite dal server di autorizzazione che ha emesso il token. Le informazioni recuperate dal server di autorizzazione vengono memorizzate nella cache da ONTAP e aggiornate a intervalli regolari.

- Introspezione remota

È inoltre possibile utilizzare l'introspezione remota per convalidare i token nel server di autorizzazione. Introspezione è un protocollo che consente alle parti autorizzate di interrogare un server di autorizzazione su un token di accesso. Fornisce a ONTAP un modo per estrarre determinati metadati da un token di accesso e convalidare il token. ONTAP memorizza nella cache alcuni dati per motivi di prestazioni.

### Posizione di rete

ONTAP potrebbe essere protetto da un firewall. In questo caso, è necessario identificare un proxy come parte della configurazione.

### Come vengono definiti i server di autorizzazione

Puoi definire un server di autorizzazione per ONTAP utilizzando qualsiasi interfaccia amministrativa, inclusa CLI, System Manager o API REST. Ad esempio, con l'interfaccia CLI si utilizza il comando `security oauth2 client create`.

### Numero di server di autorizzazione

È possibile definire fino a otto server di autorizzazione per un singolo cluster ONTAP. Lo stesso server di autorizzazione può essere definito più di una volta nello stesso cluster ONTAP, purché le attestazioni dell'emittente o dell'emittente/pubblico siano univoche. Per esempio, con Keycloak questo sarà sempre il caso quando si usano reami diversi.

### Utilizzo dei token di accesso OAuth 2,0

I token di accesso OAuth 2,0 emessi dai server di autorizzazione vengono verificati da ONTAP e utilizzati per prendere decisioni di accesso basate sui ruoli per le richieste dei client API REST.

### Acquisizione di un token di accesso

È necessario acquisire un token di accesso da un server di autorizzazione definito nel cluster ONTAP in cui si utilizza l'API REST. Per acquisire un token, è necessario contattare direttamente il server di autorizzazione.



ONTAP non rilascia token di accesso o reindirizza le richieste dai client ai server di autorizzazione.

Il modo in cui si richiede un token dipende da diversi fattori, tra cui:

- Server di autorizzazione e relative opzioni di configurazione
- Tipo di concessione OAuth 2,0
- Client o strumento software utilizzato per emettere la richiesta

## Tipi di sovvenzione

Un *grant* è un processo ben definito, che include un insieme di flussi di rete, utilizzato per richiedere e ricevere un token di accesso OAuth 2,0. A seconda dei requisiti del client, dell'ambiente e della protezione, è possibile utilizzare diversi tipi di concessione. Un elenco dei tipi di sovvenzione più comuni è presentato nella tabella seguente.

Tipo di concessione	Descrizione
Credenziali client	Tipo di concessione comune basato sull'utilizzo di credenziali (come ID e segreto condiviso). Si presuppone che il client abbia una stretta relazione di trust con il proprietario della risorsa.
Password	È possibile utilizzare il tipo di concessione delle credenziali della password del proprietario della risorsa nei casi in cui il proprietario della risorsa abbia una relazione di trust stabilita con il client. Può essere utile anche per la migrazione di client HTTP legacy a OAuth 2,0.
Codice di autorizzazione	Si tratta di un tipo di sovvenzione ideale per i client riservati e si basa su un flusso basato sul reindirizzamento. Può essere utilizzato per ottenere sia un token di accesso che un token di aggiornamento.

## Contenuti JWT

Un token di accesso OAuth 2,0 è formattato come JWT. Il contenuto viene creato dal server di autorizzazione in base alla configurazione. Tuttavia, i token sono opachi per le applicazioni client. Un cliente non ha motivo di ispezionare un token o di essere a conoscenza del contenuto.

Ogni token di accesso JWT contiene una serie di attestazioni. Le attestazioni descrivono le caratteristiche dell'emittente e l'autorizzazione basata sulle definizioni amministrative del server di autorizzazione. Alcuni dei reclami registrati con la norma sono descritti nella tabella seguente. Tutte le stringhe rilevano la distinzione tra maiuscole e minuscole.

Reclamo	Parola chiave	Descrizione
Emittente	iss	Identifica l'entità che ha emesso il token. L'elaborazione della richiesta di rimborso è specifica per l'applicazione.
Soggetto	sub	L'oggetto o l'utente del token. Il nome è considerato univoco a livello globale o locale.
Pubblico	aud	I destinatari a cui è destinato il token. Implementato come array di stringhe.
Scadenza	scad	Il tempo dopo il quale il token scade e deve essere rifiutato.

Vedere ["RFC 7519: Token Web JSON"](#) per ulteriori informazioni.

## Opzioni per l'autorizzazione client ONTAP

Sono disponibili diverse opzioni per personalizzare l'autorizzazione del client ONTAP. Le

decisioni di autorizzazione si basano, in ultima analisi, sui ruoli REST ONTAP contenuti o derivati dai token di accesso.



È possibile utilizzare solo **"Ruoli REST di ONTAP"** Quando si configura l'autorizzazione per OAuth 2,0. I ruoli tradizionali ONTAP precedenti non sono supportati.

## Introduzione

L'implementazione di OAuth 2,0 all'interno di ONTAP è progettata per essere flessibile e robusta, fornendo le opzioni necessarie per proteggere l'ambiente ONTAP. A un livello elevato, esistono tre categorie di configurazione principali per la definizione dell'autorizzazione del client ONTAP. Queste opzioni di configurazione si escludono a vicenda.

ONTAP applica la singola opzione più appropriata in base alla configurazione scelta. Vedere ["Modalità con cui ONTAP determina l'accesso"](#) Per ulteriori informazioni su come ONTAP elabora le definizioni di configurazione per prendere decisioni sugli accessi.

## Oscilloscopi indipendenti OAuth 2,0

Questi ambiti contengono uno o più ruoli REST personalizzati, ciascuno incapsulato in una singola stringa. Sono indipendenti dalle definizioni dei ruoli ONTAP. È necessario definire queste stringhe di ambito nel server di autorizzazione.

### Ruoli e utenti REST locali specifici di ONTAP

In base alla configurazione, è possibile utilizzare le definizioni di identità ONTAP locali per prendere decisioni di accesso. Le opzioni includono:

- Singolo ruolo REST denominato
- Corrispondenza del nome utente con un utente ONTAP locale

La sintassi dell'ambito per un ruolo denominato è **ontap-role-`<URL-encoded-ONTAP-role-name>`**. Ad esempio, se il ruolo è "admin" la stringa dell'ambito sarà "ontap-role-admin".

### Active Directory o gruppi LDAP

Se vengono esaminate le definizioni ONTAP locali ma non è possibile prendere alcuna decisione di accesso, vengono utilizzati i gruppi Active Directory ("dominio") o LDAP ("nsswitch"). Le informazioni sul gruppo possono essere specificate in due modi:

- Stringa OAuth 2,0 Scope

Supporta le applicazioni riservate utilizzando il flusso di credenziali client in cui non vi è alcun utente con appartenenza a un gruppo. L'ambito deve essere denominato **ontap-group-`<URL-encoded-ONTAP-group-name>`**. Ad esempio, se il gruppo è "sviluppo" la stringa dell'ambito sarà "ontap-group-development".

- Nella richiesta di "gruppo"

Questa funzione è destinata ai token di accesso emessi da ADFS utilizzando il flusso proprietario della risorsa (concessione password).

## Oscilloscopi OAuth 2,0 autonomi

Gli scope autonomi sono stringhe trasportate nel token di accesso. Ognuno di essi costituisce una definizione completa e personalizzata del ruolo e include tutto ciò che ONTAP ha bisogno per prendere una decisione di accesso. L'ambito è separato e distinto dai ruoli REST definiti all'interno di ONTAP stesso.

## Formato della stringa Scope

A livello base, l'ambito è rappresentato come una stringa contigua e composta da sei valori separati da due punti. I parametri utilizzati nella stringa Scope sono descritti di seguito.

### Letterale di ONTAP

L'ambito deve iniziare con il valore letterale `ontap` in minuscolo. Questo identifica l'ambito come specifico di ONTAP.

### Cluster

Definisce il cluster ONTAP a cui si applica l'ambito. I valori possono includere:

- UUID cluster

Identificazione di un singolo cluster.

- Asterisco (\*)

Indica che l'ambito si applica a tutti i cluster.

È possibile utilizzare il comando CLI di ONTAP `cluster identity show` Per visualizzare l'UUID del cluster. Se non specificato, l'ambito si applica a tutti i cluster.

### Ruolo

Il nome del ruolo di RIPOSO contenuto nell'ambito autonomo. Questo valore non viene esaminato da ONTAP o abbinato a ruoli REST esistenti definiti in ONTAP. Il nome viene utilizzato per la registrazione.

### Livello di accesso

Questo valore indica il livello di accesso applicato all'applicazione client quando si utilizza l'endpoint API nell'ambito. Sono disponibili sei valori, come descritto nella tabella seguente.

Livello di accesso	Descrizione
nessuno	Nega tutti gli accessi all'endpoint specificato.
readonly	Consente solo l'accesso in lettura utilizzando GET.
read_create	Consente l'accesso in lettura e la creazione di nuove istanze di risorse utilizzando POST.
read_modify	Consente l'accesso in lettura e la possibilità di aggiornare le risorse esistenti utilizzando PATCH.
read_create_modify	Consente tutti gli accessi ad eccezione dell'eliminazione. Le operazioni consentite includono GET (lettura), POST (creazione) e PATCH (aggiornamento).
tutto	Consente l'accesso completo.

### SVM

Nome della SVM all'interno del cluster a cui si applica l'ambito. Utilizzare il valore \* (asterisco) per indicare tutte le SVM.





Questa funzione non è completamente supportata con ONTAP 9.14.1. È possibile ignorare il parametro SVM e utilizzare un asterisco come segnaposto. Esaminare ["Note di rilascio di ONTAP"](#) Per verificare il supporto SVM futuro.

## URI API REST

Percorso completo o parziale di una risorsa o di una serie di risorse correlate. La stringa deve iniziare con `/api`. Se non si specifica un valore, l'ambito si applica a tutti gli endpoint API nel cluster ONTAP.

## Esempi di ambito

Di seguito sono riportati alcuni esempi di ambiti auto-contenuti.

### `ontap*:joes-role:read_create_modify:*/api/cluster`

Fornisce all'utente assegnato a questo ruolo l'accesso di lettura, creazione e modifica al `/cluster` endpoint.

## Strumento di amministrazione CLI

Per rendere più semplice e meno incline agli errori l'amministrazione degli ambiti autonomi, ONTAP fornisce il comando CLI `security oauth2 scope` per generare stringhe di ambito in base ai parametri di input.

Il comando `security oauth2 scope` ha due casi d'utilizzo sulla base delle tue indicazioni:

- Parametri CLI per la stringa di ambito

È possibile utilizzare questa versione del comando per generare una stringa di ambito in base ai parametri di input.

- Stringa di ambito per i parametri CLI

È possibile utilizzare questa versione del comando per generare i parametri del comando in base alla stringa dell'ambito di input.

## Esempio

Nell'esempio seguente viene generata una stringa di scope con l'output incluso dopo l'esempio di comando riportato di seguito. La definizione si applica a tutti i cluster.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap*:joes-role:readonly:*/api/cluster
```

## Modalità con cui ONTAP determina l'accesso

Per progettare e implementare correttamente OAuth 2.0, è necessario comprendere in che modo la configurazione delle autorizzazioni viene utilizzata da ONTAP per prendere decisioni di accesso per i client.

## Fase 1: Oscilloscopi autonomi

Se il token di accesso contiene ambiti indipendenti, ONTAP esamina prima tali ambiti. Se non sono presenti oscilloscopi autonomi, passare al punto 2.

Con uno o più ambiti auto-contenuti presenti, ONTAP applica ogni ambito fino a quando non può essere presa una decisione esplicita **ALLOW** o **DENY**. Se viene presa una decisione esplicita, l'elaborazione termina.

Se ONTAP non è in grado di prendere una decisione di accesso esplicita, continuare con il passaggio 2.

#### **Passaggio 2: Controllare il flag dei ruoli locali**

ONTAP esamina il valore del flag `use-local-roles-if-present`. Il valore di questo indicatore viene impostato separatamente per ogni server di autorizzazione definito su ONTAP.

- Se il valore è `true` passare alla fase 3.
- Se il valore è `false` l'elaborazione termina e l'accesso è negato.

#### **Passaggio 3: Ruolo REST di Named ONTAP**

Se il token di accesso contiene un ruolo REST denominato, ONTAP utilizza il ruolo per prendere la decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l'elaborazione termina.

Se non è presente alcun ruolo REST denominato o se il ruolo non è stato trovato, passare al punto 4.

#### **Fase 4: Utenti ONTAP locali**

Estrarre il nome utente dal token di accesso e tentare di associarlo a un utente ONTAP locale.

Se un utente ONTAP locale viene associato, ONTAP utilizza il ruolo definito per l'utente per prendere una decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l'elaborazione termina.

Se un utente ONTAP locale non corrisponde o se non è presente alcun nome utente nel token di accesso, passare al punto 5.

#### **Fase 5: Mappatura da gruppo a ruolo**

Estrarre il gruppo dal token di accesso e tentare di associarlo a un gruppo. I gruppi vengono definiti utilizzando Active Directory o un server LDAP equivalente.

Se esiste una corrispondenza di gruppo, ONTAP utilizza il ruolo definito per il gruppo per prendere una decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l'elaborazione termina.

Se non è presente alcuna corrispondenza di gruppo o se non è presente alcun gruppo nel token di accesso, l'accesso viene negato e l'elaborazione termina.

#### **Scenari di distribuzione di OAuth 2,0**

Quando si definisce un server di autorizzazione per ONTAP, sono disponibili diverse opzioni di configurazione. In base a queste opzioni, è possibile creare un server di autorizzazione appropriato per l'ambiente di distribuzione.

#### **Riepilogo dei parametri di configurazione**

Quando si definisce un server di autorizzazione per ONTAP, sono disponibili diversi parametri di configurazione. Questi parametri sono generalmente supportati in tutte le interfacce amministrative.

I nomi dei parametri possono variare leggermente a seconda dell'interfaccia amministrativa di ONTAP. Ad esempio, quando si configura l'introspezione remota, l'endpoint viene identificato utilizzando il parametro del comando CLI `-introspection-endpoint`. Con System Manager, il campo equivalente è *Authorization server token introspection URI*. Per soddisfare tutte le interfacce amministrative di ONTAP, viene fornita una descrizione generale dei parametri. Il parametro o il campo esatto dovrebbe essere ovvio in base al contesto.

Parametro	Descrizione
Nome	Il nome del server di autorizzazione così come è noto a ONTAP.
Applicazione	L'applicazione interna ONTAP a cui si applica la definizione. Deve essere <b>http</b> .
URI emittente	FQDN con percorso che identifica il sito o l'organizzazione che emette i token.
Provider JWKS URI	L'FQDN con percorso e nome file in cui ONTAP ottiene i set di chiavi Web JSON utilizzati per convalidare i token di accesso.
Intervallo di aggiornamento JWKS	L'intervallo di tempo che determina la frequenza con cui ONTAP aggiorna le informazioni del certificato dall'URI JWKS del provider. Il valore è specificato in formato ISO-8601.
Endpoint introspezione	L'FQDN con percorso utilizzato da ONTAP per eseguire la convalida dei token remoti tramite introspezione.
ID client	Il nome del client come definito nel server di autorizzazione. Quando questo valore è incluso, è necessario anche fornire il segreto client associato in base all'interfaccia.
Proxy in uscita	In questo modo viene fornito l'accesso al server di autorizzazione quando ONTAP è protetto da un firewall. L'URI deve essere in formato Curl.
Utilizzare i ruoli locali, se presenti	Un flag booleano che determina se vengono utilizzate le definizioni ONTAP locali, inclusi un ruolo REST denominato e gli utenti locali.
Rimuovere la richiesta di rimborso dell'utente	Un nome alternativo utilizzato da ONTAP per associare gli utenti locali. Utilizzare <code>sub</code> nel token di accesso in modo che corrisponda al nome utente locale.

## Scenari di distribuzione

Di seguito vengono presentati diversi scenari di distribuzione comuni. Sono organizzati in base al fatto che la convalida dei token venga eseguita localmente da ONTAP o in remoto dal server di autorizzazione. Ogni scenario include un elenco delle opzioni di configurazione richieste. Vedere ["Implementa OAuth 2,0 in ONTAP"](#) per esempi dei comandi di configurazione.



Dopo aver definito un server di autorizzazione, è possibile visualizzarne la configurazione tramite l'interfaccia amministrativa di ONTAP. Ad esempio, utilizzare il comando `security oauth2 client show` Con l'interfaccia a riga di comando di ONTAP.

## Convalida locale

I seguenti scenari di distribuzione si basano su ONTAP che esegue la convalida dei token localmente.

### Utilizzare gli oscilloscopi autonomi senza proxy

Questa è l'implementazione più semplice che utilizza solo gli oscilloscopi indipendenti OAuth 2,0. Nessuna delle definizioni di identità ONTAP locali viene utilizzata. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- URI emittente

È inoltre necessario aggiungere gli ambiti al server di autorizzazione.

### Utilizzare gli oscilloscopi autonomi con un proxy

Questo scenario di distribuzione utilizza gli oscilloscopi indipendenti OAuth 2.0. Nessuna delle definizioni di identità ONTAP locali viene utilizzata. Ma il server di autorizzazione è protetto da un firewall e quindi è necessario configurare un proxy. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- Proxy in uscita
- URI emittente
- Pubblico

È inoltre necessario aggiungere gli ambiti al server di autorizzazione.

### Utilizzare ruoli utente locali e associazione nome utente predefinita con un proxy

Questo scenario di distribuzione utilizza ruoli utente locali con mappatura dei nomi predefinita. La richiesta di rimborso dell'utente remoto utilizza il valore predefinito di `sub` quindi questo campo nel token di accesso viene utilizzato per corrispondere al nome utente locale. Il nome utente deve contenere al massimo 40 caratteri. Il server di autorizzazione è protetto da un firewall, quindi è necessario configurare anche un proxy. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- Utilizzare i ruoli locali, se presenti (`true`)
- Proxy in uscita
- Emittente

È necessario assicurarsi che l'utente locale sia definito su ONTAP.

### Utilizzare ruoli utente locali e mapping nome utente alternativo con un proxy

Questo scenario di distribuzione utilizza ruoli utente locali con un nome utente alternativo utilizzato per associare un utente ONTAP locale. Il server di autorizzazione è protetto da un firewall, quindi è necessario configurare un proxy. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- Utilizzare i ruoli locali, se presenti (`true`)
- Richiesta di rimborso per utenti remoti
- Proxy in uscita
- URI emittente
- Pubblico

È necessario assicurarsi che l'utente locale sia definito su ONTAP.

## Introspezione remota

Le seguenti configurazioni di distribuzione si basano su ONTAP che esegue la convalida dei token in modalità remota tramite introspezione.

### Utilizzare gli oscilloscopi autonomi senza proxy

Si tratta di una semplice implementazione basata sull'utilizzo degli oscilloscopi indipendenti OAuth 2,0. Nessuna delle definizioni di identità ONTAP viene utilizzata. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Endpoint introspezione
- ID client
- URI emittente

È necessario definire gli ambiti, nonché il segreto client e client nel server di autorizzazione.

### Autenticazione client mediante TLS reciproco

A seconda delle esigenze di protezione, è possibile configurare il protocollo mTLS (Mutual TLS) per implementare l'autenticazione client avanzata. Quando viene utilizzato con ONTAP come parte di una distribuzione OAuth 2,0, mTLS garantisce che i token di accesso vengano utilizzati solo dai client ai quali sono stati originariamente emessi.

#### TLS reciproco con OAuth 2,0

Transport Layer Security (TLS) viene utilizzato per stabilire un canale di comunicazione sicuro tra due applicazioni, in genere un browser client e un server Web. Il TLS reciproco estende questa funzione fornendo una solida identificazione del client tramite un certificato client. Quando viene utilizzata in un cluster ONTAP con OAuth 2,0, la funzionalità mTLS di base viene estesa creando e utilizzando token di accesso con vincoli di mittente.

Un token di accesso vincolato dal mittente può essere utilizzato solo dal client al quale è stato originariamente emesso. Per supportare questa funzione, è necessario presentare una nuova richiesta di conferma (cnf) è inserito nel token. Il campo contiene proprietà `x5t#S256` che contiene un digest del certificato client utilizzato quando si richiede il token di accesso. Questo valore viene verificato da ONTAP come parte della convalida del token. I token di accesso emessi dai server di autorizzazione che non sono vincolati dal mittente non includono la richiesta di conferma aggiuntiva.

È necessario configurare ONTAP in modo che utilizzi mTLS separatamente per ogni server di autorizzazione. Ad esempio, il comando CLI `security oauth2 client include` il parametro `use-mutual-tls`. Per controllare l'elaborazione mTLS in base a tre valori, come mostrato nella tabella seguente.



In ogni configurazione, il risultato e l'azione intrapresi da ONTAP dipendono dal valore del parametro di configurazione, dal contenuto del token di accesso e dal certificato client. I parametri nella tabella sono organizzati dal minimo al più restrittivo.

Parametro	Descrizione
nessuno	L'autenticazione TLS reciproca OAuth 2,0 è completamente disattivata per il server di autorizzazione. ONTAP non eseguirà l'autenticazione del certificato client mTLS anche se la richiesta di conferma è presente nel token o se viene fornito un certificato client con la connessione TLS.
richiesta	L'autenticazione reciproca TLS OAuth 2,0 viene applicata se il client presenta un token di accesso con restrizioni del mittente. Vale a dire, mTLS viene applicato solo se la richiesta di conferma (con proprietà <code>x5t#S256</code> ) è presente nel token di accesso. Questa è l'impostazione predefinita.
obbligatorio	L'autenticazione TLS reciproca OAuth 2,0 viene applicata per tutti i token di accesso emessi dal server di autorizzazione. Pertanto, tutti i token di accesso devono essere vincolati dal mittente. L'autenticazione e la richiesta dell'API REST non riescono se la richiesta di conferma non è presente nel token di accesso o se è presente un certificato client non valido.

### Flusso di implementazione di alto livello

Di seguito vengono illustrati i passaggi tipici richiesti quando si utilizza mTLS con OAuth 2,0 in un ambiente ONTAP. Vedere ["RFC 8705: Autenticazione client OAuth 2,0 Mutual-TLS e token di accesso con associazione a certificati"](#) per ulteriori dettagli.

#### Passaggio 1: Creare e installare un certificato client

La definizione dell'identità del client si basa sulla prova della conoscenza di una chiave privata del client. La chiave pubblica corrispondente viene inserita in un certificato X.509 firmato presentato dal cliente. A un livello elevato, i passaggi necessari per la creazione del certificato client includono:

1. Generare una coppia di chiavi pubbliche e private
2. Creare una richiesta di firma del certificato
3. Inviare il file CSR a una CA nota
4. CA verifica la richiesta ed emette il certificato firmato

In genere è possibile installare il certificato client nel sistema operativo locale o utilizzarlo direttamente con un'utilità comune, ad esempio curl.

#### Passaggio 2: Configurare ONTAP per l'utilizzo di mTLS

È necessario configurare ONTAP per utilizzare mTLS. Questa configurazione viene eseguita separatamente per ogni server di autorizzazione. Ad esempio, con il CLI il comando `security oauth2 client` viene utilizzato con il parametro opzionale `use-mutual-tls`. Vedere ["Implementa OAuth 2,0 in ONTAP"](#) per ulteriori informazioni.

#### Passaggio 3: Il client richiede un token di accesso

Il client deve richiedere un token di accesso dal server di autorizzazione configurato su ONTAP. L'applicazione client deve utilizzare mTLS con il certificato creato e installato nel passaggio 1.

#### Passaggio 4: Il server di autorizzazione genera il token di accesso

Il server di autorizzazione verifica la richiesta del client e genera un token di accesso. Come parte di ciò, crea un riepilogo del messaggio del certificato client che è incluso nel token come richiesta di conferma (campo `cnf`).

#### Passaggio 5: L'applicazione client presenta il token di accesso a ONTAP

L'applicazione client effettua una chiamata API REST al cluster ONTAP e include il token di accesso nell'intestazione della richiesta di autorizzazione come token **bearer**. Il client deve utilizzare mTLS con lo stesso certificato utilizzato per richiedere il token di accesso.

#### **Passaggio 6: ONTAP verifica client e token.**

ONTAP riceve il token di accesso in una richiesta HTTP e il certificato client utilizzato come parte dell'elaborazione mTLS. ONTAP prima convalida la firma nel token di accesso. In base alla configurazione, ONTAP genera un riepilogo dei messaggi del certificato client e lo confronta con l'attestazione di conferma **cnf** nel token. Se i due valori corrispondono, ONTAP ha confermato che il client che effettua la richiesta API è lo stesso client a cui è stato originariamente emesso il token di accesso.

## **Configurazione e implementazione**

### **Preparati a implementare OAuth 2,0 con ONTAP**

Prima di configurare OAuth 2,0 in un ambiente ONTAP, è necessario prepararsi per la distribuzione. Di seguito è riportato un riepilogo delle principali attività e decisioni. La disposizione delle sezioni è generalmente allineata con l'ordine da seguire. Tuttavia, sebbene sia applicabile per la maggior parte delle implementazioni, è consigliabile adattarlo all'ambiente in base alle esigenze. È inoltre opportuno prendere in considerazione la creazione di un piano di distribuzione formale.



In base all'ambiente in uso, è possibile selezionare la configurazione per i server di autorizzazione definiti in ONTAP. Sono inclusi i valori dei parametri da specificare per ogni tipo di distribuzione. Vedere ["Scenari di distribuzione di OAuth 2,0"](#) per ulteriori informazioni.

### **Risorse protette e applicazioni client**

OAuth 2,0 è un framework di autorizzazione per controllare l'accesso alle risorse protette. In questo caso, un primo passo importante per qualsiasi distribuzione consiste nel determinare quali sono le risorse disponibili e quali client devono accedervi.

#### **Identificare le applicazioni client**

È necessario decidere quali client utilizzeranno OAuth 2,0 per l'emissione di chiamate API REST e a quali endpoint API devono accedere.

#### **Esaminare i ruoli REST ONTAP esistenti e gli utenti locali**

È necessario esaminare le definizioni di identità ONTAP esistenti, inclusi i ruoli REST e gli utenti locali. A seconda della configurazione di OAuth 2,0, queste definizioni possono essere utilizzate per prendere decisioni sugli accessi.

#### **Transizione globale a OAuth 2,0**

Sebbene sia possibile implementare l'autorizzazione OAuth 2,0 gradualmente, è anche possibile spostare immediatamente tutti i client API REST in OAuth 2,0 impostando un flag globale per ogni server di autorizzazione. In questo modo, è possibile prendere decisioni di accesso in base alla configurazione ONTAP esistente senza dover creare ambiti autonomi.

### **Server di autorizzazione**

I server di autorizzazione svolgono un ruolo importante nella distribuzione di OAuth 2,0 rilasciando token di accesso e applicando criteri amministrativi.

### **Selezionare e installare il server di autorizzazione**

È necessario selezionare e installare uno o più server di autorizzazione. È importante acquisire familiarità con le opzioni di configurazione e le procedure dei provider di identità, incluse le modalità di definizione degli ambiti.

### **Determinare se è necessario installare il certificato CA principale di autorizzazione**

ONTAP utilizza il certificato del server di autorizzazione per convalidare i token di accesso firmati presentati dai client. A tale scopo, ONTAP necessita del certificato della CA principale e di eventuali certificati intermedi. Questi potrebbero essere preinstallati con ONTAP. In caso contrario, è necessario installarli.

### **Valutare la posizione e la configurazione della rete**

Se il server di autorizzazione è protetto da un firewall, ONTAP deve essere configurato per utilizzare un server proxy.

### **Autenticazione e autorizzazione del client**

È necessario prendere in considerazione diversi aspetti dell'autenticazione e dell'autorizzazione dei client.

### **Ambiti indipendenti o definizioni di identità ONTAP locali**

A un livello elevato, è possibile definire ambiti indipendenti definiti nel server di autorizzazione o fare affidamento sulle definizioni di identità ONTAP locali esistenti, inclusi ruoli e utenti.

### **Opzioni con elaborazione ONTAP locale**

Se si utilizzano le definizioni di identità ONTAP, è necessario decidere quale applicare, tra cui:

- Ruolo REST denominato
- Far corrispondere gli utenti locali
- Active Directory o gruppi LDAP

### **Convalida locale o introspezione remota**

È necessario decidere se i token di accesso verranno convalidati localmente da ONTAP o dal server di autorizzazione tramite introspezione. Ci sono anche diversi valori correlati da prendere in considerazione, come l'intervallo di aggiornamento.

### **Token di accesso con restrizioni del mittente**

Per gli ambienti che richiedono un alto livello di protezione, è possibile utilizzare token di accesso con limitazioni di invio basati su mTLS. Questo richiede un certificato per ciascun client.

### **Interfaccia amministrativa**

È possibile eseguire l'amministrazione di OAuth 2,0 tramite una qualsiasi delle interfacce ONTAP, tra cui:

- Interfaccia della riga di comando
- System Manager
- API REST

### **Modalità con cui i client richiedono i token di accesso**

Le applicazioni client devono richiedere i token di accesso direttamente dal server di autorizzazione. È necessario decidere in che modo eseguire questa operazione, incluso il tipo di concessione.



## Configure ONTAP (Configura SNMP)

È necessario eseguire diverse attività di configurazione di ONTAP.

### Definire i ruoli REST e gli utenti locali

In base alla configurazione dell'autorizzazione, è possibile utilizzare l'elaborazione dell'identificazione ONTAP locale. In questo caso, è necessario rivedere e definire i ruoli REST e le definizioni utente.

### Configurazione di base

Per eseguire la configurazione di base di ONTAP sono necessari tre passaggi principali, tra cui:

- Se si desidera, installare il certificato di origine (e qualsiasi certificato intermedio) per la CA che ha firmato il certificato del server di autorizzazione.
- Definire il server di autorizzazione.
- Abilitare l'elaborazione OAuth 2,0 per il cluster.

## Implementa OAuth 2,0 in ONTAP

L'implementazione della funzionalità principale di OAuth 2,0 richiede tre fasi principali.

### Prima di iniziare

È necessario prepararsi per la distribuzione di OAuth 2,0 prima di configurare ONTAP. Ad esempio, è necessario valutare il server di autorizzazione, incluso il modo in cui il certificato è stato firmato e se è protetto da un firewall. Vedere ["Preparati a implementare OAuth 2,0 con ONTAP"](#) per ulteriori informazioni.

### Passaggio 1: Installazione del certificato del server di autenticazione

ONTAP include un gran numero di certificati CA principali preinstallati. Pertanto, in molti casi, il certificato per il server di autorizzazione verrà immediatamente riconosciuto da ONTAP senza ulteriori configurazioni. Tuttavia, a seconda di come è stato firmato il certificato del server di autorizzazione, potrebbe essere necessario installare un certificato della CA principale e qualsiasi certificato intermedio.

Seguire le istruzioni fornite di seguito per installare il certificato, se necessario. È necessario installare tutti i certificati richiesti a livello di cluster.

Scegliere la procedura corretta in base alla modalità di accesso a ONTAP.

## Esempio 17. Fasi

### System Manager

1. In System Manager, selezionare **Cluster > Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Fare clic su → accanto a **certificati**.
4. Nella scheda **autorità di certificazione attendibili** fare clic su **Aggiungi**.
5. Fare clic su **Importa** e selezionare il file del certificato.
6. Completare i parametri di configurazione dell'ambiente.
7. Fare clic su **Aggiungi**.

### CLI

1. Avviare l'installazione:

```
security certificate install -type server-ca
```

2. Cercare il seguente messaggio della console:

```
Please enter Certificate: Press <Enter> when done
```

3. Aprire il file del certificato con un editor di testo.
4. Copiare l'intero certificato, incluse le seguenti righe:

```
-----BEGIN CERTIFICATE-----  
  
-----END CERTIFICATE-----
```

5. Incollare il certificato nel terminale dopo il prompt dei comandi.
6. Premere **Invio** per completare l'installazione.
7. Verificare che il certificato sia installato utilizzando una delle seguenti opzioni:

```
security certificate show-user-installed  
  
security certificate show
```

## Passaggio 2: Configurare il server di autorizzazione

È necessario definire almeno un server di autorizzazione per ONTAP. È necessario scegliere i valori dei parametri in base alla configurazione e al piano di distribuzione. Revisione ["OAuth2 scenari di distribuzione"](#) per determinare i parametri esatti necessari per la configurazione.



Per modificare la definizione di un server di autorizzazione, è possibile eliminare la definizione esistente e crearne una nuova.

L'esempio fornito di seguito si basa sul primo semplice scenario di distribuzione all'indirizzo ["Convalida locale"](#). Gli oscilloscopi autonomi vengono utilizzati senza proxy.

Scegliere la procedura corretta in base alla modalità di accesso a ONTAP. La procedura CLI utilizza variabili

simboliche che è necessario sostituire prima di eseguire il comando.

## Esempio 18. Fasi

### System Manager

1. In System Manager, selezionare **Cluster > Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Fare clic su **+** accanto a **autorizzazione OAuth 2,0**.
4. Selezionare **altre opzioni**.
5. Fornire i valori richiesti per la distribuzione, ad esempio:
  - Nome
  - Applicazione (http)
  - Provider JWKS URI
  - URI emittente
6. Fare clic su **Aggiungi**.

### CLI

1. Creare nuovamente la definizione:

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri  
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

Ad esempio:

```
security oauth2 client create \  
-config-name auth0 \  
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-  
realm/protocol/openid-connect/certs \  
-application http \  
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

### Fase 3: Abilitare OAuth 2,0

Il passaggio finale consiste nell'abilitare OAuth 2,0. Si tratta di un'impostazione globale per il cluster ONTAP.



Non attivare l'elaborazione OAuth 2,0 finché non si conferma che ONTAP, i server di autorizzazione e gli eventuali servizi di supporto sono stati configurati correttamente.

Scegliere la procedura corretta in base alla modalità di accesso a ONTAP.

## Esempio 19. Fasi

### System Manager

1. In System Manager, selezionare **Cluster > Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Fare clic su → accanto a **autorizzazione OAuth 2,0**.
4. Abilita **autorizzazione OAuth 2,0**.

### CLI

1. Abilita OAuth 2,0:

```
security oauth2 modify -enabled true
```

2. Confermare che OAuth 2,0 sia abilitato:

```
security oauth2 show  
Is OAuth 2.0 Enabled: true
```

## Eseguire una chiamata API REST utilizzando OAuth 2,0

L'implementazione di OAuth 2,0 in ONTAP supporta le applicazioni client API REST. È possibile eseguire una semplice chiamata API REST utilizzando curl per iniziare a utilizzare OAuth 2,0. L'esempio presentato di seguito recupera la versione del cluster ONTAP.

### Prima di iniziare

È necessario configurare e abilitare la funzione OAuth 2,0 per il cluster ONTAP. Ciò include la definizione di un server di autorizzazione.

### Fase 1: Acquisire un token di accesso

È necessario acquisire un token di accesso da utilizzare con la chiamata API REST. La richiesta token viene eseguita al di fuori di ONTAP e la procedura esatta dipende dal server di autorizzazione e dalla relativa configurazione. È possibile richiedere il token tramite un browser Web, con un comando curl o utilizzando un linguaggio di programmazione.

A scopo illustrativo, di seguito viene presentato un esempio di come un token di accesso può essere richiesto da Keycloak usando curl.

## Esempio Keycloak

```
curl --request POST \  
--location  
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-  
connect/token' \  
--header 'Content-Type: application/x-www-form-urlencoded' \  
--data-urlencode 'client_id=dp-client-1' \  
--data-urlencode 'grant_type=client_credentials' \  
--data-urlencode 'client_secret=5iTUf9QKLGxAoYaliR33v1D5A2xq09V7'
```

Copiare e salvare il token restituito.

### Passaggio 2: Eseguire la chiamata API REST

Dopo avere un token di accesso valido, è possibile utilizzare un comando curl con il token di accesso per eseguire una chiamata API REST.

#### Parametri e variabili

Le due variabili nell'esempio dell'arricciatura sono descritte nella tabella seguente.

Variabile	Descrizione
\$FQDN_IP	Il nome di dominio o l'indirizzo IP pienamente qualificato della LIF di gestione ONTAP.
\$ACCESS_TOKEN	Token di accesso OAuth 2,0 emesso dal server di autorizzazione.

Prima di eseguire l'esempio Curl, è necessario impostare queste variabili nell'ambiente della shell Bash. Ad esempio, nella CLI di Linux digitare il seguente comando per impostare e visualizzare la variabile FQDN:

```
FQDN_IP=172.14.31.224  
echo $FQDN_IP  
172.14.31.224
```

Dopo aver definito entrambe le variabili nella shell Bash locale, è possibile copiare il comando curl e incollarlo nella CLI. Premere **Invio** per sostituire le variabili ed eseguire il comando.

### Esempio di arricciamento

```
curl --request GET \  
--location "https://$FQDN_IP/api/cluster?fields=version" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Bearer $ACCESS_TOKEN"
```

# Configurare l'autenticazione SAML

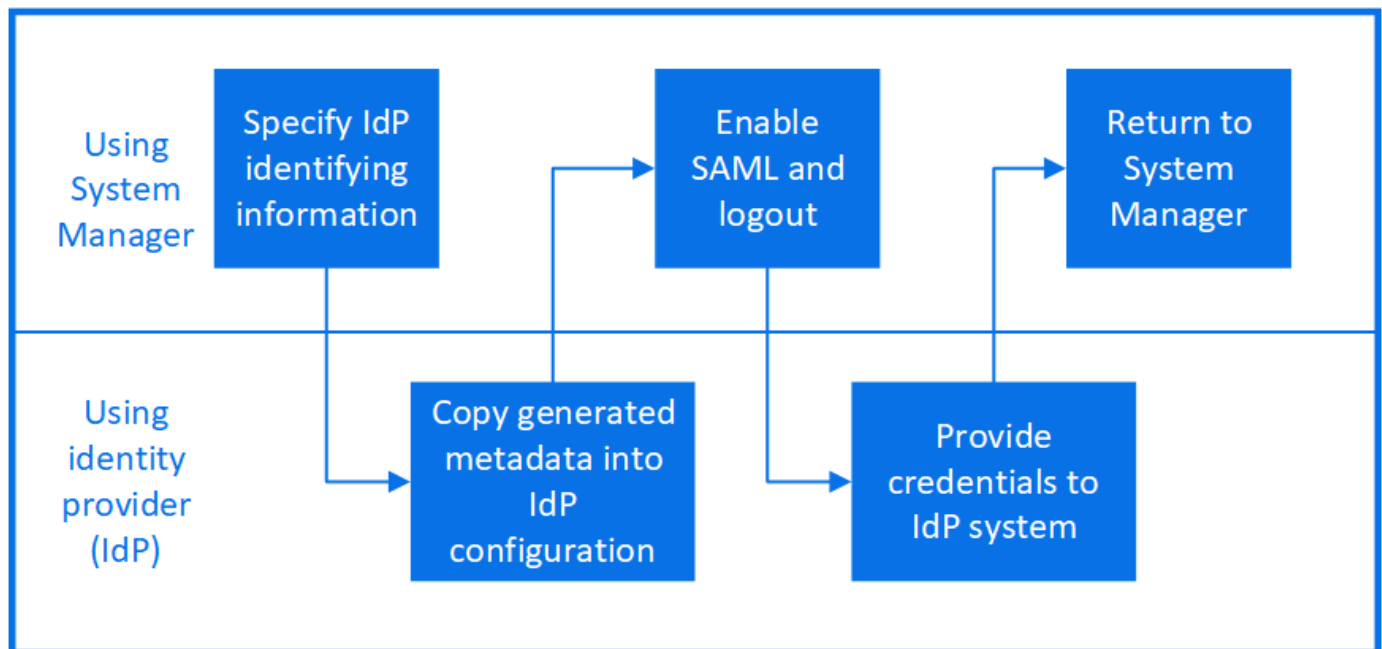
A partire da ONTAP 9.3, è possibile configurare l'autenticazione SAML (Security Assertion Markup Language) per i servizi Web. Quando l'autenticazione SAML è configurata e abilitata, gli utenti vengono autenticati da un provider di identità esterno (IdP) invece che dai provider di servizi di directory come Active Directory e LDAP.

## Abilitare l'autenticazione SAML

Per attivare l'autenticazione SAML con System Manager o con la CLI, attenersi alla seguente procedura. Se il cluster esegue ONTAP 9,7 o versione precedente, la procedura indicata è diversa da quella illustrata in System Manager. Fare riferimento alla guida in linea di System Manager disponibile sul sistema.



Dopo aver attivato l'autenticazione SAML, solo gli utenti remoti possono accedere alla GUI di System Manager. Gli utenti locali non possono accedere alla GUI di System Manager dopo l'attivazione dell'autenticazione SAML.



### Prima di iniziare

- È necessario configurare l'IdP che si intende utilizzare per l'autenticazione remota.



Consultare la documentazione fornita dall'IdP configurato.

- È necessario disporre dell'URI dell'IdP.

### A proposito di questa attività

- L'autenticazione SAML si applica solo a `http e. ontapi` applicazioni.

Il `http e. ontapi` Le applicazioni vengono utilizzate dai seguenti servizi Web: Infrastruttura del processore di servizi, API ONTAP o Gestore di sistema.

- L'autenticazione SAML è applicabile solo per l'accesso alla SVM amministrativa.


I seguenti IDP sono stati convalidati con System Manager:

- Servizi di federazione di Active Directory
- Cisco DUO (compatibile con le seguenti versioni di ONTAP:)
  - 9.7P21 e versioni successive 9,7 (fare riferimento a. ["Documentazione di System Manager Classic"](#))
  - 9.8P17 e versioni successive 9,8
  - 9,9.1P13 e versioni successive 9,9
  - 9.10.1P9 e versioni successive 9,10
  - 9.11.1P4 e versioni successive 9,11
  - 9.12.1 e versioni successive
- Shibboleth

A seconda dell'ambiente in uso, effettuare le seguenti operazioni:

## Esempio 20. Fasi

### System Manager

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Accanto a **SAML Authentication**, fare clic su .
3. Verificare che la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML) sia selezionata.
4. Inserire l'URL dell'URI IdP (incluso "[- 5. Modificare l'indirizzo del sistema host, se necessario.
- 6. Assicurarsi di utilizzare il certificato corretto:
  - Se il sistema è stato mappato con un solo certificato di tipo "server", il certificato viene considerato predefinito e non viene visualizzato.
  - Se il sistema è stato mappato con più certificati come tipo "server", viene visualizzato uno dei certificati. Per selezionare un certificato diverso, fare clic su \*\*Cambia\*\*.
- 7. Fare clic su \*\*Save\*\* \(Salva\). Una finestra di conferma visualizza le informazioni sui metadati, che sono state copiate automaticamente negli Appunti.
- 8. Accedere al sistema IdP specificato e copiare i metadati dagli Appunti per aggiornare i metadati del sistema.
- 9. Tornare alla finestra di conferma \(in System Manager\) e selezionare la casella di controllo \*\*ho configurato IdP con l'URI host o i metadati\*\*.
- 10. Fare clic su \*\*Logout\*\* per attivare l'autenticazione basata su SAML. Il sistema IdP visualizza una schermata di autenticazione.
- 11. Nel sistema IdP, immettere le credenziali basate su SAML. Una volta verificate le credenziali, viene visualizzata la home page di System Manager.](https://\)

### CLI

1. Creare una configurazione SAML in modo che ONTAP possa accedere ai metadati IdP:

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` È l'indirizzo FTP o HTTP dell'host IdP da cui è possibile scaricare i metadati IdP.

`ontap_host_name` È il nome host o l'indirizzo IP dell'host del provider di servizi SAML, che in questo caso è il sistema ONTAP. Per impostazione predefinita, viene utilizzato l'indirizzo IP della LIF di gestione del cluster.

È possibile fornire le informazioni sul certificato del server ONTAP. Per impostazione predefinita, vengono utilizzate le informazioni del certificato del server Web ONTAP.



```
cluster_12::> security saml-sp create -idp-uri  
https://example.url.net/idp/shibboleth
```

Warning: This restarts the web server. Any HTTP/S connections that are active

will be disrupted.

Do you want to continue? {y|n}: y

[Job 179] Job succeeded: Access the SAML SP metadata using the URL:  
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

Viene visualizzato l'URL per accedere ai metadati dell'host ONTAP.

2. Dall'host IdP, configurare IdP con i metadati dell'host ONTAP.

Per ulteriori informazioni sulla configurazione di IdP, consultare la documentazione di IdP.

3. Abilitare la configurazione SAML:

```
security saml-sp modify -is-enabled true
```

Qualsiasi utente esistente che accede a `http` oppure `ontapi` L'applicazione viene configurata automaticamente per l'autenticazione SAML.

4. Se si desidera creare utenti per `http` oppure `ontapi` Applicazione dopo aver configurato SAML, specificare SAML come metodo di autenticazione per i nuovi utenti.

- a. Creare un metodo di accesso per i nuovi utenti con autenticazione SAML:

```
security login create -user-or-group-name user_name -application [http |  
ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1  
-application http -authentication-method saml -vserver  
cluster_12
```

- b. Verificare che la voce utente sia stata creata:

```
security login show
```

```
cluster_12::> security login show
```

```
Vserver: cluster_12
```

```
Second
```

User/Group	Authentication		Acct
Authentication			
Name	Application	Method	Role Name
Method			Locked
-----	-----	-----	-----
admin	console	password	admin
none			
admin	http	password	admin
none			
admin	http	saml	admin
none			-
admin	ontapi	password	admin
none			
admin	ontapi	saml	admin
none			-
admin	service-processor		
		password	admin
none			
admin	ssh	password	admin
none			
admin1	http	password	backup
none			
**admin1	http	saml	backup
none**			-


## Disattiva l'autenticazione SAML

È possibile disattivare l'autenticazione SAML quando si desidera interrompere l'autenticazione degli utenti Web utilizzando un provider di identità (IdP) esterno. Quando l'autenticazione SAML è disattivata, i provider di servizi di directory configurati come Active Directory e LDAP vengono utilizzati per l'autenticazione.

A seconda dell'ambiente in uso, effettuare le seguenti operazioni:

## Esempio 21. Fasi

### System Manager

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. In **SAML Authentication**, fare clic sul pulsante di commutazione **Enabled**.
3. *Opzionale:* È anche possibile fare clic su  Accanto a **SAML Authentication**, quindi deselezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).

### CLI

1. Disattiva autenticazione SAML:

```
security saml-sp modify -is-enabled false
```

2. Se non si desidera più utilizzare l'autenticazione SAML o se si desidera modificare IdP, eliminare la configurazione SAML:

```
security saml-sp delete
```

## Risolvere i problemi relativi alla configurazione SAML

Se la configurazione dell'autenticazione SAML (Security Assertion Markup Language) non riesce, è possibile riparare manualmente ogni nodo su cui la configurazione SAML ha avuto esito negativo e ripristinarlo in caso di errore. Durante il processo di riparazione, il server Web viene riavviato e tutte le connessioni HTTP o HTTPS attive vengono interrompute.

### A proposito di questa attività

Quando si configura l'autenticazione SAML, ONTAP applica la configurazione SAML per nodo. Quando si attiva l'autenticazione SAML, ONTAP tenta automaticamente di riparare ogni nodo in caso di problemi di configurazione. In caso di problemi con la configurazione SAML su qualsiasi nodo, è possibile disattivare l'autenticazione SAML e riattivarla. Possono verificarsi situazioni in cui la configurazione SAML non viene applicata a uno o più nodi anche dopo aver riattivato l'autenticazione SAML. È possibile identificare il nodo su cui si è verificato un errore nella configurazione SAML e quindi riparare manualmente tale nodo.

### Fasi

1. Accedere al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Identificare il nodo su cui la configurazione SAML non ha avuto esito positivo:

```
security saml-sp status show -instance
```

```
cluster_12::*> security saml-sp status show -instance

Node: node1
Update Status: config-success
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 179

Node: node2
Update Status: config-failed
Database Epoch: 9
Database Transaction Count: 997
Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
ID of SAML Config Job: 180
2 entries were displayed.
```

### 3. Riparare la configurazione SAML sul nodo guasto:

**security saml-sp repair -node *node\_name***

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
    will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

Il server Web viene riavviato e tutte le connessioni HTTP o HTTPS attive vengono interrompute.

### 4. Verificare che SAML sia configurato correttamente su tutti i nodi:

**security saml-sp status show -instance**

```
cluster_12::*> security saml-sp status show -instance
```

```

                Node: node1
            Update Status: config-success
        Database Epoch: 9
    Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                Node: node2
            Update Status: **config-success**
        Database Epoch: 9
    Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

## Gestire i servizi Web

### Panoramica sulla gestione dei servizi Web

È possibile attivare o disattivare un servizio Web per il cluster o una macchina virtuale di storage (SVM), visualizzare le impostazioni per i servizi Web e controllare se gli utenti di un ruolo possono accedere a un servizio Web.

È possibile gestire i servizi Web per il cluster o una SVM nei seguenti modi:

- Attivazione o disattivazione di un servizio Web specifico
- Specifica se l'accesso a un servizio Web è limitato solo a HTTP (SSL) crittografato
- Visualizzazione della disponibilità dei servizi Web
- Consentire o negare agli utenti di un ruolo di accedere a un servizio Web
- Visualizzazione dei ruoli autorizzati ad accedere a un servizio Web

Affinché un utente possa accedere a un servizio Web, devono essere soddisfatte tutte le seguenti condizioni:

- L'utente deve essere autenticato.

Ad esempio, un servizio Web potrebbe richiedere un nome utente e una password. La risposta dell'utente deve corrispondere a un account valido.

- L'utente deve essere configurato con il metodo di accesso corretto.

L'autenticazione ha successo solo per gli utenti con il metodo di accesso corretto per il servizio Web specificato. Per il servizio Web API di ONTAP (`ontapi`), gli utenti devono disporre di `ontapi` metodo di accesso. Per tutti gli altri servizi Web, gli utenti devono disporre di `http` metodo di accesso.



Si utilizza `security login` comandi per gestire i metodi di accesso e di autenticazione degli utenti.

- Il servizio Web deve essere configurato in modo da consentire il ruolo di controllo degli accessi dell'utente.



Si utilizza `vserver services web access` comandi per controllare l'accesso di un ruolo a un servizio web.

Se un firewall è attivato, il criterio firewall per l'utilizzo della LIF per i servizi Web deve essere impostato in modo da consentire HTTP o HTTPS.

Se si utilizza HTTPS per l'accesso al servizio Web, è necessario attivare anche SSL per il cluster o SVM che offre il servizio Web e fornire un certificato digitale per il cluster o SVM.

## Gestire l'accesso ai servizi Web

Un servizio Web è un'applicazione a cui gli utenti possono accedere utilizzando HTTP o HTTPS. L'amministratore del cluster può configurare il motore del protocollo Web, configurare SSL, abilitare un servizio Web e consentire agli utenti di un ruolo di accedere a un servizio Web.

A partire da ONTAP 9.6, sono supportati i seguenti servizi Web:

- Infrastruttura del Service Processor (`spi`)

Questo servizio rende disponibili i file di log, core dump e MIB di un nodo per l'accesso HTTP o HTTPS attraverso la LIF di gestione del cluster o una LIF di gestione dei nodi. L'impostazione predefinita è `enabled`.

Su richiesta di accesso ai file di log o ai file core dump di un nodo, il `spi` il servizio web crea automaticamente un punto di montaggio da un nodo al volume root di un altro nodo in cui risiedono i file. Non è necessario creare manualmente il punto di montaggio. `

- API ONTAP (`ontapi`)

Questo servizio consente di eseguire API ONTAP per eseguire funzioni amministrative con un programma remoto. L'impostazione predefinita è `enabled`.

Questo servizio potrebbe essere richiesto per alcuni strumenti di gestione esterni. Ad esempio, se si utilizza System Manager, lasciare attivato questo servizio.

- Rilevamento Data ONTAP (`disco`)

Questo servizio consente alle applicazioni di gestione off-box di rilevare il cluster nella rete. L'impostazione predefinita è `enabled`.

- Diagnostica di supporto (`supdiag`)

Questo servizio controlla l'accesso a un ambiente privilegiato sul sistema per facilitare l'analisi e la risoluzione dei problemi. L'impostazione predefinita è `disabled`. Attivare questo servizio solo se richiesto dal supporto tecnico.

- System Manager (`sysmgr`)

Questo servizio controlla la disponibilità di Gestore di sistema, incluso in ONTAP. L'impostazione predefinita è `enabled`. Questo servizio è supportato solo sul cluster.

- Aggiornamento del firmware Baseboard Management Controller (BMC) (`FW_BMC`)

Questo servizio consente di scaricare i file del firmware BMC. L'impostazione predefinita è `enabled`.

- Documentazione ONTAP (`docs`)

Questo servizio consente di accedere alla documentazione di ONTAP. L'impostazione predefinita è `enabled`.

- API RESTful di ONTAP (`docs_api`)

Questo servizio fornisce l'accesso alla documentazione dell'API RESTful di ONTAP. L'impostazione predefinita è `enabled`.

- Caricamento e download del file (`fud`)

Questo servizio offre il caricamento e il download dei file. L'impostazione predefinita è `enabled`.

- Messaggi ONTAP (`ontapmsg`)

Questo servizio supporta un'interfaccia di pubblicazione e sottoscrizione che consente di iscriversi agli eventi. L'impostazione predefinita è `enabled`.

- Portale ONTAP (`portal`)

Questo servizio implementa il gateway in un server virtuale. L'impostazione predefinita è `enabled`.

- Interfaccia RESTful di ONTAP (`rest`)

Questo servizio supporta un'interfaccia RESTful utilizzata per gestire in remoto tutti gli elementi dell'infrastruttura cluster. L'impostazione predefinita è `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

Questo servizio fornisce risorse per supportare il provider di servizi SAML. L'impostazione predefinita è `enabled`.

- Provider di servizi SAML (`saml-sp`)

Questo servizio offre servizi come i metadati SP e il servizio di asserzione per i clienti al provider di servizi. L'impostazione predefinita è `enabled`.

A partire da ONTAP 9.7, sono supportati i seguenti servizi aggiuntivi:

- File di backup della configurazione (backups)

Questo servizio consente di scaricare i file di backup della configurazione. L'impostazione predefinita è `enabled`.

- Sicurezza ONTAP (security)

Questo servizio supporta la gestione dei token CSRF per un'autenticazione avanzata. L'impostazione predefinita è `enabled`.

## Gestire il motore dei protocolli Web

È possibile configurare il motore dei protocolli Web sul cluster per controllare se l'accesso Web è consentito e quali versioni SSL possono essere utilizzate. È inoltre possibile visualizzare le impostazioni di configurazione del motore dei protocolli Web.

È possibile gestire il motore dei protocolli Web a livello di cluster nei seguenti modi:

- È possibile specificare se i client remoti possono utilizzare HTTP o HTTPS per accedere al contenuto del servizio Web utilizzando `system services web modify` con il `-external` parametro.
- È possibile specificare se utilizzare SSLv3 per un accesso web sicuro utilizzando `security config modify` con il `-supported-protocol` parametro. Per impostazione predefinita, SSLv3 è disattivato. Transport Layer Security 1.0 (TLSv1.0) è attivato e può essere disattivato se necessario.
- È possibile attivare la modalità di conformità FIPS (Federal Information Processing Standard) 140-2 per le interfacce dei servizi Web del piano di controllo a livello di cluster.



Per impostazione predefinita, la modalità di conformità FIPS 140-2 è disattivata.

- **Quando la modalità di compliance FIPS 140-2 è disattivata**, è possibile attivare la modalità di compliance FIPS 140-2 impostando `is-fips-enabled` parametro a `true` per `security config modify` e quindi utilizzando il comando `security config show` per confermare lo stato online.
- **Quando è attivata la modalità di conformità FIPS 140-2**
  - A partire da ONTAP 9.11.1, TLSv1, TLSv1.1 e SSLv3 sono disattivati e solo TLSv1.2 e TLSv1.3 rimangono attivati. Riguarda altri sistemi e comunicazioni interni ed esterni a ONTAP 9. Se si attiva la modalità di conformità FIPS 140-2 e successivamente si disattiva, TLSv1, TLSv1.1 e SSLv3 rimangono disattivati. TLSv1 o TLSv1.3 resteranno abilitati a seconda della configurazione precedente.
  - Per le versioni di ONTAP precedenti alla 9.11.1, TLSv1 e SSLv3 sono disattivati e solo TLSv1.1 e TLSv1.2 rimangono attivati. ONTAP impedisce di abilitare sia TLSv1 che SSLv3 quando è attivata la modalità di conformità FIPS 140-2. Se si attiva la modalità di conformità FIPS 140-2 e successivamente la si disattiva, TLSv1 e SSLv3 rimangono disattivati, ma TLSv1.2 o TLSv1.1 e TLSv1.2 vengono attivati a seconda della configurazione precedente.
- È possibile visualizzare la configurazione della sicurezza a livello di cluster utilizzando `system security config show` comando.

Se il firewall è attivato, il criterio firewall per l'interfaccia logica (LIF) da utilizzare per i servizi Web deve essere impostato in modo da consentire l'accesso HTTP o HTTPS.



Se si utilizza HTTPS per l'accesso al servizio Web, è necessario attivare anche SSL per il cluster o la macchina virtuale di storage (SVM) che offre il servizio Web e fornire un certificato digitale per il cluster o la SVM.

Nelle configurazioni MetroCluster, le modifiche apportate alle impostazioni per il motore del protocollo Web su un cluster non vengono replicate sul cluster partner.

## Comandi per la gestione del motore dei protocolli web

Si utilizza `system services web` comandi per gestire il motore dei protocolli web. Si utilizza `system services firewall policy create` e `network interface modify` comandi per consentire alle richieste di accesso web di passare attraverso il firewall.

Se si desidera...	Utilizzare questo comando...
Configurare il motore del protocollo Web a livello di cluster: <ul style="list-style-type: none"><li>• Attivare o disattivare il motore dei protocolli Web per il cluster</li><li>• Attivare o disattivare SSLv3 per il cluster</li><li>• Attivazione o disattivazione della conformità FIPS 140-2 per servizi Web sicuri (HTTPS)</li></ul>	<code>system services web modify</code>
Visualizzare la configurazione del motore dei protocolli Web a livello di cluster, determinare se i protocolli Web sono funzionanti in tutto il cluster e visualizzare se la conformità FIPS 140-2 è attivata e online	<code>system services web show</code>
Visualizzare la configurazione del motore dei protocolli Web a livello di nodo e l'attività di gestione dei servizi Web per i nodi nel cluster	<code>system services web node show</code>
Creare una policy firewall o aggiungere il servizio del protocollo HTTP o HTTPS a una policy firewall esistente per consentire alle richieste di accesso Web di passare attraverso il firewall	<code>system services firewall policy create</code> Impostazione di <code>-service</code> parametro a <code>http</code> oppure <code>https</code> consente alle richieste di accesso web di passare attraverso il firewall.
Associare una policy firewall a una LIF	<code>network interface modify</code>  È possibile utilizzare <code>-firewall-policy</code> Parametro per modificare la policy firewall di una LIF.

## Configurare l'accesso ai servizi Web

La configurazione dell'accesso ai servizi Web consente agli utenti autorizzati di utilizzare

HTTP o HTTPS per accedere al contenuto del servizio sul cluster o su una macchina virtuale di storage (SVM).

## Fasi

1. Se è attivato un firewall, assicurarsi che l'accesso HTTP o HTTPS sia impostato nel criterio del firewall per la LIF che verrà utilizzata per i servizi Web:



È possibile verificare se un firewall è attivato utilizzando `system services firewall show` comando.

- a. Per verificare che HTTP o HTTPS sia impostato nel criterio firewall, utilizzare `system services firewall policy show` comando.

Impostare `-service` del parametro `system services firewall policy create` comando a `http` oppure `https` per consentire al criterio di supportare l'accesso web.

- b. Per verificare che il criterio firewall che supporta HTTP o HTTPS sia associato al LIF che fornisce servizi Web, utilizzare `network interface show` con il `-firewall-policy` parametro.

Si utilizza `network interface modify` con il `-firewall-policy` Parametro per attivare la policy firewall per una LIF.

2. Per configurare il motore del protocollo Web a livello di cluster e rendere accessibile il contenuto del servizio Web, utilizzare `system services web modify` comando.
3. Se si prevede di utilizzare servizi web sicuri (HTTPS), abilitare SSL e fornire informazioni sul certificato digitale per il cluster o SVM utilizzando `security ssl modify` comando.
4. Per attivare un servizio Web per il cluster o SVM, utilizzare `vserver services web modify` comando.

Ripetere questo passaggio per ogni servizio che si desidera attivare per il cluster o SVM.

5. Per autorizzare un ruolo ad accedere ai servizi Web sul cluster o SVM, utilizzare `vserver services web access create` comando.

Il ruolo a cui si concede l'accesso deve già esistere. È possibile visualizzare i ruoli esistenti utilizzando `security login role show` o creare nuovi ruoli utilizzando `security login role create` comando.

6. Per un ruolo autorizzato ad accedere a un servizio Web, verificare che anche i relativi utenti siano configurati con il metodo di accesso corretto controllando l'output di `security login show` comando.

Per accedere al servizio Web API di ONTAP (`ontapi`), un utente deve essere configurato con `ontapi` metodo di accesso. Per accedere a tutti gli altri servizi Web, è necessario configurare un utente con `http` metodo di accesso.



Si utilizza `security login create` per aggiungere un metodo di accesso per un utente.

## Comandi per la gestione dei servizi Web

Si utilizza `vserver services web` Comandi per gestire la disponibilità dei servizi Web

per il cluster o una macchina virtuale di storage (SVM). Si utilizza `vserver services web access` comandi per controllare l'accesso di un ruolo a un servizio web.

Se si desidera...	Utilizzare questo comando...
Configurare un servizio Web per il cluster o anSVM: <ul style="list-style-type: none"><li>• Attivare o disattivare un servizio Web</li><li>• Specificare se è possibile utilizzare solo HTTPS per accedere a un servizio Web</li></ul>	<code>vserver services web modify</code>
Visualizzare la configurazione e la disponibilità dei servizi Web per il cluster o anSVM	<code>vserver services web show</code>
Autorizzare un ruolo ad accedere a un servizio Web sul cluster o su una SVM	<code>vserver services web access create</code>
Visualizzare i ruoli autorizzati ad accedere ai servizi Web sul cluster o su una SVM	<code>vserver services web access show</code>
Impedire a un ruolo di accedere a un servizio Web sul cluster o su una SVM	<code>vserver services web access delete</code>

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

## Comandi per la gestione dei punti di montaggio sui nodi

Il `spi` il servizio web crea automaticamente un punto di montaggio da un nodo al volume root di un altro nodo su richiesta di accesso ai file di log o ai file core del nodo. Sebbene non sia necessario gestire manualmente i punti di montaggio, è possibile farlo utilizzando `system node root-mount` comandi.

Se si desidera...	Utilizzare questo comando...
Creare manualmente un punto di montaggio da un nodo al volume root di un altro nodo	<code>system node root-mount create</code> Può esistere un solo punto di montaggio da un nodo all'altro.
Visualizzare i punti di montaggio esistenti sui nodi del cluster, incluso l'ora in cui è stato creato un punto di montaggio e il relativo stato corrente	<code>system node root-mount show</code>
Eliminare un punto di montaggio da un nodo al volume root di un altro nodo e forzare la chiusura delle connessioni al punto di montaggio	<code>system node root-mount delete</code>

#### Informazioni correlate

## Gestire SSL

Il protocollo SSL migliora la sicurezza dell'accesso web utilizzando un certificato digitale per stabilire una connessione crittografata tra un server web e un browser.

È possibile gestire SSL per il cluster o una macchina virtuale di storage (SVM) nei seguenti modi:

- Abilitazione di SSL
- Generazione e installazione di un certificato digitale e associazione con il cluster o SVM
- Visualizzazione della configurazione SSL per verificare se SSL è stato attivato e, se disponibile, il nome del certificato SSL
- Impostazione di policy firewall per il cluster o SVM, in modo che le richieste di accesso Web possano essere inoltrate
- Definizione delle versioni SSL utilizzabili
- Limitazione dell'accesso solo alle richieste HTTPS per un servizio Web

## Comandi per la gestione di SSL




Si utilizza `security ssl` Comandi per gestire il protocollo SSL per la cluster ora storage virtual machine (SVM).

Se si desidera...	Utilizzare questo comando...
Abilitare SSL per il cluster oranSVM e associare un certificato digitale	<code>security ssl modify</code>
Visualizzare la configurazione SSL e il nome del certificato per il cluster oranSVM	<code>security ssl show</code>


## Risolvere i problemi di accesso al servizio Web

Gli errori di configurazione causano problemi di accesso al servizio Web. È possibile risolvere gli errori assicurandosi che LIF, policy firewall, motore del protocollo web, servizi web, certificati digitali, e l'autorizzazione all'accesso dell'utente sono tutte configurate correttamente.

La seguente tabella consente di identificare e risolvere gli errori di configurazione del servizio Web:

Questo problema di accesso...	Si verifica a causa di questo errore di configurazione...	Per risolvere l'errore...
Il browser Web restituisce un <code>unable to connect</code> oppure <code>failure to establish a connection</code> errore quando si tenta di accedere a un servizio web.	La LIF potrebbe non essere configurata correttamente.	Assicurarsi di poter eseguire il ping della LIF che fornisce il servizio Web.  <div>  <p>Si utilizza <code>network ping</code> Comando per eseguire il ping di una LIF. Per informazioni sulla configurazione di rete, consultare la <i>Guida alla gestione di rete</i>.</p> </div>
Il firewall potrebbe non essere configurato correttamente.	Assicurarsi che un criterio firewall sia impostato per supportare HTTP o HTTPS e che il criterio sia assegnato alla LIF che fornisce il servizio Web.  <div>  <p>Si utilizza <code>system services firewall policy</code> comandi per gestire le policy firewall. Si utilizza <code>network interface modify</code> con il <code>-firewall -policy</code> Parametro per associare un criterio a un LIF.</p> </div>	Il motore del protocollo Web potrebbe essere disattivato.
Assicurarsi che il motore dei protocolli Web sia abilitato in modo da poter accedere ai servizi Web.  <div>  <p>Si utilizza <code>system services web</code> comandi per gestire il motore del protocollo web per il cluster.</p> </div>	Il browser Web restituisce un <code>not found</code> errore quando si tenta di accedere a un servizio web.	Il servizio Web potrebbe essere disattivato.

Questo problema di accesso...	Si verifica a causa di questo errore di configurazione...	Per risolvere l'errore...
<p>Assicurarsi che ogni servizio Web a cui si desidera consentire l'accesso sia attivato singolarmente.</p> <div data-bbox="167 396 220 451">  </div> <p>Si utilizza <code>vserver services web modify</code> per abilitare un servizio web per l'accesso.</p>	<p>Il browser Web non riesce ad accedere a un servizio Web con il nome account e la password dell'utente.</p>	<p>L'utente non può essere autenticato, il metodo di accesso non è corretto o non è autorizzato ad accedere al servizio Web.</p>
<p>Assicurarsi che l'account utente esista e sia configurato con il metodo di accesso e di autenticazione corretti. Inoltre, assicurarsi che il ruolo dell'utente sia autorizzato ad accedere al servizio Web.</p> <div data-bbox="167 1190 220 1245">  </div> <p>Si utilizza <code>security login</code> comandi per gestire gli account utente, i relativi metodi di accesso e i metodi di autenticazione. L'accesso al servizio Web API di ONTAP richiede <code>ontapi</code> metodo di accesso. L'accesso a tutti gli altri servizi Web richiede <code>http</code> metodo di accesso. Si utilizza <code>vserver services web access</code> comandi per gestire l'accesso di un ruolo a un servizio web.</p>	<p>Si effettua la connessione al servizio Web con HTTPS e il browser Web indica che la connessione è stata interrotta.</p>	<p>È possibile che SSL non sia abilitato sul cluster o sulla SVM (Storage Virtual Machine) che fornisce il servizio Web.</p>

Questo problema di accesso...	Si verifica a causa di questo errore di configurazione...	Per risolvere l'errore...
<p>Assicurarsi che il cluster o la SVM abbia abilitato SSL e che il certificato digitale sia valido.</p> <div>  <p>Si utilizza <code>security ssl</code> Comandi per gestire la configurazione SSL per i server HTTP e il <code>security certificate show</code> per visualizzare le informazioni del certificato digitale.</p> </div>	<p>La connessione al servizio Web viene stabilita con HTTPS e il browser Web indica che la connessione non è attendibile.</p>	<p>È possibile che si stia utilizzando un certificato digitale autofirmato.</p>

## Verificare l'identità dei server remoti utilizzando i certificati

### Verificare l'identità dei server remoti utilizzando la panoramica dei certificati

ONTAP supporta le funzionalità dei certificati di sicurezza per verificare l'identità dei server remoti.

Il software ONTAP consente connessioni sicure utilizzando le seguenti funzionalità e protocolli di certificazione digitale:

- Il protocollo OCSP (Online Certificate Status Protocol) convalida lo stato delle richieste di certificati digitali dai servizi ONTAP utilizzando connessioni SSL e TLS (Transport Layer Security). Questa funzione è disattivata per impostazione predefinita.
- Il software ONTAP include un set predefinito di certificati root attendibili.
- I certificati KMIP (Key Management Interoperability Protocol) consentono l'autenticazione reciproca di un cluster e di un server KMIP.

### Verificare che i certificati digitali siano validi utilizzando OCSP

A partire da ONTAP 9.2, il protocollo OCSP (Online Certificate Status Protocol) consente alle applicazioni ONTAP che utilizzano le comunicazioni TLS (Transport Layer Security) di ricevere lo stato del certificato digitale quando OCSP è attivato. È possibile attivare o disattivare i controlli dello stato dei certificati OCSP per applicazioni specifiche in qualsiasi momento. Per impostazione predefinita, il controllo dello stato del certificato OCSP è disattivato.

#### Di cosa hai bisogno

Per eseguire questa attività, è necessario disporre di un accesso avanzato a livello di privilegi.

#### A proposito di questa attività

OCSP supporta le seguenti applicazioni:

- AutoSupport
- Sistema di gestione degli eventi (EMS)
- LDAP su TLS
- Protocollo KMIP (Key Management Interoperability Protocol)
- Registrazione dell'audit
- FabricPool
- SSH (a partire da ONTAP 9.13.1)

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`.
2. Per attivare o disattivare i controlli dello stato dei certificati OCSP per applicazioni ONTAP specifiche, utilizzare il comando appropriato.

Se si desidera che lo stato del certificato OCSP verifichi che alcune applicazioni siano...	Utilizzare il comando...
Attivato	<code>security config ocsp enable -app app name</code>
Disattivato	<code>security config ocsp disable -app app name</code>

Il seguente comando abilita il supporto OCSP per AutoSupport e EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Quando OCSP è attivato, l'applicazione riceve una delle seguenti risposte:

- Buono - il certificato è valido e la comunicazione procede.
  - Revocato - il certificato viene considerato permanentemente come non attendibile dall'autorità di certificazione di emissione e la comunicazione non riesce.
  - Sconosciuto - il server non dispone di informazioni sullo stato del certificato e la comunicazione non riesce.
  - Le informazioni del server OCSP non sono presenti nel certificato - il server agisce come se OCSP sia disattivato e continui con la comunicazione TLS, ma non si verifica alcun controllo dello stato.
  - Nessuna risposta dal server OCSP - l'applicazione non riesce a procedere.
3. Per attivare o disattivare i controlli dello stato dei certificati OCSP per tutte le applicazioni che utilizzano le comunicazioni TLS, utilizzare il comando appropriato.



Se si desidera che lo stato del certificato OCSP verifichi che tutte le applicazioni siano...	Utilizzare il comando...
Attivato	security config ocsd enable  -app all
Disattivato	security config ocsd disable  -app all

Quando questa opzione è attivata, tutte le applicazioni ricevono una risposta firmata che indica che il certificato specificato è valido, revocato o sconosciuto. In caso di certificato revocato, l'applicazione non potrà procedere. Se l'applicazione non riesce a ricevere una risposta dal server OCSP o se il server non è raggiungibile, l'applicazione non potrà procedere.

4. Utilizzare `security config ocsd show` Per visualizzare tutte le applicazioni che supportano OCSP e il relativo stato di supporto.

```
cluster::*> security config ocsd show
Application                                OCSP Enabled?
-----
autosupport                                false
audit_log                                  false
fabricpool                                 false
ems                                         false
kmip                                        false
ldap_ad                                    true
ldap_nis_namemap                           true
ssh                                         true

8 entries were displayed.
```

## Visualizza i certificati predefiniti per le applicazioni basate su TLS

A partire da ONTAP 9.2, ONTAP fornisce un set predefinito di certificati root attendibili per le applicazioni ONTAP che utilizzano TLS (Transport Layer Security).

### Di cosa hai bisogno

I certificati predefiniti vengono installati solo sulla SVM amministrativa durante la creazione o durante un aggiornamento a ONTAP 9.2.

### A proposito di questa attività

Le applicazioni correnti che agiscono come client e richiedono la convalida dei certificati sono AutoSupport, EMS, LDAP, registrazione degli audit, FabricPool, E KMIP.

Quando i certificati scadono, viene richiamato un messaggio EMS che richiede all'utente di eliminarli. I

certificati predefiniti possono essere eliminati solo al livello di privilegio avanzato.



L'eliminazione dei certificati predefiniti potrebbe causare il mancato funzionamento di alcune applicazioni ONTAP (ad esempio, AutoSupport e registrazione audit).

## Fase

1. È possibile visualizzare i certificati predefiniti installati sulla SVM amministrativa utilizzando il comando `show` del certificato di protezione:

**`security certificate show -vserver -type server-ca`**

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
                01                AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
    Expiration Date: Sun Dec 31 18:59:59 2028
```

# Autenticare reciprocamente il cluster e un server KMIP

## Autenticazione reciproca del cluster e panoramica di un server KMIP

L'autenticazione reciproca del cluster e di un gestore di chiavi esterno, ad esempio un server KMIP (Key Management Interoperability Protocol), consente al gestore di chiavi di comunicare con il cluster utilizzando KMIP su SSL. Ciò avviene quando un'applicazione o una determinata funzionalità (ad esempio, la funzionalità Storage Encryption) richiede chiavi sicure per fornire un accesso sicuro ai dati.

## Generare una richiesta di firma del certificato per il cluster

È possibile utilizzare il certificato di protezione `generate-csr` Comando per generare una richiesta di firma del certificato (CSR). Una volta elaborata la richiesta, l'autorità di certificazione (CA) invia il certificato digitale firmato.

### Di cosa hai bisogno

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

1. Generare una CSR:

**`security certificate generate-csr -common-name FQDN_or_common_name -size 512|1024|1536|2048 -country country -state state -locality locality`**

```
-organization organization -unit unit -email-addr email_of_contact -hash  
-function SHA1|SHA256|MD5
```

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando crea una CSR con una chiave privata a 2,048 bit generata dalla funzione di hashing SHA256 per l'utilizzo da parte del gruppo Software nel reparto IT di una società il cui nome comune personalizzato è server1.companyname.com, con sede a Sunnyvale, California, USA. L'indirizzo e-mail dell'amministratore del contatto SVM è [web@example.com](mailto:web@example.com). Il sistema visualizza la CSR e la chiave privata nell'output.

```
cluster1::>security certificate generate-csr -common-name  
server1.companyname.com -size 2048 -country US -state California -  
locality Sunnyvale -organization IT -unit Software -email-addr  
web@example.com -hash-function SHA256  
Certificate Signing Request :  
-----BEGIN CERTIFICATE REQUEST-----  
MIIBGjCBxQIBADBgMRQWEgYDVQQDEwtleGFtcGxlLmNvbTELMakGA1UEBhMCVVMx  
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G  
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApt1nzS  
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi  
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO  
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==  
-----END CERTIFICATE REQUEST-----  
Private Key :  
24 | Administrator Authentication and RBAC  
-----BEGIN RSA PRIVATE KEY-----  
MIIBOwIBAAJBAPXFanNoJApt1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb  
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu  
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM  
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu  
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NctEYxd0Q5  
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA  
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==  
-----END RSA PRIVATE KEY-----  
Note: Please keep a copy of your certificate request and private key  
for future reference.
```

2. Copiare la richiesta di certificato dall'output CSR, quindi inviarla in formato elettronico (ad esempio tramite e-mail) a una CA di terze parti attendibile per la firma.

Una volta elaborata la richiesta, la CA invia il certificato digitale firmato. Conservare una copia della chiave privata e del certificato digitale firmato dalla CA.

## Installare un certificato server firmato dalla CA per il cluster

Per consentire a un server SSL di autenticare la macchina virtuale del cluster o dello

storage (SVM) come client SSL, installare un certificato digitale con il tipo di client sul cluster o SVM. Quindi, fornire il certificato client-ca all'amministratore del server SSL per l'installazione sul server.

### Di cosa hai bisogno

È necessario aver già installato il certificato root del server SSL sul cluster o SVM con `server-ca` tipo di certificato.

### Fasi

1. Per utilizzare un certificato digitale autofirmato per l'autenticazione del client, utilizzare `security certificate create` con il `type client` parametro.
2. Per utilizzare un certificato digitale con firma CA per l'autenticazione del client, attenersi alla seguente procedura:
  - a. Generare una richiesta di firma del certificato digitale (CSR) utilizzando il certificato di sicurezza `generate-csr` comando.  
  
ONTAP visualizza l'output CSR, che include una richiesta di certificato e una chiave privata, e ricorda di copiare l'output in un file per riferimenti futuri.
  - b. Inviare la richiesta di certificato dall'output CSR in un formato elettronico (ad esempio un'e-mail) a una CA attendibile per la firma.

Conservare una copia della chiave privata e del certificato firmato dalla CA per riferimenti futuri.

Una volta elaborata la richiesta, la CA invia il certificato digitale firmato.

- a. Installare il certificato firmato dalla CA utilizzando `security certificate install` con il `-type client` parametro.
- b. Quando richiesto, immettere il certificato e la chiave privata, quindi premere **Invio**.
- c. Quando richiesto, immettere eventuali certificati root o intermedi aggiuntivi, quindi premere **Invio**.

Se una catena di certificati che inizia dalla CA principale attendibile e termina con il certificato SSL emesso, non dispone dei certificati intermedi, è necessario installare un certificato intermedio sul cluster o sulla SVM. Un certificato intermedio è un certificato subordinato emesso dalla radice attendibile in modo specifico per il rilascio di certificati server di entità finale. Il risultato è una catena di certificati che inizia dalla CA principale attendibile, passa attraverso il certificato intermedio e termina con il certificato SSL emesso.

3. Fornire il `client-ca` Certificato del cluster o SVM all'amministratore del server SSL per l'installazione sul server.

Il comando `show` del certificato di protezione con `-instance e. -type client-ca parameters` (parametri): visualizza `client-ca` informazioni sul certificato.

## Installare un certificato client firmato dalla CA per il server KMIP

Il sottotipo di certificato del protocollo KMIP (Key Management Interoperability Protocol) (il parametro `-subtype kmip-cert`), insieme ai tipi `client` e `server-ca`, specifica che il certificato viene utilizzato per l'autenticazione reciproca del cluster e di un gestore di

chiavi esterno, ad esempio un server KMIP.

### A proposito di questa attività

Installare un certificato KMIP per autenticare un server KMIP come server SSL nel cluster.

### Fasi

1. Utilizzare `security certificate install` con il `-type server-ca` e `-subtype kmip-cert` Parametri per installare un certificato KMIP per il server KMIP.
2. Quando richiesto, immettere il certificato, quindi premere Invio.

ONTAP ricorda di conservare una copia del certificato per riferimenti futuri.

```
cluster1::> security certificate install -type server-ca -subtype kmip-  
cert  
-vserver cluster1
```

```
Please enter Certificate: Press <Enter> when done
```

```
-----BEGIN CERTIFICATE-----
```

```
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG  
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ  
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscx1IaU5rfGW/D/xwzoiQ
```

```
...
```

```
-----END CERTIFICATE-----
```

```
You should keep a copy of the CA-signed digital certificate for future  
reference.
```

```
cluster1::>
```

# Sicurezza e crittografia dei dati

## Panoramica sulla gestione della sicurezza con System Manager

A partire da ONTAP 9.7, è possibile gestire la sicurezza del cluster con Gestione di sistema.

Con Gestione sistema, si utilizzano i metodi standard di ONTAP per proteggere l'accesso client e amministratore allo storage e per proteggerlo dai virus. Sono disponibili tecnologie avanzate per la crittografia dei dati a riposo e per lo storage WORM.

Se si utilizza la gestione di sistema classica (disponibile solo in ONTAP 9.7 e versioni precedenti), fare riferimento a ["System Manager Classic \(ONTAP da 9.0 a 9.7\)"](#)

### Scansione virus

È possibile utilizzare la funzionalità antivirus integrata nel sistema di storage per proteggere i dati da virus o altri codici dannosi. La scansione antivirus di ONTAP, denominata *Vscan*, combina il software antivirus di terze parti più all'avanguardia con le funzionalità di ONTAP che offrono la flessibilità necessaria per controllare quali file vengono sottoposti a scansione e quando.

### Crittografia

ONTAP offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

### Storage WORM

*SnapLock* è una soluzione per la compliance dalle performance elevate per le organizzazioni che utilizzano lo storage *write once, Read Many (WORM)* per conservare i file critici in forma non modificata per scopi normativi e di governance.

## Protegersi dal ransomware

### Panoramica della protezione ransomware autonoma

A partire da ONTAP 9.10.1, la funzionalità di protezione ransomware autonoma (ARP) utilizza l'analisi del carico di lavoro in ambienti NAS (NFS e SMB) per rilevare e avvisare in modo proattivo circa attività anomale che potrebbero indicare un attacco ransomware.

Quando si sospetta un attacco, ARP crea anche nuove copie Snapshot, oltre alla protezione esistente dalle copie Snapshot pianificate.

### Licenze e abilitazione

ARP richiede una licenza. ARP è disponibile con ["Licenza ONTAP ONE"](#). Se non si dispone della licenza ONTAP ONE, sono disponibili altre licenze per l'utilizzo di ARP, che variano a seconda della versione di ONTAP in uso.

Release di ONTAP	Licenza
ONTAP 9.11.1 e versioni successive	Anti_ransomware
ONTAP 9.10.1	MT_EK_MGMT (Gestione delle chiavi multi-tenant)

- Se si esegue l'aggiornamento a ONTAP 9.11.1 o versione successiva e ARP è già configurato nel sistema, non è necessario acquistare la nuova licenza Anti-ransomware. Per le nuove configurazioni ARP, è necessaria la nuova licenza.
- Se si esegue il ripristino da ONTAP 9.11.1 o versione successiva a ONTAP 9.10.1 e si attiva ARP con la licenza Anti-ransomware, viene visualizzato un messaggio di avviso e potrebbe essere necessario riconfigurare ARP. ["Scopri come ripristinare ARP"](#).

È possibile configurare ARP per volume utilizzando Gestione sistema o l'interfaccia CLI di ONTAP.

## Strategia di protezione ransomware di ONTAP

Una strategia efficace di rilevamento ransomware dovrebbe includere più di un singolo livello di protezione.

Un'analogia sarebbe la sicurezza di un veicolo. Non ci si affida a una singola funzione, ad esempio una cintura di sicurezza, per proteggersi completamente in caso di incidente. Gli airbag, i freni antibloccaggio e l'allarme anticollisione anteriore sono tutte funzioni di sicurezza aggiuntive che consentono di ottenere risultati migliori. La protezione ransomware deve essere visualizzata nello stesso modo.

Mentre ONTAP include funzionalità come FPolicy, Snapshot Copies, SnapLock e Active IQ Digital Advisor per la protezione dal ransomware, le seguenti informazioni si concentrano sulla funzionalità ARP on-box con funzionalità di machine learning.

Per ulteriori informazioni sulle altre funzionalità anti-ransomware di ONTAP, consulta la sezione ["TR-4572: Soluzione NetApp per ransomware."](#)

## Cosa rileva ARP

ARP è progettato per proteggere da attacchi di tipo Denial-of-service in cui l'utente malintenzionato trattiene i dati fino a quando non viene pagato un riscatto. ARP offre il rilevamento anti-ransomware basato su:

- Identificazione dei dati in entrata come crittografati o non crittografati.
- Analytics, che rileva
  - **Entropia:** Una valutazione della casualità dei dati in un file
  - **Tipi di estensione del file:** Un'estensione non conforme al normale tipo di estensione
  - **IOPS del file:** Aumento dell'attività anomala del volume con crittografia dei dati (a partire da ONTAP 9.11.1)

ARP è in grado di rilevare la diffusione della maggior parte degli attacchi ransomware dopo la crittografia di un numero limitato di file, intraprendere azioni automatiche per proteggere i dati e avvisare l'utente che si sta verificando un attacco sospetto.



Nessun sistema di rilevamento ransomware o prevenzione può garantire completamente la sicurezza da un attacco ransomware. Anche se è possibile che un attacco possa non essere rilevato, ARP agisce come un importante livello di difesa aggiuntivo se il software antivirus non è riuscito a rilevare un'intrusione.

## Modalità di apprendimento e attive

ARP dispone di due modalità:

- **Apprendimento** (o modalità "dry run")
- **Attivo** (o modalità "abilitato")

Quando si attiva ARP, viene eseguito in *modalità di apprendimento*. In modalità di apprendimento, il sistema ONTAP sviluppa un profilo di avviso basato sulle aree di analisi: Entropia, tipi di estensione dei file e IOPS dei file. Dopo aver eseguito ARP in modalità di apprendimento per un tempo sufficiente a valutare le caratteristiche del carico di lavoro, è possibile passare alla modalità attiva e iniziare a proteggere i dati. Una volta che ARP è passato alla modalità attiva, ONTAP crea copie snapshot ARP per proteggere i dati se viene rilevata una minaccia.

Si consiglia di lasciare ARP in modalità di apprendimento per 30 giorni. A partire da ONTAP 9.13.1, ARP determina automaticamente l'intervallo ottimale del periodo di apprendimento e automatizza lo switch, che può verificarsi prima di 30 giorni.

In modalità attiva, se un'estensione del file è contrassegnata come anomala, è necessario valutare l'avviso. Puoi agire sull'avviso per proteggere i tuoi dati o contrassegnarlo come falso positivo. Se si contrassegna un avviso come falso positivo, il profilo di avviso viene aggiornato. Ad esempio, se l'avviso viene attivato da una nuova estensione di file e l'utente contrassegna l'avviso come falso positivo, non verrà visualizzato alcun avviso alla successiva visualizzazione dell'estensione del file. Il comando `security anti-ransomware volume workload-behavior show` mostra le estensioni di file rilevate nel volume. (Se si esegue questo comando nelle prime fasi della modalità di apprendimento e viene visualizzata una rappresentazione accurata dei tipi di file, non utilizzare tali dati come base per passare alla modalità attiva, poiché ONTAP sta ancora raccogliendo altre metriche).

A partire da ONTAP 9.11.1, è possibile personalizzare i parametri di rilevamento per ARP. Per ulteriori informazioni, vedere [Gestire i parametri di rilevamento degli attacchi ARP](#).

## Valutazione delle minacce e copie snapshot ARP

In modalità attiva, ARP valuta la probabilità di minaccia in base ai dati in entrata misurati in base alle analisi apprese. Viene assegnata una misurazione quando ARP rileva una minaccia:

- **Basso:** Il primo rilevamento di un'anomalia nel volume (ad esempio, una nuova estensione del file è osservata nel volume).
- **Moderato:** Si osservano più file con la stessa estensione mai vista prima.
  - In ONTAP 9.10.1, la soglia per l'escalation a moderata è di 100 o più file. A partire da ONTAP 9.11.1, è possibile modificare la quantità di file; il valore predefinito è 20.

In una situazione di basso rischio, ONTAP rileva un'anomalia e crea una copia Snapshot del volume per creare il punto di recovery migliore. ONTAP anticipa il nome della copia snapshot ARP con `Anti-ransomware-backup` per renderla facilmente identificabile, per esempio `Anti_ransomware_backup.2022-12-20_1248`.

Dopo che ONTAP ha eseguito un report di analytics, la minaccia passa a moderata. Ciò determina se l'anomalia corrisponde a un profilo ransomware. Le minacce che rimangono a basso livello sono registrate e visibili nella sezione **Eventi** di System Manager. Quando la probabilità di attacco è moderata, ONTAP genera una notifica EMS che richiede di valutare la minaccia. ONTAP non invia avvisi relativi a minacce basse, tuttavia, a partire da ONTAP 9.14.1, è possibile [modificare le impostazioni degli avvisi](#). Per ulteriori informazioni, vedere [Rispondere ad attività anomale](#).



È possibile visualizzare informazioni su una minaccia, indipendentemente dal livello, nella sezione **Eventi** di System Manager o con `security anti-ransomware volume show` comando.

Le copie Snapshot ARP vengono conservate per un minimo di due giorni. A partire da ONTAP 9.11.1, è possibile modificare le impostazioni di conservazione. Per ulteriori informazioni, vedere [Modificare le opzioni per le copie Snapshot](#).

### **Come ripristinare i dati in ONTAP dopo un attacco ransomware**

Quando si sospetta un attacco, il sistema esegue una copia Snapshot del volume in quel momento e blocca tale copia. Se l'attacco viene confermato in seguito, il volume può essere ripristinato utilizzando la copia snapshot ARP.

Le copie Snapshot bloccate non possono essere eliminate con mezzi normali. Tuttavia, se in seguito decidi di contrassegnare l'attacco come falso positivo, la copia bloccata verrà eliminata.

Conoscendo i file interessati e il momento dell'attacco, è possibile recuperare in modo selettivo i file interessati da varie copie Snapshot, piuttosto che semplicemente riportare l'intero volume in una delle copie Snapshot.

ARP si basa quindi sulla comprovata tecnologia di protezione dei dati e disaster recovery di ONTAP per rispondere agli attacchi ransomware. Per ulteriori informazioni sul ripristino dei dati, consultare i seguenti argomenti.

- ["Ripristino da copie Snapshot \(System Manager\)"](#)
- ["Ripristino dei file da copie Snapshot \(CLI\)"](#)
- ["Ripristino ransomware intelligente"](#)

### **Casi di utilizzo e considerazioni sulla protezione ransomware autonoma**

La protezione autonoma ransomware (ARP) è disponibile per i carichi di lavoro NAS a partire da ONTAP 9.10.1. Prima di distribuire ARP, è necessario conoscere gli utilizzi consigliati e le configurazioni supportate, nonché le implicazioni in termini di prestazioni.

#### **Configurazioni supportate e non supportate**

Quando si decide di utilizzare l'ARP, è importante assicurarsi che il carico di lavoro del volume sia adatto all'ARP e che soddisfi le configurazioni di sistema richieste.

#### **Carichi di lavoro adatti**

ARP è adatto per:

- Database sullo storage NFS
- Home directory Windows o Linux

Poiché gli utenti potrebbero creare file con estensioni che non sono state rilevate durante il periodo di apprendimento, esiste una maggiore possibilità di falsi positivi in questo carico di lavoro.

- Immagini e video

Ad esempio, le cartelle cliniche e i dati EDA (Electronic Design Automation)

## Carichi di lavoro non adatti

ARP non è adatto per:

- Carichi di lavoro con un'elevata frequenza di creazione o eliminazione di file (centinaia di migliaia di file in pochi secondi, ad esempio workload di test/sviluppo).
- Il rilevamento delle minacce di ARP dipende dalla sua capacità di riconoscere un aumento insolito delle attività di creazione, ridenominazione o eliminazione dei file. Se l'applicazione stessa è l'origine dell'attività del file, non è possibile distinguerla in modo efficace dall'attività ransomware.
- Carichi di lavoro in cui l'applicazione o l'host crittografa i dati.  
ARP dipende dalla distinzione dei dati in entrata come crittografati o non crittografati. Se l'applicazione stessa sta crittografando i dati, l'efficacia della funzione viene ridotta. Tuttavia, la funzionalità può ancora funzionare in base all'attività del file (eliminazione, sovrascrittura o creazione, creazione o ridenominazione con una nuova estensione del file) e al tipo di file.

## Configurazioni supportate

ARP è disponibile per i volumi NFS e SMB nei sistemi ONTAP on-premise a partire da ONTAP 9.10.1.

Il supporto per altre configurazioni e tipi di volume è disponibile nelle seguenti versioni di ONTAP:

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Volumi protetti con SnapMirror asincrono	✓	✓	✓		
SVM protette con SnapMirror asincrono (disaster recovery SVM)	✓	✓	✓		
Mobilità dei dati SVM (vserver migrate)	✓	✓	✓		
Volumi FlexGroup	✓	✓			
Verifica multi-admin	✓	✓			

## Interoperabilità di SnapMirror e ARP

A partire da ONTAP 9.12.1, ARP è supportato sui volumi di destinazione asincroni di SnapMirror. ARP è **non** supportato con SnapMirror Synchronous.

Se un volume di origine SnapMirror è abilitato per ARP, il volume di destinazione SnapMirror acquisisce automaticamente lo stato di configurazione ARP (apprendimento, abilitato, ecc.), i dati di training ARP e l'istantanea creata da ARP del volume di origine. Non è richiesta alcuna abilitazione esplicita.

Mentre il volume di destinazione è costituito da copie Snapshot di sola lettura (RO), non viene eseguita alcuna elaborazione ARP sui dati. Tuttavia, quando il volume di destinazione di SnapMirror viene convertito in lettura/scrittura (RW), ARP viene attivato automaticamente sul volume di destinazione convertito in RW. Il volume di destinazione non richiede ulteriori procedure di apprendimento oltre a quelle già registrate nel

volume di origine.

In ONTAP 9.10.1 e 9.11.1, SnapMirror non trasferisce lo stato di configurazione ARP, i dati di training e le copie Snapshot dai volumi di origine a quelli di destinazione. Quindi, quando il volume di destinazione SnapMirror viene convertito in RW, ARP sul volume di destinazione deve essere esplicitamente abilitato in modalità di apprendimento dopo la conversione.

## **ARP e macchine virtuali**

ARP è supportato con macchine virtuali (VM). Il rilevamento ARP si comporta in modo diverso per le modifiche all'interno e all'esterno della VM. L'ARP non è consigliato per i carichi di lavoro con file ad entropia elevata all'interno della VM.

### **Modifiche esterne alla macchina virtuale**

ARP può rilevare le modifiche all'estensione di un file su un volume NFS esterno alla VM se una nuova estensione entra nel volume crittografato o se cambia l'estensione di un file. Le modifiche all'estensione dei file rilevabili sono:

- vmx
- .vmxf
- .vmdk
- -flat.vmdk
- .nvram
- .vmem
- .vmsd
- .vmsn
- .vswp
- .vmss
- log
- -\#.log

### **Modifiche all'interno della VM**

Se l'attacco ransomware riguarda la macchina virtuale e i file all'interno della macchina virtuale vengono alterati senza apportare modifiche all'esterno della macchina virtuale, ARP rileva la minaccia se l'entropia predefinita della macchina virtuale è bassa (ad esempio file .txt, .docx o .mp4). Anche se ARP crea un'istantanea di protezione in questo scenario, non genera un avviso di minaccia perché le estensioni di file esterne alla VM non sono state manomesse.

Se, per impostazione predefinita, i file sono ad entropia elevata (ad esempio file .gzip o protetti da password), le funzionalità di rilevamento di ARP sono limitate. In questo caso, ARP può ancora acquisire istantanee proattive, tuttavia non verrà attivato alcun avviso se le estensioni dei file non sono state manomesse esternamente.

### **Configurazioni non supportate**

ARP non è supportato nelle seguenti configurazioni di sistema:

- Ambienti ONTAP S3
- Ambienti SAN

ARP non supporta le seguenti configurazioni di volume:

- Volumi FlexGroup (in ONTAP da 9.10.1 a 9.12.1. A partire da ONTAP 9.13.1, sono supportati i volumi FlexGroup)
- FlexCache Volumes (ARP supportato sui volumi FlexVol di origine ma non sui volumi cache)
- Volumi offline
- Volumi solo SAN
- Volumi SnapLock
- SnapMirror sincrono
- SnapMirror asincrono (non supportato solo in ONTAP 9.10.1 e 9.11.1. SnapMirror asincrono è supportato a partire da ONTAP 9.12.1. Per ulteriori informazioni, vedere [\[snapmirror\]](#).)
- Volumi limitati
- Volumi root di storage VM
- Volumi di VM storage interrotte

### Considerazioni sulle performance e sulla frequenza ARP

ARP può avere un impatto minimo sulle prestazioni del sistema, misurato in termini di throughput e IOPS di picco. L'impatto della funzionalità ARP dipende dai carichi di lavoro dei volumi specifici. Per i carichi di lavoro comuni, si consigliano i seguenti limiti di configurazione:

Caratteristiche del carico di lavoro	Limite di volume consigliato per nodo	Peggioramento delle performance con superamento del limite di volume per nodo:[*]
I dati possono essere compressi o a uso intensivo di lettura.	150	4% degli IOPS massimi
I dati non possono essere compressi con un utilizzo intensivo di scrittura.	60	10% degli IOPS massimi

Superato:[\*] le performance di sistema non vengono degradate oltre queste percentuali, indipendentemente dal numero di volumi aggiunti in eccesso rispetto ai limiti raccomandati.

Poiché gli analytics ARP vengono eseguiti in una sequenza con priorità, con l'aumentare del numero di volumi protetti, gli analytics vengono eseguiti su ciascun volume con minore frequenza.

### Verifica multi-admin con volumi protetti con ARP

A partire da ONTAP 9.13.1, è possibile attivare la verifica multi-admin (MAV) per una maggiore sicurezza con ARP. MAV garantisce che almeno due o più amministratori autenticati siano tenuti a disattivare ARP, sospendere ARP o contrassegnare un attacco sospetto come falso positivo su un volume protetto. Scopri come ["Abilitare MAV per volumi protetti da ARP"](#).

È necessario definire gli amministratori per un gruppo MAV e creare regole MAV per security anti-ransomware volume disable, security anti-ransomware volume pause, e security anti-ransomware volume attack clear-suspect Comandi ARP che si desidera proteggere. Ogni amministratore del gruppo MAV deve approvare ogni nuova richiesta di regola e ["Aggiungere nuovamente la regola MAV"](#) Nelle impostazioni MAV.

A partire da ONTAP 9.14.1, ARP offre avvisi per la creazione di un'istantanea ARP e per l'osservazione di una

nuova estensione di file. Gli avvisi per questi eventi sono disattivati per impostazione predefinita. Gli avvisi possono essere impostati a livello di volume o SVM. È possibile creare regole MAV a livello SVM utilizzando `security anti-ransomware vserver event-log modify` o al livello del volume con `security anti-ransomware volume event-log modify`.

### Passi successivi

- ["Attiva la protezione ransomware autonoma"](#)
- ["Abilita MAV per volumi protetti da ARP"](#)

## Attiva la protezione ransomware autonoma

A partire da ONTAP 9.10.1, è possibile attivare la protezione ransomware autonoma (ARP) su volumi nuovi o esistenti. Per prima cosa, si attiva ARP in modalità di apprendimento, in cui il sistema analizza il carico di lavoro per caratterizzare il comportamento normale. È possibile attivare ARP su un volume esistente oppure creare un nuovo volume e attivare ARP dall'inizio.

### A proposito di questa attività

Si dovrebbe sempre abilitare ARP inizialmente in modalità di apprendimento (o dry-run). L'avvio in modalità attiva può causare un numero eccessivo di falsi positivi.

Si consiglia di far funzionare ARP in modalità di apprendimento per un minimo di 30 giorni. A partire da ONTAP 9.13.1, ARP determina automaticamente l'intervallo ottimale del periodo di apprendimento e automatizza lo switch, che può verificarsi prima di 30 giorni. Per ulteriori informazioni, vedere ["Modalità di apprendimento e attive"](#).



Nei volumi esistenti, l'apprendimento e le modalità attive si applicano solo ai dati scritti di recente, non ai dati già esistenti nel volume. I dati esistenti non vengono sottoposti a scansione e analizzati, poiché le caratteristiche del traffico dati normale precedente vengono assunte in base ai nuovi dati dopo che il volume è stato abilitato per ARP.

### Prima di iniziare

- Devi avere una macchina virtuale per lo storage (SVM) abilitata per NFS o SMB (o entrambi).
- Il [licenza corretta](#) Deve essere installato per la versione di ONTAP in uso.
- È necessario disporre di un carico di lavoro NAS con i client configurati.
- Il volume che si desidera impostare ARP deve essere protetto e deve avere un attivo ["percorso di giunzione"](#).
- Il volume deve essere pieno al di sotto del 100%.
- Si consiglia di configurare il sistema EMS per l'invio di notifiche e-mail, che includano avvisi relativi all'attività ARP. Per ulteriori informazioni, vedere ["Configurare gli eventi EMS per l'invio di notifiche e-mail"](#).
- A partire da ONTAP 9.13.1, si consiglia di attivare la verifica multi-admin (MAV) in modo che siano necessari due o più amministratori utente autenticati per la configurazione ARP (Autonomous ransomware Protection). Per ulteriori informazioni, vedere ["Attiva la verifica multi-admin"](#).

## Enable ARP (attiva ARP)

È possibile attivare ARP utilizzando Gestione di sistema o l'interfaccia CLI di ONTAP.

## System Manager

### Fasi

1. Selezionare **Storage > Volumes** (archiviazione > volumi), quindi selezionare il volume che si desidera proteggere.
2. Nella scheda **Security** della panoramica **Volumes**, selezionare **Status** per passare da Disabled (Disattivato) a Enabled (attivato) in Learning-mode (modalità apprendimento) nella casella **Anti-ransomware**.
3. Al termine del periodo di apprendimento, impostare ARP in modalità attiva.



A partire da ONTAP 9.13.1, ARP determina automaticamente l'intervallo ottimale del periodo di apprendimento e automatizza lo switch. È possibile ["Disattivare questa impostazione sulla VM di storage associata"](#) se si desidera controllare manualmente la modalità di apprendimento in modalità attiva, passare alla modalità attiva.

- a. Selezionare **Storage > Volumes** (archiviazione > volumi), quindi selezionare il volume pronto per la modalità attiva.
  - b. Nella scheda **Security** della panoramica **Volumes**, selezionare **Switch** to Active mode nella casella Anti-ransomware.
4. È possibile verificare lo stato ARP del volume nella casella **Anti-ransomware**.

Per visualizzare lo stato ARP per tutti i volumi: Nel riquadro **Volumes** (volumi), selezionare **Show/Hide** (Mostra/Nascondi), quindi assicurarsi che sia selezionato lo stato **Anti-ransomware**.

### CLI

Il processo di abilitazione dell'ARP con la CLI differisce se lo si attiva su un volume esistente rispetto a un nuovo volume.

#### Attivare ARP su un volume esistente

1. Modificare un volume esistente per abilitare la protezione ransomware in modalità di apprendimento:

```
security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
```

Se si esegue ONTAP 9.13.1 o versione successiva, l'apprendimento adattivo viene attivato in modo che il passaggio allo stato attivo venga eseguito automaticamente. Se non si desidera che questo comportamento venga attivato automaticamente, modificare l'impostazione a livello di SVM su tutti i volumi associati:

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

2. Al termine del periodo di apprendimento, modificare il volume protetto per passare alla modalità attiva, se non è già stato eseguito automaticamente:

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

È anche possibile passare alla modalità attiva con il comando modify volume:

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
```

### 3. Verificare lo stato ARP del volume.

```
security anti-ransomware volume show
```

#### Abilitare ARP su un nuovo volume

#### 1. Creare un nuovo volume con la protezione anti-ransomware abilitata prima del provisioning dei dati.

```
volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size nn -anti-ransomware-state dry-run -junction-path /path_name
```

Se si esegue ONTAP 9.13.1 o versione successiva, l'apprendimento adattivo viene attivato in modo che il passaggio allo stato attivo venga eseguito automaticamente. Se non si desidera che questo comportamento venga attivato automaticamente, modificare l'impostazione a livello di SVM su tutti i volumi associati:

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

#### 2. Al termine del periodo di apprendimento, modificare il volume protetto per passare alla modalità attiva, se non è già stato eseguito automaticamente:

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

È anche possibile passare alla modalità attiva con il comando `modify volume`:

```
volume modify -volume vol_name -vserver svm_name -anti-ransomware-state active
```

#### 3. Verificare lo stato ARP del volume.

```
security anti-ransomware volume show
```

## Attiva la protezione ransomware autonoma per impostazione predefinita nei nuovi volumi

A partire da ONTAP 9.10.1, è possibile configurare le VM di storage in modo che i nuovi volumi siano attivati per impostazione predefinita per la protezione ransomware autonoma (ARP) in modalità di apprendimento.

### A proposito di questa attività

Per impostazione predefinita, i nuovi volumi vengono creati con ARP in modalità disattivata. È possibile modificare questa impostazione in System Manager e con l'interfaccia CLI. I volumi abilitati per impostazione predefinita sono impostati su ARP in modalità di apprendimento (o dry-run).

ARP viene attivato solo sui volumi creati in SVM dopo aver modificato l'impostazione. ARP non verrà abilitato sui volumi esistenti. Scopri come ["Abilitare ARP in un volume esistente"](#).

A partire da ONTAP 9.13.1, l'apprendimento adattivo è stato aggiunto agli analytics ARP e il passaggio dalla modalità di apprendimento alla modalità attiva viene eseguito automaticamente. Per ulteriori informazioni, vedere ["Modalità di apprendimento e attive"](#).

## Prima di iniziare

- Il [licenza corretta](#) Deve essere installato per la versione di ONTAP in uso.
- Il volume deve essere pieno al di sotto del 100%.
- I percorsi di giunzione devono essere attivi.
- A partire da ONTAP 9.13.1, si consiglia di attivare la verifica multi-admin (MAV) in modo che siano necessari due o più amministratori utente autenticati per le operazioni anti-ransomware. ["Scopri di più"](#).

## Passare dalla modalità di apprendimento alla modalità attiva

A partire da ONTAP 9.13.1, l'apprendimento adattivo è stato aggiunto all'analisi ARP. Il passaggio dalla modalità di apprendimento alla modalità attiva viene eseguito automaticamente. La decisione autonoma di ARP di passare automaticamente dalla modalità di apprendimento alla modalità attiva si basa sulle impostazioni di configurazione delle seguenti opzioni:

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent  
-anti-ransomware-auto-switch-duration-without-new-file-extension  
-anti-ransomware-auto-switch-minimum-learning-period  
-anti-ransomware-auto-switch-minimum-file-count  
-anti-ransomware-auto-switch-minimum-file-extension
```

Dopo 30 giorni di apprendimento, un volume passa automaticamente alla modalità attiva anche se una o più di queste condizioni non sono soddisfatte. In altre parole, se la funzione di commutazione automatica è attivata, il volume passa alla modalità attiva dopo un massimo di 30 giorni. Il valore massimo di 30 giorni è fisso e non modificabile.


Per ulteriori informazioni sulle opzioni di configurazione ARP, compresi i valori predefiniti, consultare la ["Riferimento al comando ONTAP"](#).

## Fasi

È possibile utilizzare Gestione di sistema o la CLI di ONTAP per attivare ARP per impostazione predefinita.



## System Manager

1. Selezionare **Storage > Storage VM** (Storage VM > Storage VM), quindi selezionare la VM di storage contenente i volumi che si desidera proteggere con ARP.
2. Selezionare la scheda **Impostazioni**. In **sicurezza**, individuare il riquadro **Anti-ransomware**, quindi selezionare 
3. Selezionare la casella per abilitare ARP per volumi NAS. Selezionare la casella aggiuntiva per abilitare ARP su tutti i volumi NAS idonei nella VM di storage.



Se è stato eseguito l'aggiornamento a ONTAP 9.13.1, l'impostazione **passa automaticamente dalla modalità di apprendimento alla modalità attiva dopo un apprendimento sufficiente** viene attivata automaticamente. Ciò consente ad ARP di determinare l'intervallo ottimale del periodo di apprendimento e di automatizzare il passaggio alla modalità attiva. Disattivare l'impostazione se si desidera passare manualmente alla modalità attiva.

## CLI

1. Modificare una SVM esistente per attivare ARP per impostazione predefinita nei nuovi volumi:  

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

Nella CLI, è anche possibile creare una nuova SVM con ARP attivato per impostazione predefinita per i nuovi volumi.

```
vserver create -vserver svm_name -anti-ransomware-default-volume-state dry-run [other parameters as needed]
```

Se è stato eseguito l'aggiornamento a ONTAP 9.13.1 o versioni successive, l'apprendimento adattivo viene attivato in modo che il passaggio allo stato attivo venga eseguito automaticamente. Se non si desidera attivare automaticamente questo comportamento, utilizzare il seguente comando:

```
vserver modify svm_name -anti-ransomware-auto-switch-from-learning-to-enabled false
```

## Sospendere la protezione ransomware autonoma per escludere gli eventi dei workload dall'analisi

Se si prevedono eventi insoliti relativi ai carichi di lavoro, è possibile sospendere temporaneamente e riprendere l'analisi ARP (Autonomous ransomware Protection) in qualsiasi momento.

A partire da ONTAP 9.13.1, è possibile attivare la verifica multi-admin (MAV) in modo che due o più amministratori utente autenticati siano necessari per mettere in pausa l'ARP. ["Scopri di più"](#).

### A proposito di questa attività

Durante una pausa ARP, non vengono registrati eventi né vengono eseguite azioni per nuove scritture. Tuttavia, l'operazione di analisi continua per i log precedenti in background.



Non utilizzare la funzione di disattivazione ARP per mettere in pausa gli analytics. In questo modo si disattiva l'ARP sul volume e tutte le informazioni esistenti sul comportamento dei carichi di lavoro appresi vengono perse. Ciò richiederebbe un riavvio del periodo di apprendimento.

**Fasi**

È possibile utilizzare Gestione di sistema o la CLI di ONTAP per sospendere ARP.

## System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi\*), quindi selezionare il volume in cui si desidera sospendere l'ARP.
2. Nella scheda **sicurezza** della panoramica dei volumi, seleziona **Pausa anti-ransomware** nella casella **Anti-ransomware**.



A partire da ONTAP 9.13.1, se si utilizza MAV per proteggere le impostazioni ARP, l'operazione di pausa richiede di ottenere l'approvazione di uno o più amministratori aggiuntivi. "L'approvazione deve essere ricevuta da tutti gli amministratori" Associato al gruppo di approvazione MAV o l'operazione non riuscirà.

## CLI

1. Pausa ARP su un volume:

```
security anti-ransomware volume pause -vserver svm_name -volume vol_name
```

2. Per riprendere l'elaborazione, utilizzare `resume` parametro.

```
security anti-ransomware volume resume -vserver svm_name -volume vol_name
```

3. **Se si utilizza MAV (disponibile con ARP che inizia con ONTAP 9.13.1) per proteggere le impostazioni ARP**, l'operazione di pausa richiede l'approvazione di uno o più amministratori aggiuntivi. L'approvazione deve essere ricevuta da tutti gli amministratori associati al gruppo di approvazione MAV, altrimenti l'operazione non avrà esito positivo.

Se si utilizza MAV e un'operazione di pausa prevista richiede ulteriori approvazioni, ciascun responsabile dell'approvazione del gruppo MAV esegue le seguenti operazioni:

- a. Mostra la richiesta:

```
security multi-admin-verify request show
```

- b. Approvare la richiesta:

```
security multi-admin-verify request approve -index[number returned from show request]
```

La risposta dell'ultimo responsabile dell'approvazione del gruppo indica che il volume è stato modificato e che lo stato di ARP è in pausa.

Se si utilizza MAV e si è un responsabile dell'approvazione del gruppo MAV, è possibile rifiutare una richiesta di operazione di pausa:

```
security multi-admin-verify request veto -index[number returned from show request]
```

## Gestire i parametri di rilevamento degli attacchi tramite protezione autonoma dal ransomware

A partire da ONTAP 9.11.1, puoi modificare i parametri per il rilevamento del ransomware su un volume abilitato alla protezione autonoma contro il ransomware specifico e segnalare un picco noto come normale attività dei file. La regolazione dei parametri di rilevamento consente di migliorare l'accuratezza dei rapporti in base al carico di lavoro del volume specifico.

### Come funziona il rilevamento degli attacchi

Quando la protezione autonoma da ransomware (ARP) è in modalità di apprendimento, sviluppa valori di base per i comportamenti di volume. Si tratta di entropia, estensioni dei file e, a partire da ONTAP 9.11.1, IOPS. Queste baseline vengono utilizzate per valutare le minacce ransomware. Per ulteriori informazioni su questi criteri, vedere [Cosa rileva ARP](#).

In ONTAP 9.10.1, ARP genera un avviso se rileva entrambe le seguenti condizioni:

- più di 20 file con estensioni non precedentemente osservate nel volume
- elevati dati di entropia

A partire da ONTAP 9.11.1, ARP emette un avviso di minaccia se *solo* viene soddisfatta una condizione. Ad esempio, se si osservano più di 20 file con estensioni che non sono state precedentemente osservate nel volume entro un periodo di 24 ore, ARP lo classificherà come una minaccia *indipendentemente* dall'entropia osservata. (I valori dei file 24 ore e 20 sono predefiniti, che possono essere modificati).

A partire da ONTAP 9.14.1, è possibile configurare gli avvisi quando ARP osserva una nuova estensione di file e quando ARP crea un'istantanea. Per ulteriori informazioni, vedere [\[modify-alerts\]](#)

Alcuni volumi e carichi di lavoro richiedono parametri di rilevamento diversi. Ad esempio, il volume abilitato per ARP può ospitare numerosi tipi di estensioni di file, nel qual caso è possibile modificare il conteggio delle soglie per le estensioni di file mai viste prima a un numero maggiore del valore predefinito di 20 o disattivare gli avvisi in base alle estensioni di file mai viste prima. A partire da ONTAP 9.11.1, puoi modificare i parametri di rilevamento degli attacchi per adattarli meglio ai tuoi carichi di lavoro specifici.

### Modificare i parametri di rilevamento degli attacchi

A seconda dei comportamenti previsti del volume abilitato per ARP, è possibile modificare i parametri di rilevamento degli attacchi.

#### Fasi

1. Visualizzare i parametri di rilevamento degli attacchi esistenti:

```
security anti-ransomware volume attack-detection-parameters show -vserver  
svm_name -volume volume_name
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume voll
```

```

Vserver Name : vs1
Volume Name : voll
Is Detection Based on High Entropy Data Rate? : true
Is Detection Based on Never Seen before File Extension? : true
Is Detection Based on File Create Rate? : true
Is Detection Based on File Rename Rate? : true
Is Detection Based on File Delete Rate? : true
Is Detection Relaxing Popular File Extensions? : true
High Entropy Data Surge Notify Percentage : 100
File Create Rate Surge Notify Percentage : 100
File Rename Rate Surge Notify Percentage : 100
File Delete Rate Surge Notify Percentage : 100
Never Seen before File Extensions Count Notify Threshold : 20
Never Seen before File Extensions Duration in Hour : 24
```

2. Tutti i campi visualizzati sono modificabili con valori booleani o interi. Per modificare un campo, utilizzare `security anti-ransomware volume attack-detection-parameters modify` comando.

Per un elenco completo dei parametri, vedere ["Riferimento al comando ONTAP"](#).

## Segnalare le sovratensioni note

ARP continua a modificare i valori di base per i parametri di rilevamento anche in modalità attiva. Se conoscete i picchi nella vostra attività di volume—o un aumento una volta o un aumento che è caratteristica di una nuova normale—dovreste segnalarlo come sicuro. La segnalazione manuale di questi picchi come sicuri aiuta a migliorare l'accuratezza delle valutazioni delle minacce di ARP.

## Segnalare un aumento di una tantum

1. Se in circostanze note si verifica un picco una tantum e si desidera che ARP segnali un aumento simile in circostanze future, eliminare il picco dal comportamento del carico di lavoro:

```
security anti-ransomware volume workload-behavior clear-surge -vserver
svm_name -volume volume_name
```

## Modificare il picco della linea di base

1. Se un picco segnalato deve essere considerato un normale comportamento dell'applicazione, riportare il picco in quanto tale per modificare il valore di picco della linea di base.

```
security anti-ransomware volume workload-behavior update-baseline-from-surge
-vserver svm_name -volume volume_name
```

## Configurare gli avvisi ARP

A partire da ONTAP 9.14.1, ARP consente di specificare gli avvisi per due eventi ARP:

- Osservazione della nuova estensione di un file su un volume

- Creazione di un'istantanea ARP

È possibile impostare avvisi per questi due eventi su singoli volumi o per l'intera SVM. Se abiliti gli avvisi per la SVM, le impostazioni degli avvisi vengono ereditate solo dai volumi creati in seguito all'attivazione della funzione di avviso. Per impostazione predefinita, gli avvisi non sono attivati su alcun volume.

Gli avvisi di eventi possono essere controllati con verifica multi-admin. Per ulteriori informazioni, vedere [Verifica multi-admin con volumi protetti con ARP](#).

## System Manager

### Impostare gli avvisi per un volume

1. Passare a **volumi**. Selezionare il singolo volume per il quale si desidera modificare le impostazioni.
2. Selezionare la scheda **sicurezza**, quindi **Impostazioni protezione eventi**.
3. Per ricevere avvisi relativi a **Nuova estensione rilevata e istantanea ransomware creata**, selezionare il menu a discesa sotto l'intestazione **gravità**. Modificare l'impostazione da **non generare evento** a **Avviso**.
4. Selezionare **Salva**.

### Impostare gli avvisi per una SVM

1. Accedere a **Storage VM** quindi selezionare la SVM per la quale si desidera abilitare le impostazioni.
2. Sotto l'intestazione **sicurezza**, individuare la scheda **Anti-ransomware**. Selezionare **⋮** Quindi **Modifica gravità evento ransomware**.
3. Per ricevere avvisi relativi a **Nuova estensione rilevata e istantanea ransomware creata**, selezionare il menu a discesa sotto l'intestazione **gravità**. Modificare l'impostazione da **non generare evento** a **Avviso**.
4. Selezionare **Salva**.

## CLI

### Impostare gli avvisi per un volume

- Per impostare gli avvisi per una nuova estensione file:

```
security anti-ransomware volume event-log modify -vserver svm_name -is  
-enabled-on-new-file-extension-seen true
```

- Per impostare gli avvisi per la creazione di un'istantanea ARP:

```
security anti-ransomware volume event-log modify -vserver svm_name -is  
-enabled-on-snapshot-copy-creation true
```

- Confermare le impostazioni con `anti-ransomware volume event-log show` comando.

### Impostare gli avvisi per una SVM

- Per impostare gli avvisi per una nuova estensione file:

```
security anti-ransomware vserver event-log modify -vserver svm_name -is  
-enabled-on-new-file-extension-seen true
```

- Per impostare gli avvisi per la creazione di un'istantanea ARP:

```
security anti-ransomware vserver event-log modify -vserver svm_name -is  
-enabled-on-snapshot-copy-creation true
```

- Confermare le impostazioni con `security anti-ransomware vserver event-log show` comando.

## Ulteriori informazioni

- ["Comprendere gli attacchi di protezione autonoma da ransomware e lo snapshot di protezione autonoma da ransomware"](#)

## Rispondere ad attività anomale

Quando la protezione ransomware autonoma (ARP) rileva attività anomale in un volume protetto, emette un avviso. È necessario valutare la notifica per determinare se l'attività è accettabile (falso positivo) o se un attacco sembra dannoso.

### A proposito di questa attività

ARP visualizza un elenco di file sospetti quando rileva una combinazione di elevata entropia dei dati, attività anomale del volume con crittografia dei dati e estensioni di file insolite.

Quando viene visualizzato l'avviso, è possibile rispondere contrassegnando l'attività del file in uno dei due modi seguenti:

- **Falso positivo**

Il tipo di file identificato è previsto nel carico di lavoro e può essere ignorato.

- **Potenziale attacco ransomware**

Il tipo di file identificato non è previsto nel carico di lavoro e deve essere trattato come un potenziale attacco.

In entrambi i casi, il normale monitoraggio riprende dopo l'aggiornamento e la cancellazione degli avvisi. ARP registra la valutazione nel profilo di valutazione delle minacce, utilizzando la scelta dell'utente per monitorare le attività successive dei file.

In caso di attacco sospetto, è necessario determinare se si tratta di un attacco, rispondere al caso in cui si tratti e ripristinare i dati protetti prima di cancellare le notifiche. ["Scopri di più su come eseguire il ripristino da un attacco ransomware"](#).



Se si ripristina un intero volume, non vi sono avvisi da cancellare.

### Prima di iniziare

ARP deve essere in esecuzione in modalità attiva.

### Fasi

È possibile utilizzare Gestione sistema o l'interfaccia CLI di ONTAP per rispondere a un'attività anomala.



## System Manager


1. Quando si riceve una notifica di "attività anomala", seguire il collegamento o passare alla scheda **sicurezza** della panoramica **volumi**.

Gli avvisi vengono visualizzati nel riquadro **Panoramica** del menu **Eventi**.

2. Quando viene visualizzato il messaggio "rilevata attività anomala del volume", visualizzare i file sospetti.

Nella scheda **protezione**, selezionare **Visualizza tipi di file sospetti**.

3. Nella finestra di dialogo **tipi di file sospetti**, esaminare ciascun tipo di file e contrassegnarlo come "falso positivo" o "potenziale attacco ransomware".

Se si seleziona questo valore...	Eseguire questa azione...
Falso positivo	<div><div>Selezionare <b>Aggiorna</b> e <b>Cancella tipi di file sospetti</b> per registrare la decisione e riprendere il normale monitoraggio ARP.</div><div><div>A partire da ONTAP 9.13.1, se si utilizza MAV per proteggere le impostazioni ARP, l'operazione che si sospetta venga richiesta l'approvazione di uno o più amministratori aggiuntivi. <a href="#">"L'approvazione deve essere ricevuta da tutti gli amministratori"</a> Associato al gruppo di approvazione MAV o l'operazione non riuscirà.</div></div></div>
Potenziale attacco ransomware	<div>Rispondere all'attacco e ripristinare i dati protetti. Quindi selezionare <b>Aggiorna</b> e <b>Cancella tipi di file sospetti</b> per registrare la decisione e riprendere il normale monitoraggio ARP.</div> <div>Non esistono tipi di file sospetti da eliminare se è stato ripristinato un intero volume.</div>

## CLI

1. Quando ricevi una notifica di un attacco ransomware sospetto, verifica l'ora e la gravità dell'attacco:

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

Output di esempio:

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

È inoltre possibile controllare i messaggi EMS:

```
event log show -message-name callhome.arw.activity.seen
```

2. Generare un report sugli attacchi e prendere nota della posizione di output:

```
security anti-ransomware volume attack generate-report -volume vol_name  
-dest-path file_location/
```

Output di esempio:

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path  
"vs0:vol1/"
```

3. Visualizzare il report su un sistema client di amministrazione. Ad esempio:

```
[root@rhel8 mnt]# cat report_file_vs0_vol1_14-09-2021_01-21-08  
  
19  "9/14/2021 01:03:23"    test_dir_1/test_file_1.jpg.lckd  
20  "9/14/2021 01:03:46"    test_dir_2/test_file_2.jpg.lckd  
21  "9/14/2021 01:03:46"    test_dir_3/test_file_3.png.lckd`
```

4. Eseguire una delle seguenti operazioni in base alla valutazione delle estensioni dei file:

◦ Falso positivo

Immettere il seguente comando per registrare la decisione, aggiungere il nuovo interno all'elenco di quelli consentiti e riprendere il normale monitoraggio anti-ransomware:

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume  
vol_name [extension identifiers] -false-positive true
```

Per identificare gli interni, utilizzare uno dei seguenti parametri:

`[-seq-no integer]` Numero di sequenza del file nell'elenco dei file sospetti.

`[-extension text, ... ]` Estensioni di file

`[-start-time date_time -end-time date_time]` Orari di inizio e fine dell'intervallo di file da cancellare, nel formato "MM/GG/AAAA HH:MM:SS".

◦ Potenziale attacco ransomware

Rispondere all'attacco e. ["Recuperare i dati dallo snapshot di backup creato da ARP"](#). Una volta ripristinati i dati, immettere il seguente comando per registrare la decisione e riprendere il normale monitoraggio ARP:

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume  
vol_name [extension identifiers] -false-positive false
```

Per identificare gli interni, utilizzare uno dei seguenti parametri:

`[-seq-no integer]` Numero di sequenza del file nell'elenco dei file sospetti

`[-extension text, ... ]` Estensione del file

`[-start-time date_time -end-time date_time]` Orari di inizio e fine dell'intervallo di file da cancellare, nel formato "MM/GG/AAAA HH:MM:SS".

Non esistono tipi di file sospetti da eliminare se è stato ripristinato un intero volume. Lo snapshot di backup creato da ARP verrà rimosso e il report dell'attacco verrà cancellato.

5. Se si sta utilizzando MAV e un previsto clear-suspect L'operazione richiede approvazioni aggiuntive, ogni responsabile dell'approvazione del gruppo MAV esegue le seguenti operazioni:

- a. Mostra la richiesta:

```
security multi-admin-verify request show
```

- b. Approvare la richiesta di riprendere il normale monitoraggio anti-ransomware:

```
security multi-admin-verify request approve -index[number returned from show request]
```

La risposta dell'ultimo responsabile dell'approvazione del gruppo indica che il volume è stato modificato e che viene registrato un falso positivo.

6. Se si utilizza MAV e si è un responsabile dell'approvazione del gruppo MAV, è anche possibile rifiutare una richiesta con un sospetto chiaro:

```
security multi-admin-verify request veto -index[number returned from show request]
```

#### Ulteriori informazioni

- ["KB: Comprendere gli attacchi di protezione ransomware autonoma e lo snapshot di protezione ransomware autonoma"](#).

## Ripristinare i dati dopo un attacco ransomware

La protezione autonoma dal ransomware (ARP) crea copie Snapshot denominate `Anti_ransomware_backup` quando rileva una potenziale minaccia ransomware. È possibile utilizzare una di queste copie snapshot ARP o un'altra copia Snapshot del volume per ripristinare i dati.

#### A proposito di questa attività

Se il volume presenta relazioni SnapMirror, replicare manualmente tutte le copie mirror del volume immediatamente dopo il ripristino da una copia Snapshot. In caso contrario, le copie mirror non possono essere utilizzabili e devono essere eliminate e ricreate.

Per eseguire il ripristino da uno Snapshot diverso da `Anti_ransomware_backup` Snapshot dopo aver identificato un attacco di sistema, è necessario prima rilasciare lo snapshot ARP.

Se non è stato segnalato alcun attacco al sistema, è necessario prima eseguire il ripristino da `Anti_ransomware_backup` La copia Snapshot, quindi, completa un successivo ripristino del volume dalla copia Snapshot scelta.

#### Fasi

Per ripristinare i dati, è possibile utilizzare Gestione di sistema o l'interfaccia utente di ONTAP.

## System Manager

### Ripristino dopo un attacco di sistema

1. Per eseguire il ripristino dall'istantanea ARP, passare direttamente al punto 2. Per eseguire il ripristino da una copia Snapshot precedente, è necessario prima rilasciare il blocco sull'istantanea ARP.
  - a. Selezionare **Storage > Volumes** (Storage > volumi).
  - b. Selezionare **sicurezza**, quindi **Visualizza tipi di file sospetti**
  - c. Contrassegnare i file come "False Positive" (Falso positivo).
  - d. Selezionare **Aggiorna e Cancella tipi di file sospetti**
2. Visualizzare le copie Snapshot nei volumi:


Selezionare **archiviazione > volumi**, quindi selezionare il volume e **Snapshot Copies**.

3. Selezionare  Accanto alla copia istantanea che si desidera ripristinare, quindi **Restore**.

### Ripristinare se non è stato identificato un attacco di sistema

1. Visualizzare le copie Snapshot nei volumi:

Selezionare **archiviazione > volumi**, quindi selezionare il volume e **Snapshot Copies**.

2. Selezionare  loro scelgono il `Anti_ransomware_backup` Istantanea.
3. Selezionare **Restore** (Ripristina).
4. Tornare al menu **Snapshot Copies**, quindi scegliere la copia istantanea che si desidera utilizzare. Selezionare **Restore** (Ripristina).

## CLI

### Ripristino dopo un attacco di sistema

1. Per eseguire il ripristino dalla copia snapshot ARP, passare direttamente al punto 2. Per ripristinare i dati da copie Snapshot precedenti, è necessario rilasciare il blocco sullo snapshot ARP.



È necessario rilasciare il SnapLock anti-ransomware solo prima di eseguire il ripristino dalle copie Snapshot precedenti, se si utilizza `volume snap restore` come descritto di seguito. Se si ripristinano i dati utilizzando Flex Clone, Single file Snap Restore o altri metodi, ciò non è necessario.

Contrassegnare l'attacco come "falso positivo" e "chiaro sospetto":

```
anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true
```

Per identificare gli interni, utilizzare uno dei seguenti parametri:

`[-seq-no integer]` Numero di sequenza del file nell'elenco dei file sospetti.

`[-extension text, ... ]` Estensioni di file

`[-start-time date_time -end-time date_time]` Orari di inizio e fine dell'intervallo di file da cancellare, nel formato "MM/GG/AAAA HH:MM:SS".

2. Elencare le copie Snapshot in un volume:

```
volume snapshot show -vserver SVM -volume volume
```

L'esempio seguente mostra le copie Snapshot in `vol11`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

### 3. Ripristinare il contenuto di un volume da una copia Snapshot:

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

Nell'esempio riportato di seguito viene ripristinato il contenuto di vol1:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010
```

## Ripristinare se non è stato identificato un attacco di sistema

### 1. Elencare le copie Snapshot in un volume:

```
volume snapshot show -vserver SVM -volume volume
```

L'esempio seguente mostra le copie Snapshot in vol1:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

Vserver	Volume	Snapshot	State	Size	Total%	Used%
vs1	vol1	hourly.2013-01-25_0005	valid	224KB	0%	0%
		daily.2013-01-25_0010	valid	92KB	0%	0%
		hourly.2013-01-25_0105	valid	228KB	0%	0%
		hourly.2013-01-25_0205	valid	236KB	0%	0%
		hourly.2013-01-25_0305	valid	244KB	0%	0%
		hourly.2013-01-25_0405	valid	244KB	0%	0%
		hourly.2013-01-25_0505	valid	244KB	0%	0%

7 entries were displayed.

2. Ripristinare il contenuto di un volume da una copia Snapshot:

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

Nell'esempio riportato di seguito viene ripristinato il contenuto di vol1:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1  
-snapshot daily.2013-01-25_0010
```

3. Ripetere i passaggi 1 e 2 per ripristinare il volume utilizzando la copia Snapshot desiderata.

## Ulteriori informazioni

- ["KB: Prevenzione e recovery dal ransomware in ONTAP"](#)

## Modificare le opzioni per le copie Snapshot automatiche

A partire da ONTAP 9.11.1, puoi utilizzare la CLI per controllare le impostazioni di conservazione per le copie Snapshot di protezione autonoma dal ransomware (ARP), generate automaticamente in risposta a sospetti attacchi ransomware.

### Prima di iniziare

È possibile modificare solo le opzioni di ARP Snapshot su una SVM di nodo.

### Fasi

1. Per visualizzare tutte le impostazioni di copia correnti di ARP Snapshot, immettere:

```
vserver options -vserver svm_name arw*
```



Il `vserver options command` è un comando nascosto. Per visualizzare la pagina man, immettere `man vserver options` Nella CLI di ONTAP.

2. Per visualizzare le impostazioni di copia correnti di ARP Snapshot, immettere:


```
vserver options -vserver svm_name -option-name arw_setting_name
```

3. Per modificare le impostazioni di copia di ARP Snapshot, immettere:

```
vserver options -vserver svm_name -option-name arw_setting_name -option-value  
arw_setting_value
```

È possibile modificare le seguenti impostazioni:

Impostazione ARW	Descrizione
<b>arw.snap.max.count</b>	Specifica il numero massimo di copie Snapshot ARP che possono esistere in un volume in qualsiasi momento. Le copie meno recenti vengono eliminate per garantire che il numero totale di copie Snapshot ARP rientri nel limite specificato.
<b>arw.snap.create.interval.hours</b>	Specifica l'intervallo <i>in ore</i> tra le copie snapshot ARP. Una nuova copia Snapshot viene creata quando si sospetta un attacco e la copia creata in precedenza è precedente all'intervallo specificato.

Impostazione ARW	Descrizione
<b>arw.snap.normal.retain.interval.hours</b>	Specifica la durata <i>in ore</i> per la quale viene conservata una copia snapshot ARP. Quando una copia ARP Snapshot diventa vecchia, qualsiasi altra copia ARP Snapshot creata prima dell'ultima copia per raggiungere questa età viene eliminata. Nessuna copia snapshot ARP può essere precedente a questa durata.
<b>arw.snap.max.retain.interval.days</b>	<p>Specifica la durata massima <i>in giorni</i> per la quale è possibile conservare una copia snapshot ARP. Qualsiasi copia ARP Snapshot precedente a questa durata verrà eliminata se non viene segnalato alcun attacco sul volume.</p> <p>+</p> <div>  <p>L'intervallo di conservazione massimo per le copie snapshot ARP viene ignorato se viene rilevata una minaccia moderata. La copia snapshot ARP creata in risposta alla minaccia viene conservata fino a quando non si risponde alla minaccia. Contrassegnare una minaccia come falso positivo eliminare le copie snapshot ARP sul volume.</p> </div>
<b>arw.snap.create.interval.hours.post.max.count</b>	Specifica l'intervallo <i>in ore</i> tra le copie snapshot ARP quando il volume contiene già il numero massimo di copie snapshot ARP. Una volta raggiunto il numero massimo di copie, una copia snapshot ARP viene eliminata per creare spazio per una nuova copia. È possibile ridurre la velocità di creazione delle nuove copie Snapshot ARP per conservare le copie meno recenti utilizzando questa opzione. Se il volume contiene già il numero massimo di copie Snapshot ARP, questo intervallo specificato in questa opzione viene utilizzato per la successiva creazione della copia Snapshot ARP, invece di arw.snap.create.interval.hours.
<b>arw.surge.snap.interval.days</b>	Specifica l'intervallo <i>in giorni</i> tra le copie snapshot di sovracorrente ARP. ONTAP crea una copia snapshot ARP surge quando c'è un aumento del traffico io e l'ultima copia snapshot ARP creata è precedente a questo intervallo specificato. Questa opzione specifica anche il periodo di conservazione <i>in giorno</i> per un'istantanea di sovratensione ARP.

## Proteggere dai virus

### Panoramica della configurazione antivirus

Vscan è una soluzione di scansione antivirus sviluppata da NetApp che consente ai clienti di proteggere i propri dati da virus o altri codici dannosi.

Vscan esegue scansioni virus quando i client accedono ai file tramite SMB. È possibile configurare Vscan per la scansione on-demand o in base a una pianificazione. È possibile interagire con Vscan utilizzando l'interfaccia a riga di comando (CLI) di ONTAP o le API (Application Programming Interface) di ONTAP.

#### Informazioni correlate

["Soluzioni partner di Vscan"](#)

## Informazioni sulla protezione antivirus di NetApp

### Informazioni sulla scansione dei virus NetApp

Vscan è una soluzione di scansione antivirus sviluppata da NetApp che consente ai clienti di proteggere i propri dati da virus o altri codici dannosi. Combina il software antivirus fornito dal partner con le funzionalità ONTAP per offrire ai clienti la flessibilità necessaria per gestire la scansione dei file.

#### Come funziona la scansione virus

I sistemi storage trasferiscono le operazioni di scansione a server esterni che ospitano software antivirus di terze parti.

In base alla modalità di scansione attiva, ONTAP invia richieste di scansione quando i client accedono ai file tramite SMB (on-access) o accedono ai file in posizioni specifiche, in base a una pianificazione o immediatamente (on-demand).

- È possibile utilizzare *on-access scanning* per verificare la presenza di virus quando i client aprono, leggono, rinominano o chiudono i file su SMB. Le operazioni sui file vengono sospese fino a quando il server esterno non riporta lo stato di scansione del file. Se il file è già stato sottoposto a scansione, ONTAP consente l'operazione. In caso contrario, richiede una scansione dal server.

La scansione on-access non è supportata per NFS.

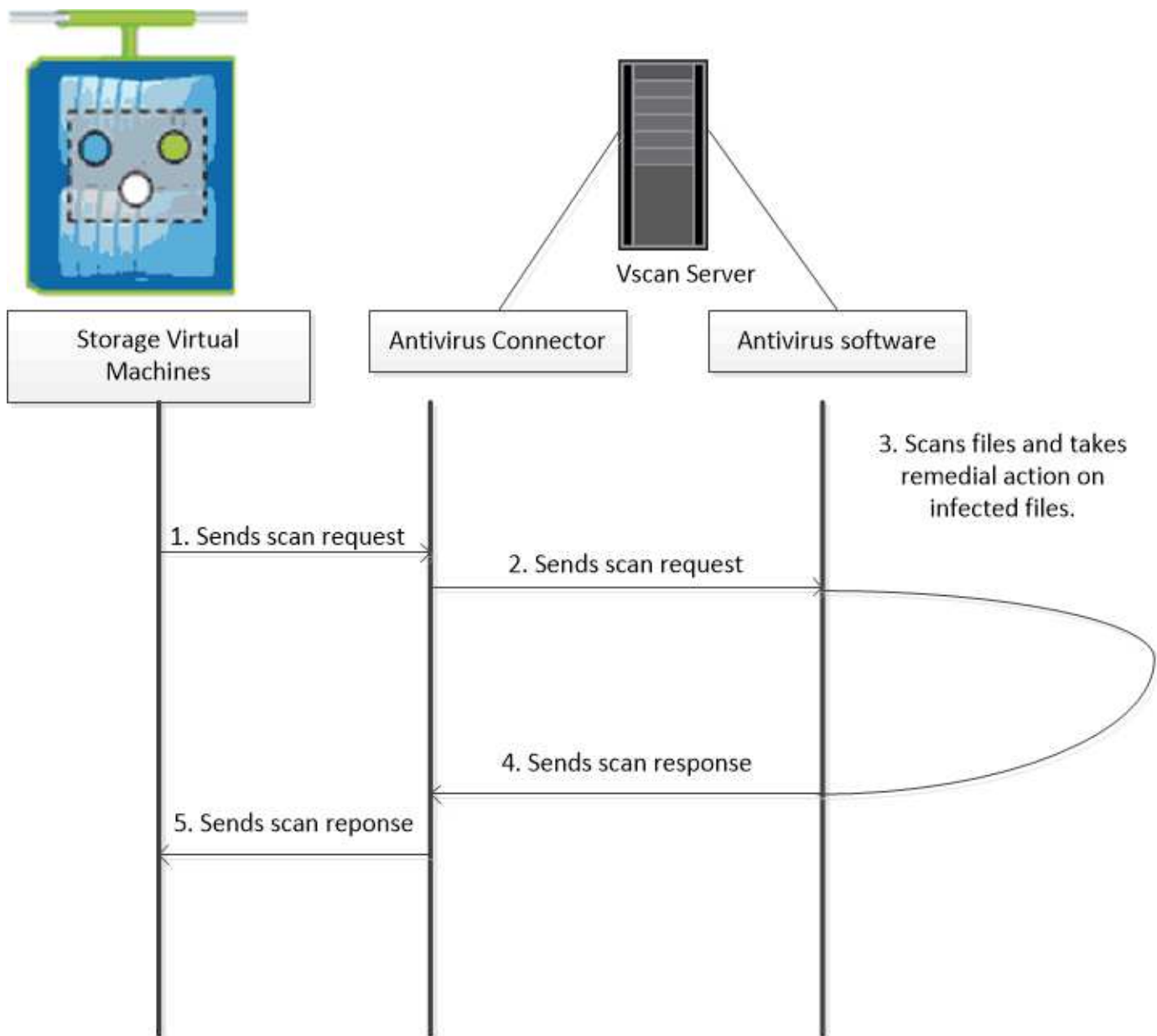
- È possibile utilizzare la *scansione on-demand* per controllare i file alla ricerca di virus immediatamente o in base a una pianificazione. Si consiglia di eseguire scansioni on-demand solo in ore non di punta per evitare di sovraccaricare l'infrastruttura AV esistente, che è normalmente dimensionata per la scansione on-access. Il server esterno aggiorna lo stato di scansione dei file selezionati, in modo da ridurre la latenza di accesso ai file su SMB. In caso di modifiche al file o aggiornamenti della versione software, viene richiesta una nuova scansione del file dal server esterno.

È possibile utilizzare la scansione on-demand per qualsiasi percorso nello spazio dei nomi SVM, anche per i volumi esportati solo tramite NFS.

In genere, si abilitano le modalità di scansione on-access e on-demand su una SVM. In entrambe le modalità, il software antivirus esegue un'azione correttiva sui file infetti in base alle impostazioni del software.

Il connettore antivirus ONTAP, fornito da NetApp e installato sul server esterno, gestisce la comunicazione tra il sistema di storage e il software antivirus.



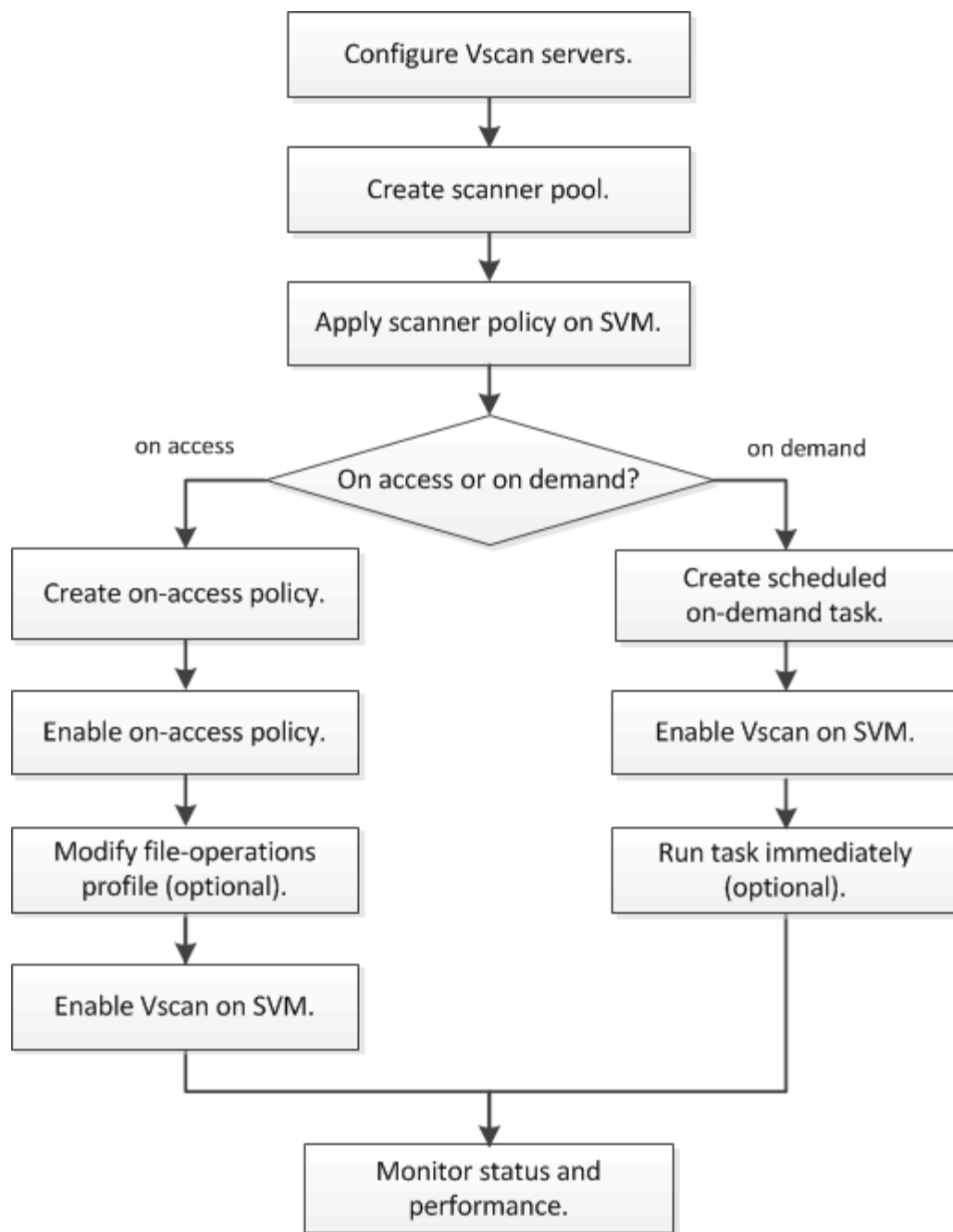


### Workflow di scansione dei virus

Prima di attivare la scansione, è necessario creare un pool di scanner e applicare un criterio scanner. In genere, si abilitano le modalità di scansione on-access e on-demand su una SVM.



È necessario aver completato la configurazione CIFS.



#### Passi successivi

- [Creare un pool di scanner su un singolo cluster](#)
- [Applicare un criterio scanner a un singolo cluster](#)
- [Creare una policy di accesso](#)

#### Architettura antivirus

L'architettura antivirus di NetApp è costituita dal software del server Vscan e dalle relative impostazioni.

#### Software del server Vscan

È necessario installare questo software sul server Vscan.

- **Connettore antivirus ONTAP**

Si tratta di un software fornito da NetApp che gestisce le comunicazioni di risposta e richiesta di scansione tra le SVM e il software antivirus. Può essere eseguito su una macchina virtuale, ma per ottenere le migliori performance utilizza una macchina fisica. È possibile scaricare questo software dal sito del supporto NetApp (richiede l'accesso).

- **Software antivirus**

Si tratta di un software fornito dal partner che esegue la scansione dei file alla ricerca di virus o altro codice dannoso. Specificare le azioni correttive da intraprendere sui file infetti durante la configurazione del software.

## **Impostazioni del software Vscan**

È necessario configurare queste impostazioni software sul server Vscan.

- **Scanner pool**

Questa impostazione definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. Definisce inoltre un periodo di timeout della richiesta di scansione, trascorso il quale la richiesta di scansione viene inviata a un server Vscan alternativo, se disponibile.



Impostare il periodo di timeout nel software antivirus sul server Vscan su un valore inferiore di cinque secondi rispetto al periodo di timeout della richiesta di scansione del pool di scanner. In questo modo si evitano situazioni in cui l'accesso al file viene ritardato o negato del tutto perché il periodo di timeout sul software è superiore al periodo di timeout per la richiesta di scansione.

- **Utente con privilegi**

Questa impostazione è un account utente di dominio utilizzato da un server Vscan per connettersi a SVM. L'account deve essere presente nell'elenco degli utenti con privilegi nel pool di scanner.

- **Criterio scanner**

Questa impostazione determina se un pool di scanner è attivo. I criteri dello scanner sono definiti dal sistema, pertanto non è possibile creare policy personalizzate dello scanner. Sono disponibili solo queste tre policy:

- **Primary** specifica che il pool di scanner è attivo.
- **Secondary** Specifica che il pool di scanner è attivo, solo quando nessuno dei server Vscan nel pool di scanner primario è connesso.
- **Idle** specifica che il pool di scanner non è attivo.

- **Policy di accesso**

Questa impostazione definisce l'ambito di una scansione all'accesso. È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e le estensioni e i percorsi dei file da escludere dalla scansione.

Per impostazione predefinita, viene eseguita la scansione solo dei volumi di lettura/scrittura. È possibile specificare i filtri che consentono la scansione di volumi di sola lettura o che limitano la scansione ai file aperti con accesso di esecuzione:

- `scan-ro-volume` consente la scansione di volumi di sola lettura.
- `scan-execute-access` limita la scansione ai file aperti con accesso di esecuzione.



“Execute access” è diverso da “Execute permission”. Un determinato client avrà “Execute Access” su un file eseguibile solo se il file è stato aperto con “Execute Intent”.

È possibile impostare `scan-mandatory` Selezionare Off per specificare che l’accesso al file è consentito quando non sono disponibili server Vscan per la scansione dei virus. Nella modalità on-access è possibile scegliere tra queste due opzioni che si escludono a vicenda:

- **Obbligatorio:** Con questa opzione, Vscan tenta di inviare la richiesta di scansione al server fino alla scadenza del periodo di timeout. Se la richiesta di scansione non viene accettata dal server, la richiesta di accesso client viene negata.
- **Non obbligatorio:** Con questa opzione, Vscan consente sempre l’accesso al client, indipendentemente dal fatto che sia disponibile un server Vscan per la scansione dei virus.

#### • Attività on-demand

Questa impostazione definisce l’ambito di una scansione on-demand. È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e le estensioni e i percorsi dei file da escludere dalla scansione. Per impostazione predefinita, i file nelle sottodirectory vengono sottoposti a scansione.

Si utilizza una pianificazione cron per specificare quando eseguire l’attività. È possibile utilizzare `vserver vscan on-demand-task run` per eseguire l’attività immediatamente.

#### • Profilo delle operazioni del file Vscan (solo scansione all’accesso)

Il `vscan-fileop-profile` parametro per `vserver cifs share create` Il comando definisce quali operazioni di file SMB attivano la scansione dei virus. Per impostazione predefinita, il parametro è impostato su `standard`, Che è la Best practice di NetApp. È possibile regolare questo parametro in base alle necessità quando si crea o si modifica una condivisione SMB:

- `no-scan` specifica che le scansioni antivirus non vengono mai attivate per la condivisione.
- `standard` specifica che le scansioni antivirus vengono attivate da operazioni di apertura, chiusura e ridenominazione.
- `strict` specifica che le scansioni antivirus vengono attivate da operazioni di apertura, lettura, chiusura e ridenominazione.

Il `strict` profile offre una maggiore sicurezza per le situazioni in cui più client accedono a un file contemporaneamente. Se un client chiude un file dopo averlo scritto e lo stesso file rimane aperto su un secondo client, `strict` garantisce che un’operazione di lettura sul secondo client attivi una scansione prima della chiusura del file.

Fare attenzione a limitare il `strict`` il profilo alle condivisioni contenenti file che prevedi sia accessibile contemporaneamente. Poiché questo profilo genera più richieste di scansione, potrebbe avere un impatto sulle performance.

- `writes-only` specifica che le scansioni antivirus vengono attivate solo quando i file modificati vengono chiusi.

Da `writes-only` genera meno richieste di scansione, in genere migliora le performance.

Se si utilizza questo profilo, lo scanner deve essere configurato per eliminare o mettere in quarantena i file infetti non riparabili, in modo che non sia possibile accedervi. Se, ad esempio, un client chiude un file dopo la scrittura di un virus e il file non viene riparato, eliminato o messo in quarantena, qualsiasi client che accede al file without la scrittura su di esso sarà infetto.



Se un'applicazione client esegue un'operazione di ridenominazione, il file viene chiuso con il nuovo nome e non viene sottoposto a scansione. Se tali operazioni rappresentano un problema di sicurezza nell'ambiente in uso, è necessario utilizzare `standard` oppure `strict` profilo.

## Soluzioni partner di Vscan

NetApp collabora con Trellix, Symantec, Trend Micro e Sentinel One per offrire soluzioni anti-malware e anti-virus leader del settore basate sulla tecnologia ONTAP Vscan. Queste soluzioni consentono di eseguire la scansione dei file per rilevare la presenza di malware e correggere eventuali file interessati.

Come mostrato nella tabella seguente, i dettagli relativi all'interoperabilità per Trellix, Symantec e Trend Micro sono conservati nella matrice di interoperabilità NetApp. I dettagli sull'interoperabilità per Trellix e Symantec sono disponibili anche sui siti Web dei partner. I dettagli sull'interoperabilità di Sentinel One e degli altri nuovi partner verranno gestiti dal partner sui propri siti Web.

Partner	Documentazione della soluzione	Dettagli sull'interoperabilità
Trellix (precedentemente McAfee)	<a href="#">"Documentazione del prodotto Trellix"</a>	<ul style="list-style-type: none"><li>• <a href="#">"Tool di matrice di interoperabilità NetApp"</a></li><li>• <a href="#">"Piattaforme supportate per Endpoint Security Storage Protection (trellix.com)"</a></li></ul>
Symantec	<a href="#">"Symantec Protection Engine 9.0.0"</a>	<ul style="list-style-type: none"><li>• <a href="#">"Tool di matrice di interoperabilità NetApp"</a></li><li>• <a href="#">"Matrice di supporto per dispositivi partner certificati con Symantec Protection Engine (SPE) per NAS (Network Attached Storage) 9.x.x"</a></li><li>• <a href="#">"Matrice di supporto per i dispositivi partner certificata con Symantec Protection Engine (SPE) per NAS (Network Attached Storage) 8.x (broadcom.com)"</a></li></ul>
Trend Micro	<a href="#">"Guida introduttiva di Trend Micro ServerProtect for Storage 6.0"</a>	<a href="#">"Tool di matrice di interoperabilità NetApp"</a>

Partner	Documentazione della soluzione	Dettagli sull'interoperabilità
Sentinel One	<ul style="list-style-type: none"> <li>• <a href="#">"SentinelOne Singularity Cloud Data Security"</a></li> <li>• <a href="#">"Supporto SentinelOne"</a></li> </ul> <p>Questo collegamento richiede l'accesso dell'utente. È possibile richiedere l'accesso da Sentinel One.</p>	Istinto profondo

## Installazione e configurazione del server Vscan

### Installazione e configurazione del server Vscan

Impostare uno o più server Vscan per verificare che i file sul sistema vengano sottoposti a scansione antivirus. Seguire le istruzioni fornite dal fornitore per installare e configurare il software antivirus sul server.

Seguire le istruzioni contenute nel file README fornito da NetApp per installare e configurare il connettore antivirus ONTAP. In alternativa, seguire le istruzioni sul ["Pagina installare il connettore antivirus ONTAP"](#).



Per le configurazioni di disaster recovery e MetroCluster, è necessario configurare server Vscan separati per i cluster ONTAP primario/locale e secondario/partner.

### Requisiti del software antivirus

- Per informazioni sui requisiti del software antivirus, consultare la documentazione del vendor.
- Per informazioni su vendor, software e versioni supportate da Vscan, consultare ["Soluzioni partner di Vscan"](#) pagina.

### Requisiti del connettore antivirus ONTAP

- È possibile scaricare il connettore antivirus ONTAP dalla pagina **Download software** sul sito di supporto NetApp. ["Download NetApp: Software"](#)
- Per informazioni sulle versioni di Windows supportate dal connettore antivirus ONTAP e sui requisiti di interoperabilità, vedere ["Soluzioni partner di Vscan"](#).



È possibile installare diverse versioni dei server Windows per diversi server Vscan in un cluster.

- Sul server Windows deve essere installato .NET 3.0 o versione successiva.
- SMB 2.0 deve essere attivato sul server Windows.

### Installare il connettore antivirus ONTAP

Installare il connettore antivirus ONTAP sul server Vscan per abilitare la comunicazione tra il sistema che esegue ONTAP e il server Vscan. Una volta installato il connettore antivirus ONTAP, il software antivirus è in grado di comunicare con una o più Storage

## Virtual Machine (SVM).

### A proposito di questa attività

- Vedere "[Soluzioni partner di Vscan](#)" Per informazioni sui protocolli supportati, le versioni del software dei fornitori antivirus, le versioni di ONTAP, i requisiti di interoperabilità e i server Windows.
- È necessario installare .NET 4.5.1 o versione successiva.
- Il connettore antivirus ONTAP può essere eseguito su una macchina virtuale. Tuttavia, per ottenere prestazioni ottimali, NetApp consiglia di utilizzare una macchina virtuale dedicata per la scansione antivirus.
- SMB 2,0 deve essere attivato sul server Windows su cui si sta installando ed eseguendo il connettore antivirus ONTAP.

### Prima di iniziare

- Scaricare il file di installazione di ONTAP Antivirus Connector dal sito di assistenza e salvarlo in una directory sul disco rigido.
- Verificare di soddisfare i requisiti per l'installazione del connettore antivirus ONTAP.
- Verificare di disporre dei privilegi di amministratore per installare il connettore antivirus.

### Fasi

1. Avviare l'installazione guidata del connettore antivirus eseguendo il file di installazione appropriato.
2. Selezionare *Avanti*. Viene visualizzata la finestra di dialogo cartella di destinazione.
3. Selezionare *Avanti* per installare il connettore antivirus nella cartella elencata oppure selezionare *Cambia* per eseguire l'installazione in una cartella diversa.
4. Viene visualizzata la finestra di dialogo credenziali servizio Windows connettore AV ONTAP.
5. Immettere le credenziali del servizio Windows o selezionare **Aggiungi** per selezionare un utente. Per un sistema ONTAP, questo utente deve essere un utente di dominio valido e deve esistere nella configurazione del pool di scanner per la SVM.
6. Selezionare **Avanti**. Viene visualizzata la finestra di dialogo Pronto per l'installazione del programma.
7. Selezionare **Installa** per avviare l'installazione o selezionare **Indietro** se si desidera apportare modifiche alle impostazioni.  
Viene visualizzata una finestra di stato che illustra l'avanzamento dell'installazione, seguita dalla finestra di dialogo InstallShield Wizard Completed (Installazione guidata InstallShield completata).
8. Selezionare la casella di controllo Configura LIF ONTAP per continuare con la configurazione di LIF dati o gestione ONTAP.  
Devi configurare almeno una gestione ONTAP o un'interfaccia LIF dati prima che questo server Vscan possa essere utilizzato.
9. Selezionare la casella di controllo Mostra registro **Windows Installer** se si desidera visualizzare i registri di installazione.
10. Selezionare **fine** per terminare l'installazione e chiudere la procedura guidata InstallShield.  
L'icona **Configura LIF ONTAP** viene salvata sul desktop per configurare le LIF ONTAP.
11. Aggiungere una SVM al connettore antivirus.  
Puoi aggiungere una SVM al connettore antivirus aggiungendo una LIF di gestione ONTAP, che viene interrogata per recuperare l'elenco di LIF dati, oppure configurando direttamente la LIF o la LIF dati.  
Se la LIF di gestione ONTAP è configurata, devi anche fornire le informazioni di polling e le credenziali dell'account amministratore di ONTAP.
  - Verifica che la LIF di gestione o l'indirizzo IP della SVM sia abilitato per `management-https`. Non è

necessario quando si configurano solo LIF dati.

- Verificare di aver creato un account utente per l'applicazione HTTP e di aver assegnato un ruolo con accesso (almeno di sola lettura) a `/api/network/ip/interfaces` API REST. Per ulteriori informazioni sulla creazione di un utente, vedere la ["creazione del ruolo di accesso di sicurezza"](#) e. ["creazione dell'accesso di sicurezza"](#) Pagine man di ONTAP.



Puoi anche utilizzare l'utente di dominio come account aggiungendo una SVM con tunnel di autenticazione per una SVM amministrativa. Per ulteriori informazioni, consultare ["login di sicurezza creazione del tunnel di dominio"](#) Pagina man di ONTAP o utilizzare `/api/security/accounts` e. `/api/security/roles` REST API per configurare l'account e il ruolo di amministratore.

## Fasi

1. Fare clic con il pulsante destro del mouse sull'icona **Configure ONTAP LIF**, salvata sul desktop al termine dell'installazione di Antivirus Connector, quindi selezionare **Esegui come amministratore**.
2. Nella finestra di dialogo Configura LIF ONTAP, selezionare il tipo di configurazione preferito, quindi eseguire le seguenti operazioni:

Per creare questo tipo di LIF...	Eseguire questa procedura...
LIF dati	<ol style="list-style-type: none"><li>a. Impostare "ruolo" su "dati"</li><li>b. Impostare "protocollo dati" su "cifs"</li><li>c. Impostare "policy firewall" su "data"</li><li>d. Impostare "politica di servizio" su "file-dati-predefiniti"</li></ol>
LIF di gestione	<ol style="list-style-type: none"><li>a. Impostare "ruolo*" su "dati"</li><li>b. Impostare "protocollo dati" su "nessuno"</li><li>c. Impostare "policy firewall" su "Mgmt"</li><li>d. Impostare "politica di servizio" su "gestione predefinita"</li></ol>

Scopri di più ["Creazione di una LIF"](#).

Dopo aver creato una LIF, inserisci i dati o l'indirizzo IP della LIF di gestione o della SVM che desideri aggiungere. Puoi anche inserire la LIF di gestione cluster. Se specifichi la LIF di gestione cluster, tutte le SVM del cluster che servono SMB potranno utilizzare il server Vscan.



Quando è richiesta l'autenticazione Kerberos per i server Vscan, ogni LIF dati SVM deve avere un nome DNS univoco ed è necessario registrarlo come nome principale server (SPN) con Windows Active Directory. Quando non è disponibile un nome DNS univoco per ogni LIF dati o registrato come SPN, il server Vscan utilizza il meccanismo NT LAN Manager per l'autenticazione. Se si aggiungono o modificano i nomi DNS e gli SPN dopo la connessione del server Vscan, è necessario riavviare il servizio Antivirus Connector sul server Vscan per applicare le modifiche.

3. Per configurare una LIF di gestione, inserisci la durata del polling in secondi. La durata del poll è la frequenza con cui il connettore antivirus verifica le modifiche alle SVM o alla configurazione LIF del cluster. L'intervallo di polling predefinito è di 60 secondi.
4. Inserisci il nome dell'account e la password dell'amministratore ONTAP per configurare una LIF di



gestione.

5. Fare clic su **Test** per controllare la connettività e verificare l'autenticazione. L'autenticazione viene verificata solo per una configurazione LIF di gestione.
6. Fare clic su **Update** (Aggiorna) per aggiungere la LIF all'elenco delle LIF a cui eseguire il polling o connettersi.
7. Fare clic su **Salva** per salvare la connessione al Registro di sistema.
8. Fare clic su **Esporta** se si desidera esportare l'elenco delle connessioni in un file di importazione del Registro di sistema o di esportazione del Registro di sistema. Ciò è utile se più server Vscan utilizzano lo stesso set di LIF di gestione o di dati.

Vedere "[Configurare la pagina ONTAP Antivirus Connector](#)" per le opzioni di configurazione.

## Configurare il connettore antivirus ONTAP

Configurare il connettore antivirus ONTAP per specificare una o più Storage Virtual Machine (SVM) a cui connettersi inserendo la LIF di gestione ONTAP, le informazioni di polling e le credenziali dell'account amministratore ONTAP o solo la LIF dati. Puoi anche modificare i dettagli di una connessione SVM o rimuovere una connessione SVM. Per impostazione predefinita, il connettore antivirus ONTAP utilizza le API REST per recuperare l'elenco di LIF di dati, se la LIF di gestione ONTAP è configurata.

### Modificare i dettagli di una connessione SVM

Puoi aggiornare i dettagli di una connessione SVM (Storage Virtual Machine), che è stata aggiunta al connettore antivirus, modificando la LIF di gestione ONTAP e le informazioni di polling. Non puoi aggiornare le LIF dati dopo che sono state aggiunte. Per aggiornare le LIF dati, devi prima rimuoverle e poi aggiungerle di nuovo con il nuovo indirizzo LIF o IP.

### Prima di iniziare

Verificare di aver creato un account utente per l'applicazione HTTP e di aver assegnato un ruolo con accesso (almeno di sola lettura) a `/api/network/ip/interfaces` API REST.

Per ulteriori informazioni sulla creazione di un utente, vedere la "[creazione del ruolo di accesso di sicurezza](#)" e a. "[creazione dell'accesso di sicurezza](#)" comandi.

Puoi anche utilizzare l'utente di dominio come account aggiungendo una SVM con tunnel di autenticazione per una SVM amministrativa.

Per ulteriori informazioni, consultare "[login di sicurezza creazione del tunnel di dominio](#)" Pagina man di ONTAP.

### Fasi

1. Fare clic con il pulsante destro del mouse sull'icona **Configura LIF ONTAP**, salvata sul desktop al termine dell'installazione di Antivirus Connector, quindi selezionare **Esegui come amministratore**. Viene visualizzata la finestra di dialogo Configura LIF ONTAP.
2. Selezionare l'indirizzo IP della SVM, quindi fare clic su **Aggiorna**.
3. Aggiornare le informazioni secondo necessità.
4. Fare clic su **Salva** per aggiornare i dettagli della connessione nel registro.
5. Fare clic su **Esporta** se si desidera esportare l'elenco delle connessioni in un'importazione del Registro di sistema o in un file di esportazione del Registro di sistema.  
Ciò è utile se più server Vscan utilizzano lo stesso set di LIF di gestione o di dati.

## Rimuovere una connessione SVM dal connettore antivirus

Se non ti serve più una connessione SVM, puoi rimuoverla.

### Fasi

1. Fare clic con il pulsante destro del mouse sull'icona **Configura LIF ONTAP**, salvata sul desktop al termine dell'installazione di Antivirus Connector, quindi selezionare **Esegui come amministratore**. Viene visualizzata la finestra di dialogo Configura LIF ONTAP.
2. Selezionare uno o più indirizzi IP SVM, quindi fare clic su **Rimuovi**.
3. Fare clic su **Salva** per aggiornare i dettagli della connessione nel registro.
4. Fare clic su **Esporta** se si desidera esportare l'elenco delle connessioni in un file di importazione del Registro di sistema o di esportazione del Registro di sistema.  
Ciò è utile se più server Vscan utilizzano lo stesso set di LIF di gestione o di dati.

### Risolvere i problemi

#### Prima di iniziare

Quando si creano i valori del Registro di sistema in questa procedura, utilizzare il riquadro a destra.

È possibile attivare o disattivare i registri dei connettori antivirus per scopi diagnostici. Per impostazione predefinita, questi registri sono disattivati. Per migliorare le prestazioni, è necessario disattivare i registri del connettore antivirus e attivarli solo per gli eventi critici.

### Fasi

1. Selezionare **Start**, digitare "regedit" nella casella di ricerca, quindi selezionare `regedit.exe` Nell'elenco programmi.
2. In **Editor del Registro di sistema**, individuare la seguente sottochiave per il connettore antivirus ONTAP:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Creare i valori del Registro di sistema specificando il tipo, il nome e i valori indicati nella tabella seguente:

Tipo	Nome	Valori
Stringa	Tracepath	c:\avshim.log

Questo valore del Registro di sistema potrebbe essere qualsiasi altro percorso valido.

4. Creare un altro valore del Registro di sistema fornendo il tipo, il nome, i valori e le informazioni di registrazione mostrate nella tabella seguente:

Tipo	Nome	Registrazione critica	Registrazione intermedia	Registrazione dettagliata
DWORD	TRACELEVEL	1	2 o 3	4

In questo modo si attivano i registri del connettore antivirus salvati al valore del percorso fornito in TracePath nel passaggio 3.

5. Disattivare i registri del connettore antivirus eliminando i valori del Registro di sistema creati nei passaggi 3 e 4.

6. Creare un altro valore di registro di tipo "MULTI\_SZ" con il nome "LogRotation" (senza virgolette). In "LogRotation",  
Fornire "logFileSize:1" come voce per la dimensione di rotazione (dove 1 rappresenta 1MB) e nella riga successiva fornire "logFileCount:5" come un'immissione del limite di rotazione (5 è il limite).



Questi valori sono facoltativi. Se non vengono forniti, vengono utilizzati i valori predefiniti dei file 20MB e 10 rispettivamente per la dimensione di rotazione e il limite di rotazione. I valori interi forniti non forniscono valori decimali o frazioni. Se si forniscono valori superiori ai valori predefiniti, vengono utilizzati i valori predefiniti.

7. Per disattivare la rotazione del registro configurata dall'utente, eliminare i valori del Registro di sistema creati nel passaggio 6.

### Banner personalizzabile

Un banner personalizzato ti consente di inserire un'istruzione legale e un'esclusione di responsabilità per l'accesso al sistema nella finestra *Configura ONTAP LIF API*.

### Fase

1. Modificare l'intestazione predefinita aggiornando il contenuto della `banner.txt` nella directory di installazione, quindi salvare le modifiche.  
Riapri la finestra Configura API LIF ONTAP per vedere le modifiche riflesse nel banner.

### Attivare la modalità Extended Ordinance (EO)

È possibile attivare e disattivare la modalità Extended Ordinance (EO) per garantire un funzionamento sicuro.

### Fasi

1. Selezionare **Start**, digitare "regedit" nella casella di ricerca, quindi selezionare `regedit.exe` Nell'elenco programmi.
2. In **Editor del Registro di sistema**, individuare la seguente sottochiave per ONTAP Antivirus Connector:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Nel riquadro a destra, creare un nuovo valore del Registro di sistema di tipo "DWORD" con il nome "EO\_Mode" (senza virgolette) e il valore "1" (senza virgolette) per attivare la modalità EO o il valore "0" (senza virgolette) per disattivare la modalità EO.



Per impostazione predefinita, se `EO_Mode` La voce del Registro di sistema è assente, la modalità EO è disattivata. Quando si attiva la modalità EO, è necessario configurare sia il server syslog esterno che l'autenticazione dei certificati reciproci.

### Configurare il server syslog esterno

#### Prima di iniziare

Tenere presente che quando si creano i valori del Registro di sistema in questa procedura, utilizzare il riquadro a destra.

### Fasi

1. Selezionare **Start**, digitare "regedit" nella casella di ricerca, quindi selezionare `regedit.exe` Nell'elenco programmi.

2. In **Editor del Registro di sistema**, creare la seguente sottochiave per ONTAP Antivirus Connector per la configurazione syslog:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog

3. Creare un valore del Registro di sistema specificando il tipo, il nome e il valore come illustrato nella tabella seguente:

Tipo	Nome	Valore
DWORD	syslog_enabled	1 o 0

Si noti che un valore "1" attiva il syslog e un valore "0" lo disattiva.

4. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome
REG_SZ	Syslog_host

Fornire l'indirizzo IP dell'host syslog o il nome di dominio per il campo valore.

5. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome
REG_SZ	Porta_syslog

Specificare il numero della porta su cui viene eseguito il server syslog nel campo Value.

6. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome
REG_SZ	Syslog_Protocol

Immettere il protocollo in uso sul server syslog, "tcp" o "udp", nel campo valore.

7. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome	LOG_CRIT	LOG_NOTICE	LOG_INFO	LOG_DEBUG
DWORD	Syslog_level	2	5	6	7

8. Creare un altro valore del Registro di sistema fornendo le informazioni indicate nella tabella seguente:

Tipo	Nome	Valore
DWORD	syslog_tls	1 o 0

Si noti che un valore "1" abilita syslog con TLS (Transport Layer Security) e un valore "0" disabilita syslog con TLS.

### Garantire il corretto funzionamento di un server syslog esterno configurato

- Se la chiave è assente o ha un valore nullo:
  - L'impostazione predefinita del protocollo è "tcp".
  - L'impostazione predefinita della porta è "514" per "tcp/udp" e "6514" per TLS.
  - Il livello syslog predefinito è 5 (LOG\_NOTICE).
- Puoi confermare che syslog è attivato verificando che `syslog_enabled` il valore è "1". Quando il `syslog_enabled` il valore è "1", dovrebbe essere possibile accedere al server remoto configurato indipendentemente dall'attivazione o meno della modalità EO.
- Se la modalità EO è impostata su "1" e si modifica la `syslog_enabled` valore compreso tra "1" e "0", vale quanto segue:
  - Non è possibile avviare il servizio se syslog non è abilitato in modalità EO.
  - Se il sistema è in esecuzione in modalità regolare, viene visualizzato un avviso che indica che syslog non può essere disattivato in modalità EO e che syslog è impostato con forza su "1", che è possibile vedere nel Registro di sistema. In questo caso, è necessario disattivare prima la modalità EO e poi disabilitare syslog.
- Se il server syslog non è in grado di funzionare correttamente quando la modalità EO e syslog sono attivati, il servizio si arresta. Questo può verificarsi per uno dei seguenti motivi:
  - È stato configurato un `syslog_host` non valido o non esistente.
  - È stato configurato un protocollo non valido tranne UDP o TCP.
  - Un numero di porta non è valido.
- Per una configurazione TCP o TLS su TCP, se il server non è in ascolto sulla porta IP, la connessione non riesce e il servizio si arresta.

### Configurare l'autenticazione reciproca dei certificati X,509

L'autenticazione reciproca basata su certificati X,509 è possibile per la comunicazione SSL (Secure Sockets Layer) tra il connettore antivirus e ONTAP nel percorso di gestione. Se la modalità EO è attivata e il certificato non viene trovato, il connettore AV termina. Eseguire la seguente procedura sul connettore dell'antivirus:

#### Fasi

1. Il connettore antivirus ricerca il certificato client del connettore antivirus e il certificato dell'autorità di certificazione (CA) per il server NetApp nel percorso di directory da cui il connettore antivirus esegue la directory di installazione. Copiare i certificati in questo percorso di directory fisso.
2. Incorporare il certificato client e la relativa chiave privata nel formato PKCS12 e denominarlo "AV\_client.P12".
3. Verificare che il certificato CA (insieme a qualsiasi autorità di firma intermedia fino alla CA principale) utilizzato per firmare il certificato per il server NetApp sia in formato PEM (Privacy Enhanced Mail) e denominato "ONTAP\_CA.pem". Posizionarlo nella directory di installazione di Antivirus Connector. Sul sistema NetApp ONTAP, installare il certificato CA (insieme a qualsiasi autorità di firma intermedia fino alla CA principale) utilizzato per firmare il certificato client per il connettore antivirus in "ONTAP" come certificato di tipo "client-ca".

## Configurare i pool di scanner

### Panoramica sulla configurazione dei pool di scanner

Un pool di scanner definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. Un criterio dello scanner determina se un pool di scanner è attivo.



Se si utilizza un criterio di esportazione su un server SMB, è necessario aggiungere ciascun server Vscan al criterio di esportazione.

### Creare un pool di scanner su un singolo cluster

Un pool di scanner definisce i server Vscan e gli utenti con privilegi che possono connettersi alle SVM. È possibile creare un pool di scanner per una singola SVM o per tutte le SVM in un cluster.

#### Di cosa hai bisogno

- I server SVM e Vscan devono trovarsi nello stesso dominio o in domini attendibili.
- Per i pool di scanner definiti per una singola SVM, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione SVM o la LIF dei dati SVM.
- Per i pool di scanner definiti per tutte le SVM in un cluster, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione del cluster.
- L'elenco degli utenti con privilegi deve includere l'account utente di dominio utilizzato dal server Vscan per connettersi a SVM.
- Una volta configurato il pool di scanner, controllare lo stato della connessione ai server.

#### Fasi

##### 1. Creazione di un pool di scanner:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users privileged_users
```

- Specificare una SVM di dati per un pool definito per una singola SVM e specificare una SVM amministrativa del cluster per un pool definito per tutte le SVM in un cluster.
- Specificare un indirizzo IP o un FQDN per ciascun nome host del server Vscan.
- Specificare il dominio e il nome utente per ciascun utente con privilegi. Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando crea un pool di scanner denominato SP su vs1 SVM:

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users cifs\u1,cifs\u2
```

##### 2. Verificare che il pool di scanner sia stato creato:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner-pool scanner_pool
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di SP pool di scanner:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool SP

Vserver: vs1
Scanner Pool: SP
Applied Policy: idle
Current Status: off
Cluster on Which Policy Is Applied: -
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-27.fsct.nb
List of Privileged Users: cifs\u1, cifs\u2
```

È inoltre possibile utilizzare `vserver vscan scanner-pool show` Per visualizzare tutti i pool di scanner su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

## Creazione di pool di scanner nelle configurazioni MetroCluster

È necessario creare pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster, corrispondente alle SVM primarie e secondarie sul cluster.

### Di cosa hai bisogno

- I server SVM e Vscan devono trovarsi nello stesso dominio o in domini attendibili.
- Per i pool di scanner definiti per una singola SVM, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione SVM o la LIF dei dati SVM.
- Per i pool di scanner definiti per tutte le SVM in un cluster, è necessario aver configurato il connettore antivirus ONTAP con la LIF di gestione del cluster.
- L'elenco degli utenti con privilegi deve includere l'account utente di dominio utilizzato dal server Vscan per connettersi a SVM.
- Una volta configurato il pool di scanner, controllare lo stato della connessione ai server.

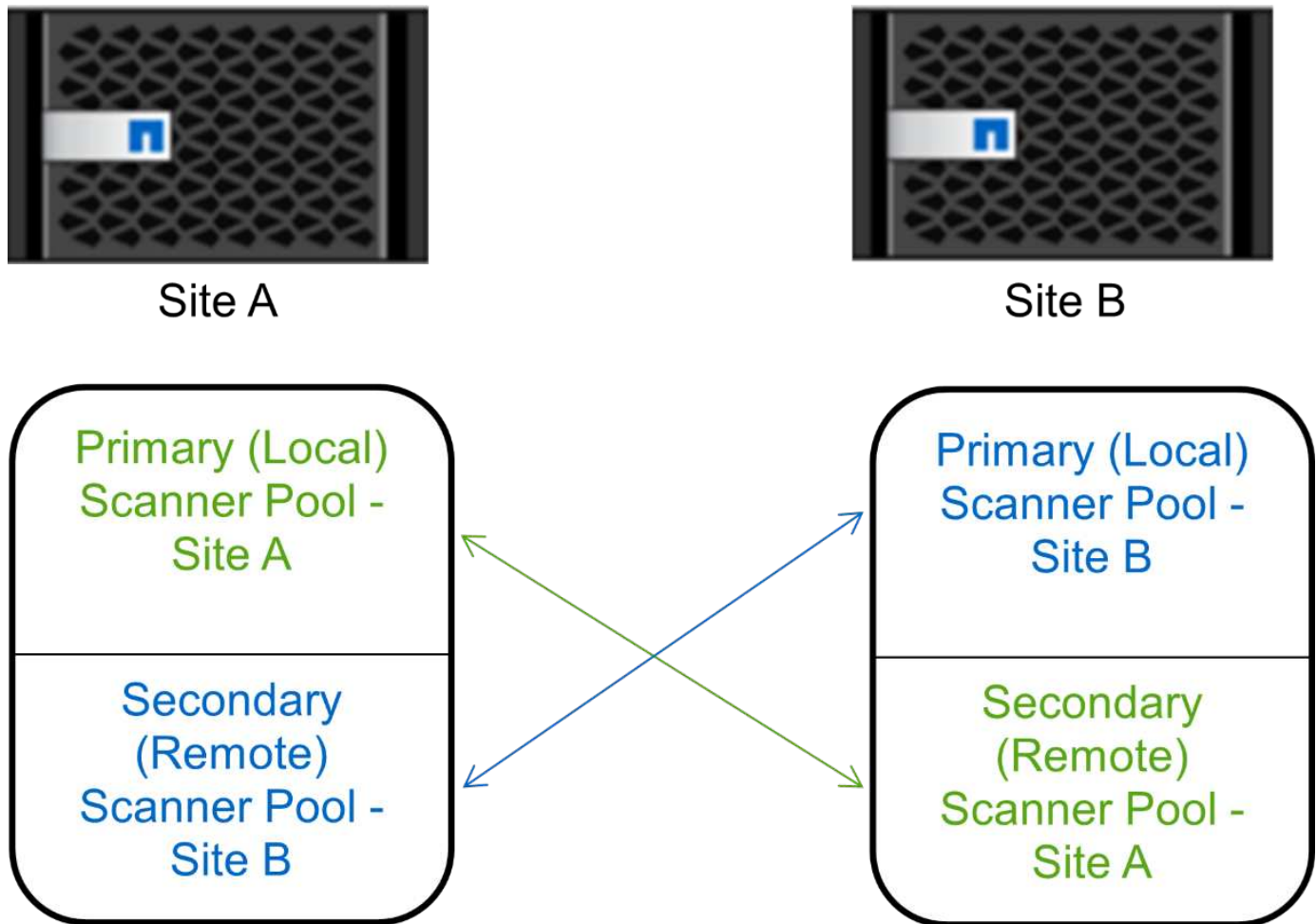
### A proposito di questa attività

Le configurazioni MetroCluster proteggono i dati implementando due cluster mirrorati fisicamente separati. Ciascun cluster replica in modo sincrono i dati e la configurazione SVM dell'altro. Una SVM primaria sul cluster locale serve i dati quando il cluster è online. Una SVM secondaria sul cluster locale serve i dati quando il cluster remoto non è in linea.

Ciò significa che è necessario creare pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster, il pool secondario diventa attivo quando il cluster inizia a servire i dati dalla SVM

secondaria. Per il disaster recovery (DR), la configurazione è simile a quella di MetroCluster.

Questa figura mostra una tipica configurazione MetroCluster/DR.



#### Fasi

##### 1. Creazione di un pool di scanner:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users  
privileged_users
```

- Specificare una SVM di dati per un pool definito per una singola SVM e specificare una SVM amministrativa del cluster per un pool definito per tutte le SVM in un cluster.
- Specificare un indirizzo IP o un FQDN per ciascun nome host del server Vscan.
- Specificare il dominio e il nome utente per ciascun utente con privilegi.



È necessario creare tutti i pool di scanner dal cluster contenente la SVM primaria.

Per un elenco completo delle opzioni, vedere la pagina man del comando.

I seguenti comandi creano pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster:



```

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

```

## 2. Verificare che i pool di scanner siano stati creati:

```

vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool

```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli del pool di scanner pool1:

```

cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: idle
Current Status: off
Cluster on Which Policy Is Applied: -
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2

```

È inoltre possibile utilizzare `vserver vscan scanner-pool show` Per visualizzare tutti i pool di scanner su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

## Applicare un criterio scanner a un singolo cluster

Un criterio dello scanner determina se un pool di scanner è attivo. È necessario attivare un pool di scanner prima che i server Vscan definiti possano connettersi a una SVM.

## A proposito di questa attività

- È possibile applicare un solo criterio scanner a un pool di scanner.
- Se è stato creato un pool di scanner per tutte le SVM in un cluster, è necessario applicare un criterio di scanner a ciascuna SVM singolarmente.

## Fasi

### 1. Applicare un criterio scanner:

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool  
scanner_pool -scanner-policy primary|secondary|idle -cluster  
cluster_to_apply_policy_on
```

Un criterio dello scanner può avere uno dei seguenti valori:

- **Primary** specifica che il pool di scanner è attivo.
- **Secondary** Specifica che il pool di scanner è attivo solo se nessuno dei server Vscan nel pool di scanner primario è connesso.
- **Idle** specifica che il pool di scanner non è attivo.

Nell'esempio seguente viene indicato il nome del pool di scanner SP su vs1 SVM è attivo:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1  
-scanner-pool SP -scanner-policy primary
```

### 2. Verificare che il pool di scanner sia attivo:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner  
-pool scanner_pool
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di SP pool di scanner:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool  
SP  
  
Vserver: vs1  
Scanner Pool: SP  
Applied Policy: primary  
Current Status: on  
Cluster on Which Policy Is Applied: cluster1  
Scanner Pool Config Owner: vserver  
List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27  
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-  
27.fsct.nb  
List of Privileged Users: cifs\u1, cifs\u2
```

È possibile utilizzare `vserver vscan scanner-pool show-active` Per visualizzare i pool di scanner attivi su una SVM. Per la sintassi completa del comando, vedere la pagina `man` del comando.

## Applicare i criteri dello scanner nelle configurazioni MetroCluster

Un criterio dello scanner determina se un pool di scanner è attivo. È necessario applicare un criterio dello scanner ai pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster.

### A proposito di questa attività

- È possibile applicare un solo criterio scanner a un pool di scanner.
- Se è stato creato un pool di scanner per tutte le SVM in un cluster, è necessario applicare un criterio di scanner a ciascuna SVM singolarmente.
- Per le configurazioni di disaster recovery e MetroCluster, è necessario applicare un criterio dello scanner a ogni pool di scanner nel cluster locale e nel cluster remoto.
- Nel criterio creato per il cluster locale, è necessario specificare il cluster locale in `cluster` parametro. Nel criterio creato per il cluster remoto, è necessario specificare il cluster remoto in `cluster` parametro. Il cluster remoto può quindi rilevare le operazioni di scansione dei virus in caso di disastro.

### Fasi

1. Applicare un criterio scanner:

```
vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
scanner_pool -scanner-policy primary|secondary|idle -cluster
cluster_to_apply_policy_on
```

Un criterio dello scanner può avere uno dei seguenti valori:

- `Primary` specifica che il pool di scanner è attivo.
- `Secondary` Specifica che il pool di scanner è attivo solo se nessuno dei server Vscan nel pool di scanner primario è connesso.
- `Idle` specifica che il pool di scanner non è attivo.



È necessario applicare tutti i criteri dello scanner dal cluster contenente la SVM primaria.

I seguenti comandi applicano i criteri dello scanner ai pool di scanner primari e secondari su ciascun cluster in una configurazione MetroCluster:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy secondary -cluster
cluster2
```

## 2. Verificare che il pool di scanner sia attivo:

```
vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli del pool di scanner pool1:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

Vserver: cifssvm1
Scanner Pool: pool1_for_site1
Applied Policy: primary
Current Status: on
Cluster on Which Policy Is Applied: cluster1
Scanner Pool Config Owner: vserver
List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
List of Privileged Users: cifs\u1,cifs\u2
```

È possibile utilizzare `vserver vscan scanner-pool show-active` Per visualizzare i pool di scanner attivi su una SVM. Per la sintassi completa dei comandi, vedere la pagina man del comando.

## Comandi per la gestione dei pool di scanner

È possibile modificare ed eliminare i pool di scanner e gestire gli utenti con privilegi e i server Vscan per un pool di scanner. È inoltre possibile visualizzare informazioni riepilogative sul pool di scanner.

Se si desidera...	Immettere il seguente comando...
Modificare un pool di scanner	<code>vserver vscan scanner-pool modify</code>
Eliminare un pool di scanner	<code>vserver vscan scanner-pool delete</code>
Aggiungere utenti con privilegi a un pool di scanner	<code>vserver vscan scanner-pool privileged-users add</code>
Eliminare gli utenti con privilegi da un pool di scanner	<code>vserver vscan scanner-pool privileged-users remove</code>
Aggiungere server Vscan a un pool di scanner	<code>vserver vscan scanner-pool servers add</code>
Eliminare i server Vscan da un pool di scanner	<code>vserver vscan scanner-pool servers remove</code>
Visualizza riepilogo e dettagli di un pool di scanner	<code>vserver vscan scanner-pool show</code>
Visualizzare gli utenti con privilegi per un pool di scanner	<code>vserver vscan scanner-pool privileged-users show</code>
Visualizzare i server Vscan per tutti i pool di scanner	<code>vserver vscan scanner-pool servers show</code>

Per ulteriori informazioni su questi comandi, consulta le pagine man.

## Configurare la scansione on-access

### Creare una policy di accesso

Un criterio di accesso definisce l'ambito di una scansione all'accesso. È possibile creare una policy di accesso per una singola SVM o per tutte le SVM in un cluster. Se è stata creata una policy di accesso per tutte le SVM in un cluster, è necessario attivare la policy su ogni SVM singolarmente.

#### A proposito di questa attività

- È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e le estensioni e i percorsi dei file da escludere dalla scansione.
- È possibile impostare `scan-mandatory` Selezionare Off per specificare che l'accesso al file è consentito quando non sono disponibili server Vscan per la scansione dei virus.
- Per impostazione predefinita, ONTAP crea una policy di accesso denominata "default\_CIFS" e la abilita per tutte le SVM in un cluster.
- Qualsiasi file idoneo per l'esclusione della scansione in base a `paths-to-exclude`, `file-ext-to-exclude`, o `max-file-size` i parametri non vengono presi in considerazione per la scansione, anche se `scan-mandatory` l'opzione è impostata su on. (Selezionare questa opzione ["risoluzione dei problemi"](#) sezione per i problemi di connettività relativi a `scan-mandatory` opzione).

- Per impostazione predefinita, viene eseguita la scansione solo dei volumi di lettura/scrittura. È possibile specificare i filtri che consentono la scansione di volumi di sola lettura o che limitano la scansione ai file aperti con accesso di esecuzione.
- La scansione virus non viene eseguita su una condivisione SMB per la quale il parametro *Continuously-Available* è impostato su Yes.
- Vedere "[Architettura antivirus](#)" Per ulteriori informazioni sul profilo *Vscan file-Operations*.
- È possibile creare un massimo di dieci (10) criteri di accesso per SVM. Tuttavia, è possibile attivare un solo criterio di accesso alla volta.
  - È possibile escludere un massimo di cento (100) percorsi ed estensioni di file dalla scansione virus in una policy di accesso.
- Alcuni consigli sull'esclusione dei file:
  - Considerare l'esclusione di file di grandi dimensioni (è possibile specificare le dimensioni del file) dalla scansione dei virus perché possono causare un rallentamento della risposta o timeout delle richieste di scansione per gli utenti CIFS. La dimensione predefinita del file per l'esclusione è 2 GB.
  - Considerare l'esclusione di estensioni di file come `.vhd` e `.tmp` perché i file con queste estensioni potrebbero non essere appropriati per la scansione.
  - Considerare l'esclusione di percorsi di file come la directory di quarantena o i percorsi in cui sono memorizzati solo i dischi rigidi o i database virtuali.
  - Verificare che tutte le esclusioni siano specificate nello stesso criterio, in quanto è possibile attivare un solo criterio alla volta. NetApp consiglia di utilizzare lo stesso set di esclusioni specificato nel motore antivirus.
- Per un è necessario un criterio di accesso [scansione su richiesta](#). Per evitare la scansione all'accesso per, è necessario impostare `-scan-files-with-no-ext` a false e `-file-ext-to-exclude` a `*` per escludere tutte le estensioni.

## Fasi

### 1. Creare una policy di accesso:

```
vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
-policy-name policy_name -protocol CIFS -max-file-size
max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
-file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
-exclude paths_of_files_to_exclude -scan-mandatory on|off
```

- Specificare una SVM di dati per una policy definita per una singola SVM, una SVM amministrativa del cluster per una policy definita per tutte le SVM in un cluster.
- Il `-file-ext-to-exclude` l'impostazione ha la precedenza su `-file-ext-to-include` impostazione.
- Impostare `-scan-files-with-no-ext` a true per eseguire la scansione dei file senza estensioni. Il comando seguente crea una policy di accesso denominata `Policy1` su `vs1` SVM:

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include "mp*", "tx*" -file-ext-to-exclude "mp3", "txt" -scan
-files-with-no-ext false -paths-to-exclude "\\vol\ a b\","\\vol\ a, b\"
```

2. Verificare che il criterio di accesso sia stato creato: `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di Policy1 policy:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

Vserver: vs1
Policy: Policy1
Policy Status: off
Policy Config Owner: vserver
File-Access Protocol: CIFS
Filters: scan-ro-volume
Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
File Paths Not to Scan: \vol\ a b\, \vol\ a,b\
File Extensions Not to Scan: mp3, txt
File Extensions to Scan: mp*, tx*
Scan Files with No Extension: false
```

### Attivare un criterio di accesso

Un criterio di accesso definisce l'ambito di una scansione all'accesso. È necessario attivare un criterio di accesso su una SVM prima di poter eseguire la scansione dei relativi file.

Se è stata creata una policy di accesso per tutte le SVM in un cluster, è necessario attivare la policy su ogni SVM singolarmente. È possibile attivare un solo criterio di accesso su una SVM alla volta.

#### Fasi

1. Attivare una policy di accesso:

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name
policy_name
```

Il comando seguente attiva un criterio di accesso denominato Policy1 su vs1 SVM:

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. Verificare che il criterio di accesso sia attivato:

```
vserver vscan on-access-policy show -instance data_SVM -policy-name
```

*policy\_name*

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di Policy1 policy di accesso:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

Vserver: vs1
Policy: Policy1
Policy Status: on
Policy Config Owner: vserver
File-Access Protocol: CIFS
Filters: scan-ro-volume
Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
File Paths Not to Scan: \vol\ a b\, \vol\ a, b\
File Extensions Not to Scan: mp3, txt
File Extensions to Scan: mp*, tx*
Scan Files with No Extension: false
```

### Modificare il profilo delle operazioni del file Vscan per una condivisione SMB

Il *profilo delle operazioni del file Vscan* per una condivisione SMB definisce le operazioni sulla condivisione che possono attivare la scansione. Per impostazione predefinita, il parametro è impostato su `standard`. È possibile regolare il parametro in base alle necessità quando si crea o si modifica una condivisione SMB.

Vedere ["Architettura antivirus"](#) Per ulteriori informazioni sul profilo *Vscan file-Operations*.



La scansione antivirus non viene eseguita su una condivisione SMB che dispone di `continuously-available` parametro impostato su `Yes`.

### Fase

1. Modificare il valore del profilo delle operazioni del file Vscan per una condivisione SMB:

```
vserver cifs share modify -vserver data_SVM -share-name share -path share_path
-vscan-fileop-profile no-scan|standard|strict|writes-only
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando modifica il profilo delle operazioni del file Vscan per una condivisione SMB in `strict`:



```
cluster1::> vserver cifs share modify -vserver vs1 -share-name  
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

### Comandi per la gestione delle policy di accesso

È possibile modificare, disattivare o eliminare un criterio di accesso. È possibile visualizzare un riepilogo e i dettagli della policy.

Se si desidera...	Immettere il seguente comando...
Creare una policy di accesso	<code>vserver vscan on-access-policy create</code>
Modificare un criterio di accesso	<code>vserver vscan on-access-policy modify</code>
Attivare un criterio di accesso	<code>vserver vscan on-access-policy enable</code>
Disattiva un criterio di accesso	<code>vserver vscan on-access-policy disable</code>
Eliminare un criterio di accesso	<code>vserver vscan on-access-policy delete</code>
Visualizza riepilogo e dettagli per una policy di accesso	<code>vserver vscan on-access-policy show</code>
Aggiungere all'elenco di percorsi da escludere	<code>vserver vscan on-access-policy paths-to-exclude add</code>
Eliminare dall'elenco dei percorsi da escludere	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
Visualizzare l'elenco dei percorsi da escludere	<code>vserver vscan on-access-policy paths-to-exclude show</code>
Aggiungere all'elenco delle estensioni di file da escludere	<code>vserver vscan on-access-policy file-ext-to-exclude add</code>
Eliminare dall'elenco delle estensioni di file da escludere	<code>vserver vscan on-access-policy file-ext-to-exclude remove</code>
Visualizzare l'elenco delle estensioni di file da escludere	<code>vserver vscan on-access-policy file-ext-to-exclude show</code>
Aggiungere all'elenco delle estensioni di file da includere	<code>vserver vscan on-access-policy file-ext-to-include add</code>

Eliminare dall'elenco delle estensioni di file da includere	<code>vserver vscan on-access-policy file-ext-to-include remove</code>
Visualizzare l'elenco delle estensioni di file da includere	<code>vserver vscan on-access-policy file-ext-to-include show</code>

Per ulteriori informazioni su questi comandi, consulta le pagine man.

## Configurare la scansione on-demand

### Configurare una panoramica della scansione on-demand

È possibile utilizzare la scansione on-demand per controllare i file alla ricerca di virus immediatamente o in base a una pianificazione.

Ad esempio, è possibile eseguire scansioni solo in ore non di punta oppure eseguire la scansione di file di grandi dimensioni esclusi da una scansione all'accesso. È possibile utilizzare una pianificazione cron per specificare quando eseguire l'attività.

#### A proposito di questo argomento

- È possibile assegnare una pianificazione quando si crea un'attività.
- È possibile pianificare una sola attività alla volta su una SVM.
- La scansione on-demand non supporta la scansione di collegamenti simbolici o file di flusso.



La scansione on-demand non supporta la scansione di collegamenti simbolici o file di flusso.



Per creare un'attività on-demand, è necessario abilitare almeno una policy di accesso. Può essere il criterio predefinito o un criterio di accesso creato dall'utente.

### Crea un'attività on-demand

Un'attività su richiesta definisce l'ambito della scansione antivirus su richiesta. È possibile specificare le dimensioni massime dei file da sottoporre a scansione, le estensioni e i percorsi dei file da includere nella scansione e le estensioni e i percorsi dei file da escludere dalla scansione. Per impostazione predefinita, i file nelle sottodirectory vengono sottoposti a scansione.

#### A proposito di questa attività

- È possibile eseguire un massimo di dieci (10) task on-demand per ogni SVM, ma è possibile attivarne solo una.
- Un'attività on-demand crea un report contenente informazioni relative alle statistiche relative alle scansioni. Questo report è accessibile con un comando o scaricando il file di report creato dall'attività nella posizione definita.

#### Prima di iniziare

- Devi avere [creazione di un criterio di accesso](#). Il criterio può essere predefinito o creato dall'utente. Senza il criterio di accesso, non è possibile attivare la scansione.

## Fasi

### 1. Crea un'attività on-demand:

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
-no-ext true|false -directory-recursion true|false
```

- Il `-file-ext-to-exclude` l'impostazione ha la precedenza su `-file-ext-to-include` impostazione.
- Impostare `-scan-files-with-no-ext` a `true` per eseguire la scansione dei file senza estensioni.

Per un elenco completo delle opzioni, consultare la ["riferimento al comando"](#).

Il seguente comando crea un'attività on-demand denominata `Task1` Sulla ``VS1`SVM`:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/", "/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?", "mp*" -file-ext-to-exclude "mp3", "mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+



È possibile utilizzare `job show` per visualizzare lo stato del lavoro. È possibile utilizzare `job pause` e `job resume` comandi per mettere in pausa e riavviare il lavoro o `job stop` per terminare il lavoro.

### 2. Verificare che l'attività on-demand sia stata creata:

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di `Task1` attività:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name Task1
```

```
                Vserver: vs1
                Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
                Report Directory Path: /report
                Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
                File Paths Not to Scan: /vol1/cold-files/
                File Extensions Not to Scan: mp3, mp4
                File Extensions to Scan: vmdk?, mp*
Scan Files with No Extension: false
                Request Service Timeout: 5m
                Cross Junction: true
                Directory Recursion: true
                Scan Priority: low
                Report Log Level: info
                Expiration Time for Report: -
```

### Al termine

Prima di pianificare l'esecuzione dell'operazione, è necessario attivare la scansione sulla SVM.

### Pianificare un'attività on-demand

È possibile creare un'attività senza assegnare una pianificazione e utilizzare `vserver vscan on-demand-task schedule` comando per assegnare un programma o aggiungere un programma durante la creazione dell'attività.

### A proposito di questa attività

La pianificazione assegnata con `vserver vscan on-demand-task schedule` il comando sovrascrive un programma già assegnato con `vserver vscan on-demand-task create` comando.

### Fasi

1. Pianificare un'attività on-demand:

```
vserver vscan on-demand-task schedule -vserver data_SVM -task-name task_name  
-schedule cron_schedule
```

Il seguente comando pianifica un'attività di accesso denominata Task2 su vs2 SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task  
-name Task2 -schedule daily  
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"  
command to view the status.
```

Per visualizzare lo stato del lavoro, utilizzare `job show` comando. Il `job pause` e `job resume` i comandi, rispettivamente mettere in pausa e riavviare il lavoro; la `job stop` il comando termina il lavoro.

## 2. Verificare che l'attività on-demand sia stata pianificata:

```
vserver vscan on-demand-task show -instance data_SVM -task-name task_name
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza i dettagli di Task 2 attività:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name Task2

Vserver: vs2
Task Name: Task2
List of Scan Paths: /vol1/, /vol2/cifs/
Report Directory Path: /report
Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
File Paths Not to Scan: /vol1/cold-files/
File Extensions Not to Scan: mp3, mp4
File Extensions to Scan: vmdk, mp*
Scan Files with No Extension: false
Request Service Timeout: 5m
Cross Junction: true
Directory Recursion: true
Scan Priority: low
Report Log Level: info
```

### Al termine

Prima di pianificare l'esecuzione dell'operazione, è necessario attivare la scansione sulla SVM.

### Eeguire immediatamente un'attività on-demand

È possibile eseguire un'attività on-demand immediatamente, indipendentemente dal fatto che sia stata assegnata o meno una pianificazione.

### Prima di iniziare

È necessario aver attivato la scansione su SVM.

### Fase

#### 1. Eseguire immediatamente un'attività on-demand:

```
vserver vscan on-demand-task run -vserver data_SVM -task-name task_name
```

Il seguente comando esegue un'attività di accesso denominata Task1 su vs1 SVM:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161" command to view the status.
```



È possibile utilizzare `job show` per visualizzare lo stato del lavoro. È possibile utilizzare `job pause` e `job resume` comandi per mettere in pausa e riavviare il lavoro o `job stop` per terminare il lavoro.

## Comandi per la gestione delle attività on-demand

È possibile modificare, eliminare o annullare la pianificazione di un'attività on-demand. È possibile visualizzare un riepilogo e i dettagli dell'attività e gestire i report per l'attività.

Se si desidera...	Immettere il seguente comando...
Crea un'attività on-demand	<code>vserver vscan on-demand-task create</code>
Modificare un'attività on-demand	<code>vserver vscan on-demand-task modify</code>
Eliminare un'attività on-demand	<code>vserver vscan on-demand-task delete</code>
Eseguire un'attività on-demand	<code>vserver vscan on-demand-task run</code>
Pianificare un'attività on-demand	<code>vserver vscan on-demand-task schedule</code>
Annulla pianificazione di un'attività on-demand	<code>vserver vscan on-demand-task unschedule</code>
Visualizza riepilogo e dettagli per un'attività on-demand	<code>vserver vscan on-demand-task show</code>
Visualizza report on-demand	<code>vserver vscan on-demand-task report show</code>
Elimina i report on-demand	<code>vserver vscan on-demand-task report delete</code>

Per ulteriori informazioni su questi comandi, consulta le pagine man.

## Procedure consigliate per la configurazione della funzionalità antivirus off-box in ONTAP

Prendere in considerazione i seguenti consigli per configurare la funzionalità off-box in ONTAP.

- Limitare gli utenti con privilegi alle operazioni di scansione antivirus. Gli utenti normali devono essere scoraggiati dall'utilizzo di credenziali utente con privilegi. Questa restrizione può essere ottenuta disattivando i diritti di accesso per gli utenti con privilegi in Active Directory.
- Gli utenti con privilegi non devono far parte di alcun gruppo di utenti con un elevato numero di diritti nel dominio, ad esempio il gruppo Administrators o il gruppo di operatori di backup. Gli utenti con privilegi devono essere convalidati solo dal sistema di archiviazione in modo che possano creare connessioni al server Vscan e accedere ai file per la scansione antivirus.
- Utilizzare i computer su cui sono in esecuzione i server Vscan solo a scopo di scansione antivirus. Per scoraggiare l'uso generale, disattivare i servizi terminal di Windows e altre disposizioni di accesso remoto su questi computer e concedere il diritto di installare nuovo software su questi computer solo agli amministratori.
- Dedicare i server Vscan alla scansione antivirus e non utilizzarli per altre operazioni, ad esempio i backup. Si potrebbe decidere di eseguire il server Vscan come macchina virtuale (VM). Se si esegue il server Vscan come macchina virtuale, assicurarsi che le risorse assegnate alla macchina virtuale non siano condivise e siano sufficienti per eseguire la scansione antivirus.
- Fornire CPU, memoria e capacità del disco adeguate al server Vscan per evitare un'allocazione eccessiva delle risorse. La maggior parte dei server Vscan è progettata per utilizzare più server core CPU e per distribuire il carico tra le CPU.
- NetApp consiglia di utilizzare una rete dedicata con una VLAN privata per la connessione dalla SVM al server Vscan, in modo che il traffico di scansione non sia influenzato da altro traffico di rete client. Creare una scheda di interfaccia di rete (NIC) separata dedicata alla VLAN antivirus sul server Vscan e alla LIF dati sulla SVM. Questo passaggio semplifica l'amministrazione e la risoluzione dei problemi in caso di problemi di rete. Il traffico antivirus deve essere segregato utilizzando una rete privata. Il server antivirus deve essere configurato per comunicare con il controller di dominio (DC) e ONTAP in uno dei seguenti modi:
  - Il controller di dominio deve comunicare con i server antivirus tramite la rete privata utilizzata per separare il traffico.
  - Il DC e il server antivirus devono comunicare attraverso una rete diversa (non la rete privata menzionata in precedenza), che non è la stessa della rete client CIFS.
  - Per attivare l'autenticazione Kerberos per la comunicazione antivirus, creare una voce DNS per la LIF privata e un nome dell'entità di servizio sul controller di dominio corrispondente alla voce DNS creata per la LIF privata. Usare questo nome quando si aggiunge una LIF al connettore antivirus. Il DNS dovrebbe essere in grado di restituire un nome univoco per ogni LIF privato collegato al connettore antivirus.



Se la LIF per il traffico Vscan è configurata su una porta diversa dalla LIF per il traffico client, in caso di guasto a una porta la LIF Vscan potrebbe essere sottoposta a failover su un altro nodo. La modifica rende il server Vscan non raggiungibile dal nuovo nodo e le notifiche di scansione per le operazioni sui file sul nodo non riescono. Verificare che il server Vscan sia raggiungibile tramite almeno una LIF su un nodo in modo da poter elaborare le richieste di scansione per le operazioni su file eseguite su quel nodo.

- Collegare il sistema storage NetApp e il server Vscan utilizzando almeno una rete 1GbE.
- Per un ambiente con più server Vscan, collegare tutti i server con connessioni di rete simili ad alte prestazioni. La connessione dei server Vscan migliora le performance consentendo la condivisione del carico.
- Per i siti remoti e le filiali, NetApp consiglia di utilizzare un server Vscan locale piuttosto che un server Vscan remoto, poiché il primo è il candidato ideale per ottenere una latenza elevata. Se il costo è un fattore, utilizzare un notebook o un PC per una protezione antivirus moderata. È possibile pianificare

scansioni periodiche e complete del file system condividendo i volumi o i qtree ed eseguendone la scansione da qualsiasi sistema del sito remoto.

- Utilizzare più server Vscan per eseguire la scansione dei dati sulla SVM a scopo di bilanciamento del carico e ridondanza. La quantità di carico di lavoro CIFS e il conseguente traffico antivirus varia in base alla SVM. Monitorare la latenza di scansione virus e CIFS sullo storage controller. Monitorare l'andamento dei risultati nel tempo. Se la latenza CIFS e la latenza della scansione virus aumentano a causa delle code della CPU o delle applicazioni sui server Vscan oltre le soglie di trend, i client CIFS potrebbero riscontrare lunghi tempi di attesa. Aggiungere altri server Vscan per distribuire il carico.
- Installare la versione più recente del connettore antivirus ONTAP.
- Mantenere aggiornati i motori e le definizioni antivirus. Consulta i partner per consigli sulla frequenza di aggiornamento.
- In un ambiente multi-tenancy, è possibile condividere un pool di scanner (pool di server Vscan) con più SVM, a condizione che i server Vscan e le SVM facciano parte dello stesso dominio o dominio attendibile.
- Il criterio del software antivirus per i file infetti deve essere impostato su "elimina" o "quarantena", che è il valore predefinito impostato dalla maggior parte dei fornitori di antivirus. Se "vscan-fileop-profile" è impostato su "write\_only" e se viene trovato un file infetto, il file rimane nella condivisione e può essere aperto perché l'apertura di un file non attiva una scansione. La scansione antivirus viene attivata solo dopo la chiusura del file.
- Il `scan-engine timeout` il valore deve essere inferiore a `scanner-pool request-timeout` valore. Se è impostato su un valore più alto, l'accesso ai file potrebbe subire un ritardo e alla fine potrebbe scadere.  
Per evitare questo problema, configurare `scan-engine timeout` a 5 secondi in meno di `scanner-pool request-timeout` valore. Fare riferimento alla documentazione del fornitore del motore di scansione per le istruzioni su come cambiare `scan-engine timeout` impostazioni. Il `scanner-pool timeout` può essere modificato utilizzando il seguente comando in modalità avanzata e fornendo il valore appropriato per `request-timeout` parametro:  
`vserver vscan scanner-pool modify.`
- Per un ambiente dimensionato per i carichi di lavoro di scansione ad accesso e che richiede l'utilizzo di una scansione su richiesta, NetApp consiglia di pianificare il lavoro di scansione su richiesta in orari non di punta per evitare carichi aggiuntivi sull'infrastruttura antivirus esistente.

Scopri di più sulle Best practice specifiche per i partner all'indirizzo ["Soluzioni partner di Vscan"](#).

## Abilitare la scansione virus su una SVM

È necessario attivare la scansione virus su una SVM prima di eseguire una scansione on-access o on-demand.

### Fasi

1. Abilitare la scansione virus su una SVM:

```
vserver vscan enable -vserver data_SVM
```



È possibile utilizzare `vserver vscan disable` comando per disattivare la scansione virus, se necessario.

Il seguente comando attiva la scansione virus su `vs1` SVM:



```
cluster1::> vserver vscan enable -vserver vs1
```

## 2. Verificare che la scansione virus sia attivata su SVM:

```
vserver vscan show -vserver data_SVM
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando visualizza lo stato Vscan di vs1 SVM:

```
cluster1::> vserver vscan show -vserver vs1
```

```
Vserver: vs1  
Vscan Status: on
```

## Ripristinare lo stato dei file sottoposti a scansione

Talvolta, è possibile ripristinare lo stato di scansione dei file sottoposti a scansione su una SVM utilizzando `vserver vscan reset` per eliminare le informazioni memorizzate nella cache per i file. È possibile utilizzare questo comando per riavviare l'elaborazione della scansione virus, ad esempio in caso di una scansione non configurata correttamente.

### A proposito di questa attività

Dopo aver eseguito il `vserver vscan reset` comando, tutti i file idonei verranno sottoposti a scansione al successivo accesso.



Questo comando può influire negativamente sulle prestazioni, a seconda del numero e delle dimensioni dei file da ripetere.

### Di cosa hai bisogno

Per questa attività sono richiesti privilegi avanzati.

### Fasi

#### 1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

#### 2. Ripristinare lo stato dei file sottoposti a scansione:

```
vserver vscan reset -vserver data_SVM
```

Il seguente comando ripristina lo stato dei file sottoposti a scansione su vs1 SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

## Visualizzare le informazioni del registro eventi di Vscan

È possibile utilizzare `vserver vscan show-events` Comando per visualizzare le informazioni del registro eventi relative ai file infetti, agli aggiornamenti dei server Vscan e simili. È possibile visualizzare le informazioni sugli eventi per il cluster o per dati nodi, SVM o server Vscan.

### Prima di iniziare

Per visualizzare il registro eventi Vscan sono necessari privilegi avanzati.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Visualizzare le informazioni del registro eventi di Vscan:

```
vserver vscan show-events
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il comando seguente visualizza le informazioni del registro eventi per il cluster `cluster1`:

```
cluster1::*> vserver vscan show-events
```

Vserver	Node	Server	Event Type	Event Time
-----	-----	-----	-----	
vs1	Cluster-01	192.168.1.1	file-infected	9/5/2014 11:37:38
vs1	Cluster-01	192.168.1.1	scanner-updated	9/5/2014 11:37:08
vs1	Cluster-01	192.168.1.1	scanner-connected	9/5/2014 11:34:55
3 entries were displayed.				

## Monitoraggio e risoluzione dei problemi di connettività

### Potenziati problemi di connettività che coinvolgono l'opzione di scansione obbligatoria

È possibile utilizzare `vserver vscan connection-status show` Comandi per visualizzare informazioni sulle connessioni del server Vscan che potrebbero essere utili per la risoluzione dei problemi di connettività.

Per impostazione predefinita, il `scan-mandatory` L'opzione per la scansione all'accesso nega l'accesso ai file quando non è disponibile una connessione al server Vscan per la scansione. Sebbene questa opzione offra importanti funzioni di sicurezza, può causare problemi in alcune situazioni.

- Prima di abilitare l'accesso client, è necessario assicurarsi che almeno un server Vscan sia connesso a una SVM su ciascun nodo che dispone di una LIF. Se è necessario connettere i server alle SVM dopo aver attivato l'accesso client, è necessario disattivare `scan-mandatory` Opzione su SVM per garantire che l'accesso al file non venga negato perché non è disponibile una connessione al server Vscan. È possibile riattivare l'opzione dopo aver collegato il server.
- Se una LIF di destinazione ospita tutte le connessioni del server Vscan per una SVM, la connessione tra il server e la SVM andrà persa se la LIF viene migrata. Per garantire che l'accesso al file non venga negato perché non è disponibile una connessione al server Vscan, è necessario disattivare `scan-mandatory` Prima di migrare LIF. È possibile riattivare l'opzione dopo la migrazione del LIF.

A ciascuna SVM devono essere assegnati almeno due server Vscan. Si consiglia di collegare i server Vscan al sistema storage su una rete diversa da quella utilizzata per l'accesso client.

## Comandi per visualizzare lo stato di connessione del server Vscan

È possibile utilizzare `vserver vscan connection-status show` Comandi per visualizzare informazioni riepilogative e dettagliate sullo stato di connessione del server Vscan.

Se si desidera...	Immettere il seguente comando...
Visualizza un riepilogo delle connessioni del server Vscan	<code>vserver vscan connection-status show</code>
Visualizza i dettagli delle connessioni al server Vscan	<code>vserver vscan connection-status show-all</code>
Visualizza i dettagli dei server Vscan connessi	<code>vserver vscan connection-status show-connected</code>
Visualizza i dettagli dei server Vscan disponibili non connessi	<code>vserver vscan connection-status show-not-connected</code>

Per ulteriori informazioni su questi comandi, consultare la ["Pagine man di ONTAP"](#).

## Risolvere i problemi relativi alla scansione antivirus

Per i problemi più comuni di scansione dei virus, esistono possibili cause e modi per risolverli. La scansione dei virus è nota anche come Vscan.

Problema	Come risolverlo
----------	-----------------

I server Vscan non sono in grado di connettersi a. Il sistema storage Clustered ONTAP.	Verificare se la configurazione del pool di scanner specifica l'indirizzo IP del server Vscan. Controllare inoltre se gli utenti con privilegi consentiti nell'elenco dei pool di scanner sono attivi. Per controllare il pool di scanner, eseguire <code>vserver vscan scanner-pool show</code> al prompt dei comandi del sistema di storage. Se i server Vscan non riescono ancora a connettersi, potrebbe esserci un problema di rete.
I client osservano una latenza elevata.	È probabilmente giunto il momento di aggiungere altri server Vscan al pool di scanner.
Troppe scansioni attivate.	Modificare il valore di <code>vscan-fileop-profile</code> parametro per limitare il numero di operazioni sui file monitorate per la scansione antivirus.
Alcuni file non vengono sottoposti a scansione.	Verificare la policy di accesso. È possibile che il percorso di questi file sia stato aggiunto all'elenco di esclusione del percorso o che la loro dimensione superi il valore configurato per le esclusioni. Per verificare il criterio di accesso, eseguire <code>vserver vscan on-access-policy show</code> al prompt dei comandi del sistema di storage.
Accesso al file negato.	Controllare se l'impostazione <i>scan-Mandatory</i> è specificata nella configurazione dei criteri. Questa impostazione nega l'accesso ai dati se non sono connessi server Vscan. Modificare l'impostazione come necessario.

## Monitorare lo stato e le attività delle performance

È possibile monitorare gli aspetti critici del modulo Vscan, ad esempio lo stato di connessione del server Vscan, Lo stato dei server Vscan e il numero di file sottoposti a scansione. Queste informazioni sono utili Si diagnosticano i problemi relativi al server Vscan.

### Visualizzare le informazioni di connessione del server Vscan

È possibile visualizzare lo stato di connessione dei server Vscan per gestire le connessioni già in uso e le connessioni disponibili per l'utilizzo. I vari comandi visualizzano informazioni Informazioni sullo stato di connessione dei server Vscan.

Comando...	Informazioni visualizzate...
<code>vserver vscan connection-status show</code>	Riepilogo dello stato della connessione

<code>vserver vscan connection-status show-all</code>	Informazioni dettagliate sullo stato della connessione
<code>vserver vscan connection-status show-not-connected</code>	Stato delle connessioni disponibili ma non connesse
<code>vserver vscan connection-status show-connected</code>	Informazioni sul server Vscan collegato

Per ulteriori informazioni su questi comandi, consultare la ["pagine man"](#).

### Visualizzare le statistiche del server Vscan

È possibile visualizzare le statistiche specifiche del server Vscan per monitorare le prestazioni e diagnosticare i problemi relativi a.

scansione virus. È necessario raccogliere un campione di dati prima di poter utilizzare `statistics show` comando a.

Visualizzare le statistiche del server Vscan.

Per completare un campione di dati, completare la seguente fase:

#### Fase

1. Eseguire `statistics start` e il `optional statistics` comando di arresto.

### Visualizzare le statistiche per le richieste e le latenze del server Vscan

È possibile utilizzare `ONTAP offbox_vscan` Contatori per SVM per monitorare la velocità di Vscan

Le richieste del server inviate e ricevute al secondo e le latenze del server in tutte le Vscan server. Per visualizzare queste statistiche, completare la seguente fase:

#### Fase

1. Eseguire la visualizzazione delle statistiche `object offbox_vscan -instance SVM` con il contatori seguenti:

Contatore...	Informazioni visualizzate...
<code>scan_request_dispatched_rate</code>	Numero di richieste di scansione virus inviate da ONTAP ai server Vscan al secondo
<code>scan_noti_received_rate</code>	Numero di richieste di scansione virus ricevute da ONTAP dai server Vscan al secondo
<code>dispatch_latency</code>	Latenza all'interno di ONTAP per identificare un server Vscan disponibile e inviare la richiesta a tale server Vscan
<code>scan_latency</code>	Latenza di andata e ritorno da ONTAP al server Vscan, compreso il tempo di esecuzione della scansione

Esempio di statistiche generate da un contatore vscan ONTAP offbox

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-----
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-----
```

Visualizzare le statistiche per le singole richieste e latenze del server Vscan

È possibile utilizzare ONTAP offbox\_vscan\_server Contatori su un server Vscan per-SVM, per-off-box, E per nodo per monitorare il tasso di richieste del server Vscan inviate e la latenza del server su Ciascun server Vscan singolarmente. Per raccogliere queste informazioni, completare la seguente fase:

Fase

- 1. Eseguire `statistics show -object offbox_vscan -instance SVM:servername:nodename` comando con i seguenti contatori:

Contatore...	Informazioni visualizzate...
scan_request_dispatched_rate	Numero di richieste di scansione virus inviate da ONTAP
scan_latency	Latenza di andata e ritorno da ONTAP al server Vscan, compreso il tempo di esecuzione della scansione Ai server Vscan al secondo

Esempio di statistiche generate da un contatore ONTAP offbox\_vscan\_server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
```

```
-----
scan_request_dispatched_rate 291
scan_latency 3433830us
-----
```

## Visualizzare le statistiche per l'utilizzo del server Vscan

È anche possibile utilizzare ONTAP `offbox_vscan_server` Contatori per raccogliere l'utilizzo del server Vscan

statistiche. Queste statistiche vengono monitorate per SVM, per server Vscan off-box e per nodo. Loro Includere l'utilizzo della CPU sul server Vscan, la profondità della coda per le operazioni di scansione sul server Vscan

(corrente e massima), memoria utilizzata e rete utilizzata.

Queste statistiche vengono inoltrate dal connettore antivirus ai contatori delle statistiche all'interno di ONTAP. Loro

sono basati su dati che vengono interrogati ogni 20 secondi e devono essere raccolti più volte per la precisione;

in caso contrario, i valori visualizzati nelle statistiche riflettono solo l'ultimo polling. L'utilizzo della CPU e le code sono

particolarmente importante per il monitoraggio e l'analisi. Un valore elevato per una coda media può indicare che

Il server Vscan presenta un collo di bottiglia.

Per raccogliere le statistiche di utilizzo per il server Vscan su un server Vscan per SVM, per server Vscan e per nodo

di base, completare il seguente passaggio:

### Fase

1. Raccogliere le statistiche di utilizzo per il server Vscan

Eseguire `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` con i seguenti comandi `offbox_vscan_server` contatori:

Contatore...	Informazioni visualizzate...
<code>scanner_stats_pct_cpu_used</code>	Utilizzo della CPU sul server Vscan
<code>scanner_stats_pct_input_queue_avg</code>	Coda media di richieste di scansione sul server Vscan
<code>scanner_stats_pct_input_queue_hiwatemark</code>	Coda di picco delle richieste di scansione sul server Vscan

scanner_stats_pct_mem_used	Memoria utilizzata sul server Vscan
scanner_stats_pct_network_used	Rete utilizzata sul server Vscan

### Esempio di statistiche di utilizzo per il server Vscan

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-----
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
-----
```

## Audit degli eventi NAS su SVM

### Controllo SMB e NFS e tracciamento della sicurezza

È possibile utilizzare le funzionalità di controllo dell'accesso ai file disponibili per i protocolli SMB e NFS con ONTAP, come il controllo nativo e la gestione dei criteri dei file utilizzando FPolicy.

È necessario progettare e implementare il controllo degli eventi di accesso ai file SMB e NFS nei seguenti casi:

- È stato configurato l'accesso di base ai file dei protocolli SMB e NFS.
- Si desidera creare e gestire una configurazione di controllo utilizzando uno dei seguenti metodi:
  - Funzionalità ONTAP nativa
  - Server FPolicy esterni

### Audit degli eventi NAS su SVM

Il controllo degli eventi NAS è una misura di sicurezza che consente di tenere traccia e registrare determinati eventi SMB e NFS sulle macchine virtuali di storage (SVM). In questo modo è possibile tenere traccia dei potenziali problemi di sicurezza e fornire prove di eventuali violazioni della sicurezza. È inoltre possibile organizzare e controllare le policy di accesso centrale di Active Directory per verificare il risultato dell'implementazione.



## Eventi SMB

È possibile controllare i seguenti eventi:

- Eventi di accesso a file e cartelle SMB

È possibile controllare gli eventi di accesso a file e cartelle SMB sugli oggetti memorizzati nei volumi FlexVol appartenenti alle SVM abilitate per l'auditing.

- Eventi di logon e logoff SMB

È possibile controllare gli eventi di logon e logoff SMB per i server SMB sulle SVM.

- Eventi di staging dei criteri di accesso centrale

È possibile controllare l'accesso effettivo degli oggetti sui server SMB utilizzando le autorizzazioni applicate attraverso le policy di accesso centrale proposte. Il controllo attraverso lo staging delle policy di accesso centrale consente di verificare gli effetti delle policy di accesso centrale prima che vengano implementate.

Il controllo dello staging dei criteri di accesso centrale viene impostato utilizzando gli oggetti Criteri di gruppo di Active Directory; tuttavia, la configurazione di controllo SVM deve essere configurata per controllare gli eventi di staging dei criteri di accesso centrale.

Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, gli eventi di staging dei criteri di accesso centrale vengono generati solo se è attivato il controllo dinamico degli accessi. Il controllo dinamico degli accessi viene attivato tramite un'opzione server SMB. Non è attivato per impostazione predefinita.

## Eventi NFS

È possibile controllare gli eventi di file e directory utilizzando ACL NFSv4 sugli oggetti memorizzati sulle SVM.

## Come funziona il controllo

### Concetti di controllo di base

Per comprendere il controllo in ONTAP, è necessario conoscere alcuni concetti di base relativi al controllo.

- **File di staging**

I file binari intermedi sui singoli nodi in cui vengono memorizzati i record di audit prima del consolidamento e della conversione. I file di staging sono contenuti nei volumi di staging.

- **Volume di staging**

Un volume dedicato creato da ONTAP per memorizzare i file di staging. Esiste un volume di staging per aggregato. I volumi di staging sono condivisi da tutte le SVM (Storage Virtual Machine) abilitate all'audit per memorizzare i record di audit dell'accesso ai dati per i volumi di dati in quel particolare aggregato. I record di audit di ogni SVM sono memorizzati in una directory separata all'interno del volume di staging.

Gli amministratori dei cluster possono visualizzare informazioni sui volumi di staging, ma la maggior parte delle altre operazioni sui volumi non è consentita. Solo ONTAP può creare volumi di staging. ONTAP assegna automaticamente un nome ai volumi di staging. Tutti i nomi dei volumi di staging iniziano con

MDV\_aud\_ Seguito dall'UUID dell'aggregato contenente il volume di staging (ad esempio:  
MDV\_aud\_1d0131843d4811e296fc123478563412.)

- **Volumi di sistema**

Volume FlexVol contenente metadati speciali, ad esempio metadati per i log di audit dei servizi file. La SVM amministrativa possiede i volumi di sistema, visibili all'interno del cluster. I volumi di staging sono un tipo di volume di sistema.

- **Attività di consolidamento**

Un'attività che viene creata quando viene attivato il controllo. Questa attività a esecuzione prolungata su ogni SVM prende i record di audit dai file di staging attraverso i nodi membri della SVM. Questa attività unisce i record di audit in ordine cronologico ordinato, quindi li converte in un formato di registro eventi leggibile dall'utente specificato nella configurazione di controllo, ovvero IL formato DI file EVTX o XML. I registri eventi convertiti vengono memorizzati nella directory del registro eventi di controllo specificata nella configurazione di controllo SVM.

## **Come funziona il processo di audit di ONTAP**

Il processo di controllo di ONTAP è diverso dal processo di controllo di Microsoft. Prima di configurare il controllo, è necessario comprendere il funzionamento del processo di controllo di ONTAP.

I record di audit vengono inizialmente memorizzati in file di staging binari su singoli nodi. Se il controllo è attivato su una SVM, ogni nodo membro mantiene i file di staging per tale SVM. Periodicamente, vengono consolidati e convertiti in registri eventi leggibili dall'utente, memorizzati nella directory del registro eventi di controllo per SVM.

### **Processo quando il controllo è attivato su una SVM**

Il controllo può essere attivato solo sulle SVM. Quando l'amministratore dello storage abilita il controllo sulla SVM, il sottosistema di controllo verifica se sono presenti volumi di staging. Per ogni aggregato che contiene volumi di dati di proprietà di SVM deve esistere un volume di staging. Il sottosistema di auditing crea tutti i volumi di staging necessari, se non esistono.

Il sottosistema di auditing completa anche altre attività prerequisite prima che sia attivato il controllo:

- Il sottosistema di controllo verifica che il percorso della directory di log sia disponibile e non contenga symlink.

La directory di log deve già esistere come percorso all'interno dello spazio dei nomi SVM. Si consiglia di creare un nuovo volume o qtree per contenere i file di log dell'audit. Il sottosistema di controllo non assegna una posizione predefinita per il file di log. Se il percorso della directory di log specificato nella configurazione di controllo non è un percorso valido, il controllo della creazione della configurazione non riesce con `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name" errore.`

La creazione della configurazione non riesce se la directory esiste ma contiene collegamenti simbolici.

- Il controllo pianifica l'attività di consolidamento.

Una volta pianificata questa attività, viene attivato il controllo. La configurazione di controllo SVM e i file di log rimangono durante un riavvio o se i server NFS o SMB vengono arrestati o riavviati.

## Consolidamento del registro eventi

Il consolidamento dei log è un'attività pianificata che viene eseguita di routine fino alla disattivazione del controllo. Quando il controllo è disattivato, l'attività di consolidamento verifica che tutti i log rimanenti siano consolidati.

### Auditing garantito

Per impostazione predefinita, il controllo è garantito. ONTAP garantisce la registrazione di tutti gli eventi di accesso ai file verificabili (come specificato dagli ACL dei criteri di controllo configurati), anche se un nodo non è disponibile. Un'operazione di file richiesta non può essere completata fino a quando il record di audit per tale operazione non viene salvato nel volume di staging sullo storage persistente. Se non è possibile eseguire il commit dei record di audit sul disco nei file di staging, a causa di spazio insufficiente o a causa di altri problemi, le operazioni del client vengono negate.



Un amministratore, o un utente di account con accesso a livello di privilegio, può ignorare l'operazione di registrazione dell'audit del file utilizzando NetApp Manageability SDK o API REST. È possibile determinare se sono state eseguite azioni sui file utilizzando NetApp Manageability SDK o API REST esaminando i log della cronologia dei comandi memorizzati in `audit.log` file.

Per ulteriori informazioni sui registri di audit della cronologia dei comandi, vedere la sezione "Gestione della registrazione dell'audit per le attività di gestione" in ["Amministrazione del sistema"](#).

### Processo di consolidamento quando un nodo non è disponibile

Se un nodo contenente volumi appartenenti a una SVM con il controllo attivato non è disponibile, il comportamento dell'attività di consolidamento del controllo dipende dalla disponibilità del partner di storage failover (SFO) del nodo (o del partner ha nel caso di un cluster a due nodi):

- Se il volume di staging è disponibile tramite il partner SFO, l'ultima scansione dei volumi di staging segnalati dal nodo viene eseguita e il consolidamento procede normalmente.
- Se il partner SFO non è disponibile, l'attività crea un file di log parziale.

Quando un nodo non è raggiungibile, l'attività di consolidamento consolida i record di audit degli altri nodi disponibili di tale SVM. Per identificare che non è completo, l'attività aggiunge il suffisso `.partial` al nome del file consolidato.

- Una volta disponibile il nodo non disponibile, i record di audit in quel nodo vengono consolidati con i record di audit degli altri nodi in quel momento.
- Tutti i record di audit vengono conservati.

### Rotazione del registro eventi

I file di log degli eventi di audit vengono ruotati quando raggiungono una dimensione di log di soglia configurata o in base a una pianificazione configurata. Quando un file di registro eventi viene ruotato, l'attività di consolidamento pianificata rinomina prima il file convertito attivo in un file di archivio con data e ora, quindi crea un nuovo file di registro eventi convertito attivo.

### Processo quando il controllo è disattivato su SVM

Quando il controllo viene disattivato sulla SVM, l'attività di consolidamento viene attivata una volta finale. Tutti i record di audit registrati in sospeso vengono registrati in un formato leggibile dall'utente. I registri eventi

esistenti memorizzati nella directory del registro eventi non vengono cancellati quando il controllo viene disattivato sulla SVM e sono disponibili per la visualizzazione.

Una volta consolidati tutti i file di staging esistenti per la SVM, l'attività di consolidamento viene rimossa dalla pianificazione. La disattivazione della configurazione di controllo per SVM non rimuove la configurazione di controllo. Un amministratore dello storage può riabilitare il controllo in qualsiasi momento.

Il processo di consolidamento di controllo, creato quando viene attivato il controllo, monitora l'attività di consolidamento e la ricrea se l'attività di consolidamento viene chiusa a causa di un errore. Gli utenti non possono eliminare il processo di consolidamento del controllo.

## Requisiti e considerazioni per il controllo

Prima di configurare e abilitare l'auditing sulla macchina virtuale di storage (SVM), è necessario essere a conoscenza di determinati requisiti e considerazioni.

- Il numero massimo di SVM abilitate all'audit supportate dipende dalla versione di ONTAP in uso:

Versione di ONTAP	Massimo
9,8 e precedenti	50
9.9.1 e versioni successive	400

- Il controllo non è legato alle licenze SMB o NFS.

È possibile configurare e abilitare il controllo anche se le licenze SMB e NFS non sono installate nel cluster.

- Il controllo NFS supporta ACE di sicurezza (tipo U).
- Per il controllo NFS, non esiste alcuna mappatura tra i bit di modalità e le ACE di controllo.

Quando si convertono gli ACL in bit di modalità, gli ACE di controllo vengono ignorati. Quando si convertono i bit di modalità in ACL, non vengono generati ACE di controllo.

- La directory specificata nella configurazione di controllo deve esistere.

Se non esiste, il comando per creare la configurazione di controllo non riesce.

- La directory specificata nella configurazione di controllo deve soddisfare i seguenti requisiti:
  - La directory non deve contenere collegamenti simbolici.

Se la directory specificata nella configurazione di controllo contiene collegamenti simbolici, il comando per creare la configurazione di controllo non riesce.

- Specificare la directory utilizzando un percorso assoluto.

Non specificare un percorso relativo, ad esempio `/vs1/././`.

- Il controllo dipende dalla disponibilità di spazio nei volumi di staging.

È necessario conoscere e disporre di un piano per garantire che vi sia spazio sufficiente per i volumi di staging negli aggregati che contengono volumi sottoposti a audit.

- Il controllo dipende dalla disponibilità di spazio nel volume contenente la directory in cui sono memorizzati i registri degli eventi convertiti.

È necessario conoscere e disporre di un piano per garantire che vi sia spazio sufficiente nei volumi utilizzati per memorizzare i registri degli eventi. È possibile specificare il numero di registri eventi da conservare nella directory di controllo utilizzando `-rotate-limit` parametro durante la creazione di una configurazione di controllo, che può aiutare a garantire che vi sia spazio disponibile sufficiente per i registri degli eventi nel volume.

- Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, il controllo dinamico degli accessi deve essere abilitato per generare eventi di staging dei criteri di accesso centrale.

Dynamic Access Control non è attivato per impostazione predefinita.

### **Aggregare le considerazioni sullo spazio quando si abilita il controllo**

Quando viene creata una configurazione di audit e viene attivato il controllo su almeno una macchina virtuale di storage (SVM) nel cluster, il sottosistema di audit crea volumi di staging su tutti gli aggregati esistenti e su tutti i nuovi aggregati creati. Quando si abilita il controllo sul cluster, è necessario tenere conto di alcune considerazioni relative allo spazio aggregato.

La creazione del volume di staging potrebbe non riuscire a causa della non disponibilità di spazio in un aggregato. Questo potrebbe verificarsi se si crea una configurazione di controllo e gli aggregati esistenti non dispongono di spazio sufficiente per contenere il volume di staging.

Prima di attivare il controllo su una SVM, è necessario assicurarsi che vi sia spazio sufficiente sugli aggregati esistenti per i volumi di staging.

### **Limiti per la dimensione dei record di audit sui file di staging**

La dimensione di un record di audit in un file di staging non può essere superiore a 32 KB.

### **Quando possono verificarsi record di audit di grandi dimensioni**

Durante il controllo della gestione potrebbero verificarsi record di audit di grandi dimensioni in uno dei seguenti scenari:

- Aggiunta o eliminazione di utenti a o da gruppi con un elevato numero di utenti.
- Aggiunta o eliminazione di un elenco di controllo di accesso (ACL) per la condivisione di file con un gran numero di utenti per la condivisione di file.
- Altri scenari.

Disattivare il controllo di gestione per evitare questo problema. A tale scopo, modificare la configurazione dell'audit e rimuovere quanto segue dall'elenco dei tipi di eventi di audit:

- condivisione file
- account utente
- security-group
- authorization-policy-change

Dopo la rimozione, non verranno controllati dal sottosistema di controllo dei file Services.

## Gli effetti di record di audit troppo grandi

- Se la dimensione di un record di audit è troppo grande (oltre 32 KB), il record di audit non viene creato e il sottosistema di audit genera un messaggio EMS (Event Management System) simile a quanto segue:

```
File Services Auditing subsystem failed the operation or truncated an audit
record because it was greater than max_audit_record_size value. Vserver
UUID=%s, event_id=%u, size=%u
```

Se il controllo è garantito, l'operazione del file non riesce perché non è possibile creare il relativo record di audit.

- Se la dimensione del record di audit è superiore a 9,999 byte, viene visualizzato lo stesso messaggio EMS riportato sopra. Viene creato un record di audit parziale con il valore chiave più grande mancante.
- Se il record di audit supera i 2,000 caratteri, viene visualizzato il seguente messaggio di errore anziché il valore effettivo:

```
The value of this field was too long to display.
```

## Quali sono i formati di registro eventi di audit supportati

I formati di file supportati per i registri degli eventi di audit convertiti sono EVTX e XML formati di file.

È possibile specificare il tipo di formato del file quando si crea la configurazione di controllo. Per impostazione predefinita, ONTAP converte i registri binari in EVTX formato del file.

## Visualizzare i registri degli eventi di audit

È possibile utilizzare i registri degli eventi di audit per determinare se si dispone di una protezione dei file adeguata e se si sono verificati tentativi di accesso a file e cartelle non corretti. È possibile visualizzare ed elaborare i registri degli eventi di audit salvati in EVTX oppure XML formati di file.

- EVTX formato del file

È possibile aprire il file convertito EVTX Controllare i log degli eventi come file salvati utilizzando Microsoft Event Viewer.

È possibile utilizzare due opzioni per la visualizzazione dei registri eventi mediante il Visualizzatore eventi:

- Vista generale

Le informazioni comuni a tutti gli eventi vengono visualizzate per il record dell'evento. In questa versione di ONTAP, i dati specifici dell'evento per il record dell'evento non vengono visualizzati. È possibile utilizzare la vista dettagliata per visualizzare i dati specifici dell'evento.

- Vista dettagliata

Sono disponibili una vista intuitiva e una vista XML. La visualizzazione semplice e la visualizzazione XML visualizzano sia le informazioni comuni a tutti gli eventi che i dati specifici dell'evento per il record dell'evento.

- XML formato del file

È possibile visualizzare ed elaborare XML registri degli eventi di audit su applicazioni di terze parti che supportano XML formato del file. È possibile utilizzare gli strumenti di visualizzazione XML per visualizzare i registri di controllo, a condizione che si disponga dello schema XML e delle informazioni sulle definizioni dei campi XML. Per ulteriori informazioni sullo schema e sulle definizioni XML, vedere ["Riferimento allo schema di controllo ONTAP"](#).

## Visualizzazione dei registri di controllo attivi mediante Event Viewer

Se il processo di consolidamento dell'audit è in esecuzione sul cluster, il processo di consolidamento aggiunge nuovi record al file di log dell'audit attivo per le macchine virtuali dello storage abilitate all'audit (SVM). È possibile accedere a questo registro di controllo attivo e aprirlo tramite una condivisione SMB in Microsoft Event Viewer.

Oltre a visualizzare i record di audit esistenti, Event Viewer offre un'opzione di refresh che consente di aggiornare il contenuto nella finestra della console. La possibilità di visualizzare i nuovi registri aggiunti nel Visualizzatore eventi dipende dall'attivazione o meno degli oplock nella condivisione utilizzata per accedere al registro di controllo attivo.

Impostazione degli oplock sulla condivisione	Comportamento
Attivato	Event Viewer apre il registro contenente gli eventi scritti fino a quel momento. L'operazione di refresh non aggiorna il log con nuovi eventi aggiunti dal processo di consolidamento.
Disattivato	Event Viewer apre il registro contenente gli eventi scritti fino a quel momento. L'operazione di refresh aggiorna il log con nuovi eventi aggiunti dal processo di consolidamento.



Queste informazioni sono valide solo per EVTX registri eventi. XML I registri degli eventi possono essere visualizzati tramite SMB in un browser o NFS utilizzando qualsiasi editor o visualizzatore XML.

## Eventi SMB che possono essere verificati

### Panoramica degli eventi SMB che è possibile verificare

ONTAP può controllare alcuni eventi SMB, inclusi determinati eventi di accesso a file e cartelle, determinati eventi di accesso e disconnessione ed eventi di staging dei criteri di accesso centrale. Sapere quali eventi di accesso è possibile verificare è utile quando si interpretano i risultati dei registri eventi.

I seguenti eventi SMB aggiuntivi possono essere verificati in ONTAP 9.2 e versioni successive:

ID EVENTO (EVT/EVTX)	Evento	Descrizione	Categoria
4670	Le autorizzazioni degli oggetti sono state modificate	OBJECT ACCESS (ACCESSO A OGGETTI): Autorizzazioni modificate.	Accesso al file
4907	Le impostazioni di controllo degli oggetti sono state modificate	OBJECT ACCESS (ACCESSO A OGGETTI): Impostazioni di controllo modificate.	Accesso al file
4913	La policy di accesso di Object Central è stata modificata	ACCESSO A OGGETTI: CAP MODIFICATO.	Accesso al file

I seguenti eventi SMB possono essere verificati in ONTAP 9.0 e versioni successive:

ID EVENTO (EVT/EVTX)	Evento	Descrizione	Categoria
540/4624	Un account è stato collegato correttamente	LOGON/LOGOFF: Accesso alla rete (SMB).	Accesso e disconnessione
529/4625	Impossibile accedere a un account	LOGON/LOGOFF: Nome utente sconosciuto o password errata.	Accesso e disconnessione
530/4625	Impossibile accedere a un account	LOGON/LOGOFF: Limite di tempo per l'accesso all'account.	Accesso e disconnessione
531/4625	Impossibile accedere a un account	LOGON/LOGOFF: Account attualmente disattivato.	Accesso e disconnessione
532/4625	Impossibile accedere a un account	LOGON/LOGOFF: L'account utente è scaduto.	Accesso e disconnessione
533/4625	Impossibile accedere a un account	LOGON/LOGOFF (ACCESSO/DISCONNESSIONE): L'utente non può accedere al computer.	Accesso e disconnessione
534/4625	Impossibile accedere a un account	LOGON/LOGOFF: L'utente non ha concesso il tipo di accesso qui.	Accesso e disconnessione
535/4625	Impossibile accedere a un account	LOGON/LOGOFF: La password dell'utente è scaduta.	Accesso e disconnessione
537/4625	Impossibile accedere a un account	LOGON/LOGOFF: Accesso non riuscito per motivi diversi da quelli sopra indicati.	Accesso e disconnessione



539/4625	Impossibile accedere a un account	LOGON/LOGOFF: Account bloccato.	Accesso e disconnessione
538/4634	Un account è stato disconnesso	LOGON/LOGOFF: Disconnessione dell'utente locale o di rete.	Accesso e disconnessione
560/4656	Apri oggetto/Crea oggetto	ACCESSO A OGGETTI: Oggetto (file o directory) aperto.	Accesso al file
563/4659	Aprire l'oggetto con l'intento di eliminare	ACCESSO A OGGETTI: È stato richiesto un handle a un oggetto (file o directory) con l'intento di eliminare.	Accesso al file
564/4660	Elimina oggetto	OBJECT ACCESS (ACCESSO A OGGETTI): Elimina oggetto (file o directory). ONTAP genera questo evento quando un client Windows tenta di eliminare l'oggetto (file o directory).	Accesso al file
567/4663	Read Object/Write Object/Get Object Attributes/Set Object Attributes	ACCESSO A OGGETTI: Tentativo di accesso a oggetti (lettura, scrittura, attributo get, attributo set).  <b>Nota:</b> per questo evento, ONTAP controlla solo la prima operazione di lettura SMB e la prima operazione di scrittura SMB (successo o errore) su un oggetto. Ciò impedisce a ONTAP di creare voci di registro eccessive quando un singolo client apre un oggetto ed esegue molte operazioni di lettura o scrittura successive sullo stesso oggetto.	Accesso al file
NA/4664	Collegamento rigido	OBJECT ACCESS (ACCESSO A OGGETTI): Tentativo di creazione di un hard link.	Accesso al file
NA/4818	Il criterio di accesso centrale proposto non concede le stesse autorizzazioni di accesso del criterio di accesso centrale corrente	ACCESSO A OGGETTI: Gestione temporanea dei criteri di accesso centrale.	Accesso al file

ID evento Data ONTAP NA/NA 9999	Rinominare l'oggetto	ACCESSO AGLI OGGETTI: Oggetto rinominato. Si tratta di un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	Accesso al file
ID evento Data ONTAP NA/NA 9998	Scollegare l'oggetto	ACCESSO A OGGETTI: Oggetto non collegato. Si tratta di un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	Accesso al file

#### Ulteriori informazioni sull'evento 4656

Il `HandleID` tag nell'audit XML l'evento contiene l'handle dell'oggetto (file o directory) a cui si accede. Il `HandleID` Tag per L'evento EVTX 4656 contiene informazioni diverse a seconda che l'evento aperto sia per la creazione di un nuovo oggetto o per l'apertura di un oggetto esistente:

- Se l'evento open è una richiesta di apertura per creare un nuovo oggetto (file o directory), il `HandleID` Il tag nell'evento XML di audit mostra un valore vuoto `HandleID` (ad esempio: `<Data Name="HandleID">0000000000000000;00;00000000;00000000</Data>` ).

Il `HandleID` È vuoto perché la richiesta DI APERTURA (per la creazione di un nuovo oggetto) viene controllata prima che avvenga la creazione effettiva dell'oggetto e prima che esista un handle. Gli eventi controllati successivi per lo stesso oggetto hanno il giusto handle di oggetto in `HandleID` tag.

- Se l'evento open è una richiesta aperta per aprire un oggetto esistente, l'evento di audit avrà l'handle assegnato di tale oggetto in `HandleID` tag (ad esempio: `<Data Name="HandleID">000000000000401;00;000000ea;00123ed4</Data>` ).

#### Determinare il percorso completo dell'oggetto verificato

Il percorso dell'oggetto stampato in `<ObjectName>` il tag per un record di audit contiene il nome del volume (tra parentesi) e il percorso relativo dalla directory principale del volume contenente. Se si desidera determinare il percorso completo dell'oggetto sottoposto a audit, incluso il percorso di giunzione, è necessario eseguire alcuni passaggi.

#### Fasi

1. Determinare il nome del volume e il relativo percorso dell'oggetto sottoposto a controllo osservando il `<ObjectName>` tag nell'evento di audit.

In questo esempio, il nome del volume è "data1" e il percorso relativo al file è `/dir1/file.txt`:

```
<Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
```

2. Utilizzando il nome del volume determinato nella fase precedente, determinare il percorso di giunzione per il volume contenente l'oggetto verificato:

In questo esempio, il nome del volume è "data1" e il percorso di giunzione per il volume contenente

l'oggetto sottoposto a audit è /data/data1:

```
volume show -junction -volume data1
```

Vserver	Volume	Junction		Junction Path	Junction Path Source
		Language	Active		
vs1	data1	en_US.UTF-8	true	/data/data1	RW_volume

3. Determinare il percorso completo dell'oggetto verificato aggiungendo il percorso relativo trovato in <ObjectName> contrassegnare il percorso di giunzione per il volume.

In questo esempio, il percorso di giunzione per il volume:

```
/data/data1/dir1/file.text
```

### Considerazioni per il controllo di collegamenti simbolici e hard link

Ci sono alcune considerazioni da tenere a mente quando si esegue il controllo dei collegamenti simbolici e dei collegamenti rigidi.

Un record di audit contiene informazioni sull'oggetto sottoposto a audit, incluso il percorso dell'oggetto sottoposto a audit, identificato in `ObjectName` tag. È necessario conoscere come vengono registrati i percorsi per i collegamenti simbolici e gli hard link in `ObjectName` tag.

#### Link simbolici

Un collegamento simbolico è un file con un inode separato che contiene un puntatore alla posizione di un oggetto di destinazione, noto come destinazione. Quando si accede a un oggetto tramite un collegamento simbolico, ONTAP interpreta automaticamente il collegamento simbolico e segue il percorso indipendente dal protocollo canonico effettivo verso l'oggetto di destinazione nel volume.

Nell'output dell'esempio seguente, sono presenti due collegamenti simbolici, entrambi rivolti a un file denominato `target.txt`. Uno dei link simbolici è un link simbolico relativo e uno è un link simbolico assoluto. Se uno dei collegamenti simbolici viene controllato, il `ObjectName` tag nell'evento di audit contiene il percorso del file `target.txt`:

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

#### Collegamenti hardware

Un hard link è una voce di directory che associa un nome a un file esistente su un file system. L'hard link punta

alla posizione inode del file originale. Analogamente a quanto ONTAP interpreta i collegamenti simbolici, ONTAP interpreta il collegamento rigido e segue il percorso canonico effettivo dell'oggetto di destinazione nel volume. Quando viene verificato l'accesso a un oggetto hard link, l'evento di audit registra questo percorso canonico assoluto in `ObjectName` piuttosto che il percorso hard link.

### Considerazioni per il controllo di flussi di dati NTFS alternativi

È necessario tenere presente alcune considerazioni durante il controllo dei file con flussi di dati alternativi NTFS.

La posizione di un oggetto sottoposto a audit viene registrata in un record di evento utilizzando due tag, l'`ObjectName` tag (il percorso) e il `HandleID` tag (l'impugnatura). Per identificare correttamente le richieste di flusso registrate, è necessario conoscere i record ONTAP presenti in questi campi per i flussi di dati alternativi NTFS:

- ID EVTX: 4656 eventi (aprire e creare eventi di audit)
  - Il percorso del flusso di dati alternativo viene registrato in `ObjectName` tag.
  - L'handle del flusso di dati alternativo viene registrato in `HandleID` tag.
- ID EVTX: 4663 eventi (tutti gli altri eventi di audit, come lettura, scrittura, `getattr` e così via)
  - Il percorso del file di base, non del flusso di dati alternativo, viene registrato in `ObjectName` tag.
  - L'handle del flusso di dati alternativo viene registrato in `HandleID` tag.

### Esempio

Nell'esempio seguente viene illustrato come identificare L'ID EVTX: 4663 eventi per flussi di dati alternativi che utilizzano `HandleID` tag. Anche se il `ObjectName` il tag (percorso) registrato nell'evento di controllo in lettura si trova nel percorso del file di base, il `HandleID` il tag può essere utilizzato per identificare l'evento come record di audit per il flusso di dati alternativo.

I nomi dei file di streaming hanno la forma `base_file_name:stream_name`. In questo esempio, il `dir1` la directory contiene un file di base con un flusso di dati alternativo con i seguenti percorsi:

```
/dir1/file1.txt  
/dir1/file1.txt:stream1
```



L'output nel seguente esempio di evento viene troncato come indicato; l'output non visualizza tutti i tag di output disponibili per gli eventi.

Per un ID EVTX 4656 (evento di audit aperto), l'output del record di audit per il flusso di dati alternativo registra il nome del flusso di dati alternativo in `ObjectName` tag:

```

- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\\(data1\\);/dir1/file1.txt:stream1</Data>
  **
  [...]
</EventData>
</Event>
- <Event>

```

Per un ID EVTX 4663 (evento di audit in lettura), l'output del record di audit per lo stesso flusso di dati alternativo registra il nome del file di base in `ObjectName` tag; tuttavia, l'handle in `HandleID` tag è l'handle alternativo del flusso di dati e può essere utilizzato per correlare questo evento con il flusso di dati alternativo:

```

- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
</System>
- <EventData>
  [...]
  **<Data Name="ObjectType">Stream</Data>
  <Data Name="HandleID">00000000000401;00;000001e4;00176767</Data>
  <Data Name="ObjectName">\\(data1\\);/dir1/file1.txt</Data> **
  [...]
</EventData>
</Event>
- <Event>

```

## Eventi di accesso a file e directory NFS che possono essere controllati

ONTAP può controllare alcuni eventi di accesso a file e directory NFS. Sapere quali eventi di accesso possono essere verificati è utile quando si interpretano i risultati dei registri degli eventi di audit convertiti.

È possibile controllare i seguenti eventi di accesso a file e directory NFS:

- LEGGI
- APRIRE
- CHIUDERE
- READDIR
- DI SCRITTURA
- SETATTR
- CREARE
- COLLEGAMENTO
- OPENATTR
- RIMUOVERE
- GETATTR
- VERIFICARE
- NVERIFICARE
- RINOMINARE

Per controllare in modo affidabile gli eventi DI RIDENOMINAZIONE NFS, è necessario impostare ACE di controllo sulle directory invece che sui file, in quanto le autorizzazioni dei file non vengono controllate per un'operazione DI RIDENOMINAZIONE, se le autorizzazioni della directory sono sufficienti.

## Pianificare la configurazione di controllo

Prima di configurare il controllo sulle macchine virtuali di storage, è necessario comprendere quali opzioni di configurazione sono disponibili e pianificare i valori che si desidera impostare per ciascuna opzione. Queste informazioni possono aiutarti a configurare la configurazione di controllo che soddisfa le tue esigenze di business.

Alcuni parametri di configurazione sono comuni a tutte le configurazioni di controllo.

Inoltre, è possibile utilizzare alcuni parametri per specificare i metodi da utilizzare durante la rotazione dei registri di controllo consolidati e convertiti. Quando si configura il controllo, è possibile specificare uno dei tre metodi seguenti:

- Ruotare i registri in base alle dimensioni del registro

Questo è il metodo predefinito utilizzato per ruotare i registri.

- Ruotare i registri in base a una pianificazione
  - Rotazione dei registri in base alle dimensioni e alla pianificazione del registro (a seconda dell'evento che si verifica per primo)
- F

È necessario impostare almeno uno dei metodi per la rotazione del log.

## Parametri comuni a tutte le configurazioni di controllo

Sono necessari due parametri da specificare quando si crea la configurazione di controllo. Sono inoltre disponibili tre parametri opzionali che è possibile specificare:

Tipo di informazione	Opzione	Obbligatorio	Includi	I tuoi valori
<b>Nome SVM</b>  Nome della SVM su cui creare la configurazione di controllo. La SVM deve già esistere.	<code>-vserver vserver_name</code>	Sì	Sì	
<b>Percorso di destinazione del registro</b>  Specifica la directory in cui sono memorizzati i log di audit convertiti, in genere un volume dedicato o un qtree. Il percorso deve già esistere nello spazio dei nomi SVM.  Il percorso può contenere fino a 864 caratteri e deve disporre di permessi di lettura/scrittura.  Se il percorso non è valido, il comando di configurazione del controllo non riesce.  Se SVM è un'origine di disaster recovery SVM, il percorso di destinazione del log non può trovarsi sul volume root. Questo perché il contenuto del volume root non viene replicato nella destinazione del disaster recovery.  Non è possibile utilizzare un volume FlexCache come destinazione del registro (ONTAP 9.7 e versioni successive).	<code>-destination text</code>	Sì	Sì	

<p><b>Categorie di eventi da controllare</b></p> <p>Specifica le categorie di eventi da controllare. È possibile verificare le seguenti categorie di eventi:</p> <ul style="list-style-type: none"> <li>• Eventi di accesso al file (SMB e NFSv4)</li> <li>• Eventi di logon e logoff SMB</li> <li>• Eventi di staging dei criteri di accesso centrale</li> </ul> <p>Gli eventi di staging dei criteri di accesso centrale sono disponibili a partire dai domini Active Directory di Windows 2012.</p> <ul style="list-style-type: none"> <li>• Eventi categoria condivisione file</li> <li>• Eventi di modifica delle policy di audit</li> <li>• Eventi di gestione dell'account utente locale</li> <li>• Eventi di gestione dei gruppi di sicurezza</li> <li>• Eventi di modifica del criterio di autorizzazione</li> </ul> <p>Per impostazione predefinita, viene eseguito il controllo dell'accesso al file e degli eventi di logon e logoff SMB.</p> <p><b>Nota:</b> prima di poter specificare <code>cap-staging</code> Come categoria di evento, un server SMB deve esistere sulla SVM. Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, gli eventi di staging dei criteri di accesso centrale vengono generati solo se è attivato il controllo dinamico degli accessi. Il controllo dinamico degli accessi viene attivato tramite un'opzione server SMB. Non è attivato per impostazione predefinita.</p>	-events {file-ops	cifs-logon-logoff	cap-staging	file-share
audit-policy-change	user-account	security-group	authorization-policy-change}	No



		<p><i>Formato di output del file di log</i></p> <p>Determina il formato di output dei registri di controllo. Il formato di output può essere specifico di ONTAP XML O Microsoft Windows EVTX formato del log. Per impostazione predefinita, il formato di output è EVTX.</p>	<p>-format {xml</p>	<p>evtx}</p>
--	--	--	---------------------	--------------

No			<p><i>Limite di rotazione dei file di log</i></p> <p>Determina il numero di file di log di audit da conservare prima di estrarre il file di log più vecchio. Ad esempio, se si immette un valore di 5, vengono conservati i gli ultimi cinque file di log.</p> <p>Un valore di 0 indica che tutti i file di log vengono conservati. Il valore predefinito è 0.</p>	<p>-rotate -limit integer</p>
----	--	--	--	---------------------------------------

## Parametri utilizzati per determinare quando ruotare i registri degli eventi di audit

### Ruota i registri in base alle dimensioni del registro

L'impostazione predefinita prevede la rotazione dei registri di controllo in base alle dimensioni.

- La dimensione predefinita del registro è 100 MB
- Se si desidera utilizzare il metodo di rotazione del log predefinito e la dimensione del log predefinita, non è necessario configurare alcun parametro specifico per la rotazione del log.
- Se si desidera ruotare i registri di controllo solo in base alle dimensioni del registro, utilizzare il comando seguente per annullare l'impostazione di `-rotate-schedule-minute` parametro: `vserver audit`

```
modify -vserver vs0 -destination / -rotate-schedule-minute -
```

Se non si desidera utilizzare la dimensione predefinita del registro, è possibile configurare `-rotate-size` parametro per specificare una dimensione di log personalizzata:

Tipo di informazione	Opzione	Obbligatorio	Includi	I tuoi valori
<i>Limite dimensioni file di log</i>  Determina il limite delle dimensioni del file di log di audit.	<code>-rotate-size {integer}[KB</code>	MB	GB	TB

### Rotazione dei registri in base a una pianificazione

Se si sceglie di ruotare i registri di controllo in base a una pianificazione, è possibile pianificare la rotazione dei registri utilizzando i parametri di rotazione basati sul tempo in qualsiasi combinazione.

- Se si utilizza la rotazione basata sul tempo, il `-rotate-schedule-minute` il parametro è obbligatorio.
- Tutti gli altri parametri di rotazione basati sul tempo sono opzionali.
- Il programma di rotazione viene calcolato utilizzando tutti i valori relativi al tempo.

Ad esempio, se si specifica solo il `-rotate-schedule-minute` i file di log di audit vengono ruotati in base ai minuti specificati in tutti i giorni della settimana, durante tutte le ore in tutti i mesi dell'anno.

- Se si specificano solo uno o due parametri di rotazione basati sul tempo (ad esempio, `-rotate-schedule-month` e `-rotate-schedule-minutes`), i file di log vengono ruotati in base ai valori dei minuti specificati in tutti i giorni della settimana, durante tutte le ore, ma solo durante i mesi specificati.

Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato durante i mesi di gennaio, marzo e agosto tutti i lunedì, mercoledì e sabato alle 10:30

- Se si specificano i valori per entrambi `-rotate-schedule-dayofweek` e `-rotate-schedule-day`, sono considerati indipendenti.

Ad esempio, se si specifica `-rotate-schedule-dayofweek` Come venerdì e `-rotate-schedule-day` Come 13, i registri di audit verrebbero ruotati ogni venerdì e il 13° giorno del mese specificato, non solo ogni venerdì 13.

- Se si desidera ruotare i registri di controllo solo in base a una pianificazione, utilizzare il comando seguente per annullare l'impostazione di `-rotate-size` parametro: `vserver audit modify -vserver vs0 -destination / -rotate-size -`

È possibile utilizzare il seguente elenco di parametri di controllo disponibili per determinare i valori da utilizzare per la configurazione di una pianificazione per le rotazioni del registro eventi di controllo:

Tipo di informazione	Opzione	Obbligatorio	Includi	I tuoi valori
----------------------	---------	--------------	---------	---------------

<p><b>Programma di rotazione del log: Mese</b></p> <p>Determina la pianificazione mensile per la rotazione dei registri di audit.</p> <p>I valori validi sono January attraverso December, e. all. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato nei mesi di gennaio, marzo e agosto.</p>	<p>-rotate-schedule-month chron_month</p>	No		
<p><b>Programma di rotazione del log: Giorno della settimana</b></p> <p>Determina la pianificazione giornaliera (giorno della settimana) per la rotazione dei registri di audit.</p> <p>I valori validi sono Sunday attraverso Saturday, e. all. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato il martedì e il venerdì o durante tutti i giorni di una settimana.</p>	<p>-rotate-schedule -dayofweek chron_dayofweek</p>	No		
<p><b>Programma di rotazione del log: Giorno</b></p> <p>Determina il giorno della pianificazione del mese per la rotazione del registro di audit.</p> <p>I valori validi sono compresi tra 1 attraverso 31. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato il 10° e il 20° giorno di un mese o tutti i giorni di un mese.</p>	<p>-rotate-schedule-day chron_dayofmonth</p>	No		
<p><b>Programma di rotazione del log: Ora</b></p> <p>Determina la pianificazione oraria per la rotazione del registro di audit.</p> <p>I valori validi sono compresi tra 0 (mezzanotte) a. 23 (11:00). Specificare all ruota i registri di controllo ogni ora. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato alle 6 (6:00) e alle 18 (18:00).</p>	<p>-rotate-schedule-hour chron_hour</p>	No		

<p><b>Log Rotation schedule: Minute</b></p> <p>Determina la pianificazione dei minuti per la rotazione del registro di controllo.</p> <p>I valori validi sono compresi tra 0 a. 59. Ad esempio, è possibile specificare che il registro di controllo deve essere ruotato al 30° minuto.</p>	<p><code>-rotate-schedule-minute</code> <code>chron_minute</code></p>	<p>Sì, se si configura la rotazione del log in base alla pianificazione; in caso contrario, no</p>		
---	---	--	--	--

## Rotazione dei registri in base alle dimensioni e alla pianificazione dei registri

È possibile scegliere di ruotare i file di log in base alle dimensioni e alla pianificazione del log impostando entrambi i campi `-rotate-size` e i parametri di rotazione basati sul tempo in qualsiasi combinazione. Ad esempio: Se `-rotate-size` È impostato su 10 MB e `-rotate-schedule-minute` È impostato su 15, i file di log ruotano quando le dimensioni del file di log raggiungono i 10 MB o al 15° minuto di ogni ora (a seconda dell'evento che si verifica per primo).

## Creare una configurazione di controllo di file e directory sulle SVM

### Creare la configurazione di controllo

La creazione di una configurazione per il controllo di file e directory sulla macchina virtuale di storage (SVM) include la comprensione delle opzioni di configurazione disponibili, la pianificazione della configurazione, quindi la configurazione e l'abilitazione della configurazione. È quindi possibile visualizzare le informazioni sulla configurazione di controllo per confermare che la configurazione risultante è quella desiderata.

Prima di iniziare il controllo degli eventi di file e directory, è necessario creare una configurazione di controllo sulla macchina virtuale di storage (SVM).

### Prima di iniziare

Se si prevede di creare una configurazione di controllo per lo staging dei criteri di accesso centrale, è necessario che un server SMB esista sulla SVM.



- Sebbene sia possibile attivare lo staging dei criteri di accesso centrale nella configurazione di controllo senza attivare il controllo dinamico degli accessi sul server SMB, gli eventi di staging dei criteri di accesso centrale vengono generati solo se è attivato il controllo dinamico degli accessi.

Il controllo dinamico degli accessi viene attivato tramite un'opzione server SMB. Non è attivato per impostazione predefinita.

- Se gli argomenti di un campo in un comando non sono validi, ad esempio voci non valide per campi, voci duplicate e voci non esistenti, il comando non riesce prima della fase di audit.

Tali errori non generano un record di audit.

## A proposito di questa attività

Se SVM è un'origine di disaster recovery SVM, il percorso di destinazione non può trovarsi sul volume root.

### Fase

1. Utilizzando le informazioni contenute nel foglio di lavoro di pianificazione, creare la configurazione di controllo per ruotare i registri di controllo in base alle dimensioni del log o a una pianificazione:

Se si desidera ruotare i registri di audit di...	Inserisci...
Dimensione del log	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}} [-format {xml	evtx}} [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB}}]`
Un calendario	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}} [-format {xml

### Esempi

Nell'esempio seguente viene creata una configurazione di controllo che controlla le operazioni dei file e gli eventi di logon e logoff SMB (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il formato del log è EVTX (impostazione predefinita). I registri vengono memorizzati in `/audit_log` directory. Il limite delle dimensioni del file di registro è 200 MB. I log vengono ruotati quando raggiungono le dimensioni di 200 MB:

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log  
-rotate-size 200MB
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla le operazioni dei file e gli eventi di logon e logoff SMB (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il formato del log è EVTX (impostazione predefinita). I registri vengono memorizzati in `/cifs_event_logs` directory. Il limite delle dimensioni del file di registro è 100 MB (l'impostazione predefinita) e il limite di rotazione del registro è 5:

```
cluster1::> vserver audit create -vserver vs1 -destination  
/cifs_event_logs -rotate-limit 5
```

Nell'esempio seguente viene creata una configurazione di controllo che controlla le operazioni dei file, gli

eventi di logon e logoff di CIFS e gli eventi di staging dei criteri di accesso centrale utilizzando la rotazione basata sul tempo. Il formato del log è EVTX (impostazione predefinita). I registri di audit vengono ruotati mensilmente alle 12:30 tutti i giorni della settimana. Il limite di rotazione del log è 5:

```
cluster1::> vsserver audit create -vsserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

## Abilitare il controllo su SVM

Una volta completata l'impostazione della configurazione di controllo, è necessario attivare il controllo sulla macchina virtuale di storage (SVM).

### Di cosa hai bisogno

La configurazione dell'audit SVM deve già esistere.

### A proposito di questa attività

Quando una configurazione di eliminazione dell'ID di disaster recovery SVM viene avviata per la prima volta (dopo il completamento dell'inizializzazione di SnapMirror) e la SVM dispone di una configurazione di controllo, ONTAP disattiva automaticamente la configurazione di controllo. Il controllo viene disattivato sulla SVM di sola lettura per impedire il riempimento dei volumi di staging. È possibile attivare il controllo solo dopo che la relazione SnapMirror è stata interrotta e la SVM è in lettura/scrittura.

### Fase

1. Abilitare il controllo su SVM:

```
vsserver audit enable -vsserver vsserver_name

vsserver audit enable -vsserver vs1
```

## Verificare la configurazione di controllo

Dopo aver completato la configurazione di controllo, verificare che il controllo sia configurato correttamente e che sia attivato.

### Fasi

1. Verificare la configurazione di controllo:

```
vsserver audit show -instance -vsserver vsserver_name
```

Il seguente comando visualizza sotto forma di elenco tutte le informazioni di controllo della configurazione per la macchina virtuale di storage (SVM) vs1:

```
vsserver audit show -instance -vsserver vs1
```

```
Vserver: vs1
Auditing state: true
Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
Log Format: evt
Log File Size Limit: 200MB
Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
Log Rotation Schedule: Day: -
Log Rotation Schedule: Hour: -
Log Rotation Schedule: Minute: -
Rotation Schedules: -
Log Files Rotation Limit: 0
```

## Configurare i criteri di controllo di file e cartelle

### Configurare i criteri di controllo di file e cartelle

L'implementazione del controllo sugli eventi di accesso a file e cartelle è un processo in due fasi. Innanzitutto, è necessario creare e abilitare una configurazione di controllo sulle macchine virtuali di storage (SVM). In secondo luogo, è necessario configurare i criteri di controllo nei file e nelle cartelle che si desidera monitorare. È possibile configurare criteri di controllo per monitorare i tentativi di accesso riusciti e non riusciti.

È possibile configurare policy di audit SMB e NFS. Le policy di audit SMB e NFS hanno requisiti di configurazione e funzionalità di audit differenti.

Se sono configurati i criteri di audit appropriati, ONTAP monitora gli eventi di accesso SMB e NFS come specificato nelle policy di audit solo se i server SMB o NFS sono in esecuzione.

### Configurare le policy di audit su file e directory di sicurezza NTFS

Prima di poter controllare le operazioni di file e directory, è necessario configurare i criteri di audit sui file e sulle directory per cui si desidera raccogliere le informazioni di audit. Oltre all'impostazione e all'abilitazione della configurazione di audit. È possibile configurare i criteri di controllo NTFS utilizzando la scheda protezione di Windows o l'interfaccia utente di ONTAP.

#### Configurazione dei criteri di controllo NTFS mediante la scheda protezione di Windows

È possibile configurare i criteri di controllo NTFS su file e directory utilizzando la scheda **Windows Security** nella finestra Proprietà di Windows. Si tratta dello stesso metodo utilizzato per la configurazione dei criteri di controllo sui dati che risiedono su un client Windows, che consente di utilizzare la stessa interfaccia GUI utilizzata.

#### Di cosa hai bisogno

Il controllo deve essere configurato sulla macchina virtuale di storage (SVM) che contiene i dati a cui si



applicano gli elenchi di controllo di accesso al sistema (SACL).

**A proposito di questa attività**

La configurazione dei criteri di audit NTFS viene eseguita aggiungendo voci ai SACL NTFS associate a un descrittore di protezione NTFS. Il descrittore di protezione viene quindi applicato ai file e alle directory NTFS. Queste attività vengono gestite automaticamente dalla GUI di Windows. Il descrittore di protezione può contenere elenchi di controllo degli accessi discrezionali (DACL) per l'applicazione delle autorizzazioni di accesso a file e cartelle, SACL per il controllo di file e cartelle o SACL e DACL.

Per impostare i criteri di controllo NTFS utilizzando la scheda protezione di Windows, completare la seguente procedura su un host Windows:

**Fasi**

- 1. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
- 2. Completare la casella **Map Network Drive** (Connetti unità di rete):
  - a. Selezionare una lettera **Drive**.
  - b. Nella casella **Folder** (cartella), digitare il nome del server SMB che contiene la condivisione, contenente i dati che si desidera controllare e il nome della condivisione.

È possibile specificare l'indirizzo IP dell'interfaccia dati per il server SMB invece del nome del server SMB.

Se il nome del server SMB è "SMB\_SERVER" e la condivisione è denominata "share1", immettere \\SMB\_SERVER\share1.

- c. Fare clic su **fine**.

Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

- 3. Selezionare il file o la directory per cui si desidera abilitare l'accesso di controllo.
- 4. Fare clic con il pulsante destro del mouse sul file o sulla directory, quindi selezionare **Proprietà**.
- 5. Selezionare la scheda **sicurezza**.
- 6. Fare clic su **Avanzate**.
- 7. Selezionare la scheda **Auditing**.
- 8. Eseguire le azioni desiderate:

Se si desidera	Effettuare le seguenti operazioni
Impostare il controllo per un nuovo utente o gruppo	<ul style="list-style-type: none"><li>a. Fare clic su <b>Aggiungi</b>.</li><li>b. Nella casella immettere il nome dell'oggetto da selezionare, digitare il nome dell'utente o del gruppo che si desidera aggiungere.</li><li>c. Fare clic su <b>OK</b>.</li></ul>

Rimuovere il controllo da un utente o gruppo	<p>a. Nella casella immettere il nome dell'oggetto da selezionare, selezionare l'utente o il gruppo che si desidera rimuovere.</p> <p>b. Fare clic su <b>Rimuovi</b>.</p> <p>c. Fare clic su <b>OK</b>.</p> <p>d. Ignorare il resto di questa procedura.</p>
Controllo delle modifiche per un utente o un gruppo	<p>a. Nella casella immettere il nome dell'oggetto da selezionare, selezionare l'utente o il gruppo che si desidera modificare.</p> <p>b. Fare clic su <b>Edit</b> (Modifica).</p> <p>c. Fare clic su <b>OK</b>.</p>

Se si imposta il controllo su un utente o un gruppo o si modifica il controllo su un utente o un gruppo esistente, viene visualizzata la casella voce di controllo per <object>.

9. Nella casella **Applica a**, selezionare la modalità di applicazione della voce di controllo.

È possibile selezionare una delle seguenti opzioni:

- **Questa cartella, sottocartelle e file**
- **Questa cartella e sottocartelle**
- **Solo questa cartella**
- **Questa cartella e file**
- **Solo sottocartelle e file**
- **Solo sottocartelle**
- **Solo file** se si imposta il controllo su un singolo file, la casella **Applica a** non è attiva. L'impostazione predefinita della casella **Applica a** è **solo questo oggetto**.



Poiché il controllo richiede risorse SVM, selezionare solo il livello minimo che fornisce gli eventi di controllo che soddisfano i requisiti di sicurezza.

10. Nella casella **Access**, selezionare i dati da sottoporre a verifica e se si desidera controllare gli eventi di successo, gli eventi di errore o entrambi.

- Per controllare gli eventi riusciti, selezionare la casella Success (successo).
- Per controllare gli eventi di errore, selezionare la casella Failure (errore).

Selezionare solo le azioni da monitorare per soddisfare i requisiti di sicurezza. Per ulteriori informazioni su questi eventi verificabili, consultare la documentazione di Windows. È possibile controllare i seguenti eventi:

- **Controllo completo**
- **Cartella Traverse / file di esecuzione**
- **Elenca cartella / leggi dati**
- **Attributi di lettura**
- **Leggi attributi estesi**

- **Creare file / scrivere dati**
- **Crea cartelle/Aggiungi dati**
- **Attributi di scrittura**
- **Scrivi attributi estesi**
- **Elimina sottocartelle e file**
- **Elimina**
- **Permessi di lettura**
- **Modifica delle autorizzazioni**
- **Assumere la proprietà**

11. Se non si desidera che l'impostazione di controllo si propaghi ai file e alle cartelle successivi del contenitore originale, selezionare la casella **Applica queste voci di controllo solo agli oggetti e/o ai contenitori all'interno di questo contenitore**.
12. Fare clic su **Apply** (Applica).
13. Dopo aver aggiunto, rimosso o modificato le voci di controllo, fare clic su **OK**.

La casella voce di controllo per <object> viene chiusa.

14. Nella casella **Auditing**, selezionare le impostazioni di ereditarietà per questa cartella.

Selezionare solo il livello minimo che fornisce gli eventi di controllo che soddisfano i requisiti di sicurezza. È possibile scegliere una delle seguenti opzioni:

- Selezionare la casella **Includi voci di controllo ereditabili dall'oggetto principale**.
- Selezionare la casella **Sostituisci tutte le voci di controllo ereditabili esistenti su tutti i discendenti con voci di controllo ereditabili da questo oggetto**.
- Selezionare entrambe le caselle.
- Selezionare nessuna delle due caselle. Se si impostano SACL su un singolo file, la casella di controllo **Sostituisci tutte le voci di controllo ereditabili esistenti su tutti i discendenti con voci di controllo ereditabili da questo oggetto** non è presente nella casella di controllo.

15. Fare clic su **OK**.

La finestra Auditing si chiude.

#### **Configurare i criteri di audit NTFS utilizzando l'interfaccia CLI di ONTAP**

È possibile configurare i criteri di controllo su file e cartelle utilizzando l'interfaccia utente di ONTAP. Ciò consente di configurare le policy di audit NTFS senza la necessità di connettersi ai dati utilizzando una condivisione SMB su un client Windows.

È possibile configurare i criteri di audit NTFS utilizzando `vserver security file-directory` famiglia di comandi.

È possibile configurare SACL NTFS solo utilizzando la CLI. La configurazione dei SACL NFSv4 non è supportata con questa famiglia di comandi ONTAP. Consultare le pagine man per ulteriori informazioni sull'utilizzo di questi comandi per configurare e aggiungere SACL NTFS a file e cartelle.

## Configurare il controllo per i file e le directory di sicurezza UNIX

È possibile configurare il controllo per i file e le directory di sicurezza UNIX aggiungendo ACE di controllo agli ACL NFSv4.x. Ciò consente di monitorare determinati eventi di accesso a file e directory NFS per motivi di sicurezza.

### A proposito di questa attività

Per NFSv4.x, le ACE discrezionali e di sistema sono memorizzate nello stesso ACL. Non sono memorizzati in DACL e SACL separati. Pertanto, è necessario prestare attenzione quando si aggiungono ACE di audit a un ACL esistente per evitare di sovrascrivere e perdere un ACL esistente. L'ordine in cui si aggiungono le ACE di audit a un ACL esistente non ha importanza.

### Fasi

1. Recuperare l'ACL esistente per il file o la directory utilizzando `nfs4_getfacl` o comando equivalente.

Per ulteriori informazioni sulla manipolazione degli ACL, consulta le pagine man del tuo client NFS.

2. Aggiungere gli ACE di audit desiderati.
3. Applicare l'ACL aggiornato al file o alla directory utilizzando `nfs4_setfacl` o comando equivalente.

## Visualizza informazioni sui criteri di controllo applicati a file e directory

### Visualizzare le informazioni sui criteri di controllo utilizzando la scheda protezione di Windows

È possibile visualizzare informazioni sui criteri di controllo applicati a file e directory utilizzando la scheda Security (protezione) della finestra Windows Properties (Proprietà di Windows). Si tratta dello stesso metodo utilizzato per i dati residenti su un server Windows, che consente ai clienti di utilizzare la stessa interfaccia GUI a cui sono abituati.

### A proposito di questa attività

La visualizzazione delle informazioni sui criteri di controllo applicati a file e directory consente di verificare che siano impostati gli elenchi di controllo di accesso di sistema (SACL) appropriati su file e cartelle specificati.

Per visualizzare informazioni sui SACL applicati a file e cartelle NTFS, completare la seguente procedura su un host Windows.

### Fasi

1. Dal menu **Strumenti** di Esplora risorse, selezionare **Connetti unità di rete**.
2. Completare la finestra di dialogo **Map Network Drive** (Connetti unità di rete):
  - a. Selezionare una lettera **Drive**.
  - b. Nella casella **Folder** (cartella), digitare l'indirizzo IP o il nome del server SMB della macchina virtuale di storage (SVM) contenente la condivisione che contiene sia i dati che si desidera controllare che il nome della condivisione.

Se il nome del server SMB è "SMB\_SERVER" e la condivisione è denominata "share1", immettere \\SMB\_SERVER\share1.



È possibile specificare l'indirizzo IP dell'interfaccia dati per il server SMB invece del nome del server SMB.

c. Fare clic su **fine**.

Il disco selezionato viene montato e pronto con la finestra Esplora risorse che visualizza i file e le cartelle contenuti nella condivisione.

3. Selezionare il file o la directory per cui vengono visualizzate le informazioni di controllo.
4. Fare clic con il pulsante destro del mouse sul file o sulla directory e selezionare **Proprietà**.
5. Selezionare la scheda **sicurezza**.
6. Fare clic su **Avanzate**.
7. Selezionare la scheda **Auditing**.
8. Fare clic su **continua**.

Viene visualizzata la finestra Auditing. Nella casella **voci di controllo** viene visualizzato un riepilogo degli utenti e dei gruppi a cui sono stati applicati SACL.

9. Nella casella **voci di controllo** selezionare l'utente o il gruppo di cui si desidera visualizzare le voci SACL.
10. Fare clic su **Edit** (Modifica).

Viene visualizzata la finestra voce di controllo per <object>.

11. Nella casella **Access**, visualizzare i SACL correnti applicati all'oggetto selezionato.
12. Fare clic su **Annulla** per chiudere la casella **voce di controllo per <object>**.
13. Fare clic su **Annulla** per chiudere la casella **controllo**.

### Visualizza informazioni sui criteri di audit NTFS sui volumi FlexVol utilizzando l'interfaccia CLI

È possibile visualizzare informazioni sui criteri di controllo NTFS sui volumi FlexVol, inclusi gli stili di sicurezza e gli stili di sicurezza effettivi, le autorizzazioni applicate e le informazioni sugli elenchi di controllo degli accessi al sistema. È possibile utilizzare le informazioni per convalidare la configurazione della protezione o per risolvere i problemi di controllo.

#### A proposito di questa attività

La visualizzazione delle informazioni sui criteri di controllo applicati a file e directory consente di verificare che siano impostati gli elenchi di controllo di accesso di sistema (SACL) appropriati su file e cartelle specificati.

Specificare il nome della macchina virtuale di storage (SVM) e il percorso dei file o delle cartelle di cui si desidera visualizzare le informazioni di audit. È possibile visualizzare l'output in forma di riepilogo o come elenco dettagliato.

- I volumi e i qtree di sicurezza NTFS utilizzano solo SACL (System Access Control List) NTFS per i criteri di controllo.
- I file e le cartelle in un volume misto di sicurezza con protezione efficace NTFS possono applicare criteri di controllo NTFS.

I volumi misti di sicurezza e le qtree possono contenere alcuni file e directory che utilizzano permessi di file UNIX, i bit di modalità o gli ACL NFSv4 e alcuni file e directory che utilizzano permessi di file NTFS.

- Il livello superiore di un volume misto di sicurezza può avere una protezione efficace UNIX o NTFS e potrebbe contenere o meno SACL NTFS.

- Poiché la protezione di Storage-Level Access Guard può essere configurata su un volume misto di sicurezza o qtree anche se lo stile di sicurezza effettivo della root del volume o del qtree è UNIX, L'output di un volume o percorso qtree in cui Storage-Level Access Guard è configurato potrebbe visualizzare sia SACL NFSv4 di file e cartelle standard che SACL NTFS di Storage-Level Access Guard.
- Se il percorso immesso nel comando è relativo ai dati con protezione effettiva NTFS, l'output visualizza anche le informazioni relative alle ACE di controllo dinamico degli accessi se Dynamic Access Control è configurato per il percorso di file o directory specificato.
- Quando si visualizzano informazioni di sicurezza su file e cartelle con protezione efficace NTFS, i campi di output relativi a UNIX contengono informazioni di autorizzazione file UNIX di sola visualizzazione.

I file e le cartelle di sicurezza NTFS utilizzano solo le autorizzazioni per i file NTFS e gli utenti e i gruppi Windows per determinare i diritti di accesso ai file.

- L'output ACL viene visualizzato solo per file e cartelle con protezione NTFS o NFSv4.

Questo campo è vuoto per i file e le cartelle che utilizzano la protezione UNIX e che dispongono solo delle autorizzazioni di bit di modalità applicate (nessun ACL NFSv4).

- I campi owner e group output nell'output ACL sono validi solo nel caso di descrittori di protezione NTFS.

## Fase

1. Visualizzare le impostazioni dei criteri di controllo di file e directory con il livello di dettaglio desiderato:

Se si desidera visualizzare le informazioni...	Immettere il seguente comando...
In forma riassuntiva	<code>vserver security file-directory show -vserver vserver_name -path path</code>
Come elenco dettagliato	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>

## Esempi

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso `/corp` in SVM vs1. Il percorso offre una protezione efficace con NTFS. Il descrittore di protezione NTFS contiene sia una voce SACL RIUSCITA che UNA SACL RIUSCITA/NON RIUSCITA.

```

cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8014
            Owner:DOMAIN\Administrator
            Group:BUILTIN\Administrators
            SACL - ACEs
                  ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                  SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
            DACL - ACEs
                  ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                  ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                  ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                  ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI

```

Nell'esempio riportato di seguito vengono visualizzate le informazioni relative ai criteri di controllo per il percorso /datavol1 in SVM vs1. Il percorso contiene SACL di file e cartelle e SACL Storage-Level Access Guard.

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      Security Style: ntfs
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
              AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
              ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
              ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
        AUDIT-EXAMPLE\Domain Users-0x120089-FA
        AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
        ALLOW-EXAMPLE\Domain Users-0x120089
        ALLOW-EXAMPLE\engineering-0x1f01ff
        ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

### Modi per visualizzare informazioni sulla sicurezza dei file e sulle policy di audit

È possibile utilizzare il carattere jolly (\*) per visualizzare informazioni sulla sicurezza dei file e sulle policy di controllo di tutti i file e le directory in un determinato percorso o



volume root.

Il carattere jolly (\*) può essere utilizzato come ultimo sottocomponente di un determinato percorso di directory al di sotto del quale si desidera visualizzare le informazioni di tutti i file e le directory.

Se si desidera visualizzare le informazioni di un determinato file o directory denominata "\*", è necessario fornire il percorso completo tra virgolette doppie (" ").

### **Esempio**

Il seguente comando con il carattere jolly visualizza le informazioni su tutti i file e le directory sotto il percorso /1/ Di SVM vs1:

```

cluster::> vserver security file-directory show -vserver vs1 -path /1/*

      Vserver: vs1
      File Path: /1/1
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8514
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

      Vserver: vs1
      File Path: /1/1/abc
      Security Style: mixed
      Effective Style: ntfs
      DOS Attributes: 10
      DOS Attributes in Text: ----D---
      Expanded Dos Attributes: -
      Unix User Id: 0
      Unix Group Id: 0
      Unix Mode Bits: 777
      Unix Mode Bits in Text: rwxrwxrwx
      ACLs: NTFS Security Descriptor
            Control:0x8404
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

```

Il seguente comando visualizza le informazioni di un file denominato "" sotto il percorso /vol1/a Di SVM vs1. Il percorso è racchiuso tra virgolette doppie (" ").

```
cluster::> vserver security file-directory show -vserver vs1 -path  
"/vol1/a/*"
```

```
        Vserver: vs1  
        File Path: "/vol1/a/*"  
        Security Style: mixed  
        Effective Style: unix  
        DOS Attributes: 10  
        DOS Attributes in Text: ----D---  
        Expanded Dos Attributes: -  
        Unix User Id: 1002  
        Unix Group Id: 65533  
        Unix Mode Bits: 755  
        Unix Mode Bits in Text: rwxr-xr-x  
        ACLs: NFSV4 Security Descriptor  
        Control:0x8014  
        SACL - ACEs  
        AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
        DACL - ACEs  
        ALLOW-EVERYONE@-0x1f00a9-FI|DI  
        ALLOW-OWNER@-0x1f01ff-FI|DI  
        ALLOW-GROUP@-0x1200a9-IG
```

## CLI modifica gli eventi che possono essere verificati

### Panoramica degli eventi di cambiamento CLI che possono essere verificati

ONTAP è in grado di controllare alcuni eventi di modifica dell'interfaccia CLI, tra cui determinati eventi di condivisione SMB, determinati eventi dei criteri di controllo, determinati eventi dei gruppi di protezione locali, eventi dei gruppi di utenti locali ed eventi dei criteri di autorizzazione. La comprensione degli eventi di modifica che è possibile verificare è utile quando si interpretano i risultati dei registri degli eventi.

È possibile gestire la macchina virtuale dello storage (SVM) per il controllo degli eventi di modifica della CLI ruotando manualmente i registri di controllo, attivando o disattivando il controllo, visualizzando le informazioni relative al controllo degli eventi di modifica, modificando gli eventi di modifica del controllo ed eliminando gli eventi di modifica del controllo.

In qualità di amministratore, se si esegue un comando per modificare la configurazione relativa agli eventi SMB-share, User-group locale, Security-group locale, Authorization-policy e audit-policy, viene generato un record e viene verificato l'evento corrispondente:

Categoria di controllo	Eventi	ID evento	Eseguire questo comando...
------------------------	--------	-----------	----------------------------

Mhost Auditing	cambiamento di policy	[4719] Configurazione dell'audit modificata	`vserver audit disable
enable	modify`	condivisione file	[5142] è stata aggiunta la condivisione di rete
vserver cifs share create	[5143] la condivisione di rete è stata modificata	vserver cifs share modify `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144] condivisione di rete eliminata	vserver cifs share delete
Controllo	account utente	[4720] utente locale creato	vserver cifs users-and-groups local-user create vserver services name-service unix-user create
[4722] utente locale abilitato	`vserver cifs users-and-groups local-user create	modify`	[4724] reimpostazione della password utente locale
vserver cifs users-and-groups local-user set-password	[4725] utente locale disattivato	`vserver cifs users-and-groups local-user create	modify`
[4726] utente locale cancellato	vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete	[4738] Modifica utente locale	vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify
[4781] Rinomina utente locale	vserver cifs users-and-groups local-user rename	security-group	[4731] Gruppo di sicurezza locale creato
vserver cifs users-and-groups local-group create vserver services name-service unix-group create	[4734] Gruppo di sicurezza locale cancellato	vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete	[4735] Gruppo di sicurezza locale modificato

<code>`vserver cifs users-and-groups local-group rename`</code>	<code>modify` vserver services name-service unix-group modify`</code>	[4732] utente aggiunto al gruppo locale	<code>vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser`</code>
[4733] utente rimosso dal gruppo locale	<code>vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`</code>	authorization-policy-change	[4704] diritti utente assegnati
<code>vserver cifs users-and-groups privilege add-privilege`</code>	[4705] diritti utente rimossi	<code>`vserver cifs users-and-groups privilege remove-privilege`</code>	<code>reset-privilege`</code>

### Gestire l'evento di condivisione file

Quando viene configurato un evento di condivisione file per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit. Gli eventi di condivisione file vengono generati quando la condivisione di rete SMB viene modificata utilizzando `vserver cifs share` comandi correlati.

Gli eventi di file-share con gli id evento 5142, 5143 e 5144 vengono generati quando una condivisione di rete SMB viene aggiunta, modificata o eliminata per la SVM. La configurazione della condivisione di rete SMB viene modificata utilizzando `cifs share access control create|modify|delete` comandi.

Nell'esempio seguente viene visualizzato un evento di condivisione file con ID 5143, quando viene creato un oggetto di condivisione denominato 'audit\_dest':

```

netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  5142
  EventName Share Object Added
  ...
  ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;;FA;;;WD)

```

### Gestire l'evento audit-policy-change

Quando viene configurato un evento audit-policy-change per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit. Gli eventi audit-policy-change vengono generati quando un criterio di audit viene modificato utilizzando `vserver audit` comandi correlati.

L'evento audit-policy-change con l'id evento 4719 viene generato ogni volta che un criterio di audit viene disattivato, attivato o modificato e aiuta a identificare quando un utente tenta di disattivare il controllo per coprire le tracce. È configurato per impostazione predefinita e richiede il privilegio di diagnostica per la disattivazione.

Nell'esempio riportato di seguito viene visualizzato un evento di modifica della policy di audit con l'ID 4719 generato, quando un audit viene disattivato:

```

netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4719
  EventName Audit Disabled
  ...
  ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort

```

## Gestire l'evento dell'account utente

Quando viene configurato un evento account utente per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi dell'account utente con id evento 4720, 4722, 4724, 4725, 4726, 4738 e 4781 vengono generati quando un utente SMB o NFS locale viene creato o cancellato dal sistema, l'account utente locale viene attivato, disattivato o modificato e la password utente SMB locale viene reimpostata o modificata. Gli eventi dell'account utente vengono generati quando un account utente viene modificato utilizzando `vserver cifs users-and-groups <local user>e.vserver services name-service <unix user>` comandi.

Nell'esempio seguente viene visualizzato un evento dell'account utente con l'ID 4720 generato, quando viene creato un utente SMB locale:

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID   4720
  EventName Local Cifs User Created
  ...
  ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

Nell'esempio seguente viene visualizzato un evento dell'account utente con l'ID 4781 generato, quando l'utente SMB locale creato nell'esempio precedente viene rinominato:

```

netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4781
  EventName Local Cifs User Renamed
  ...
  ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~

```

## Gestire gli eventi del gruppo di sicurezza

Quando viene configurato un evento di gruppo di sicurezza per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi del gruppo di sicurezza con id evento 4731, 4732, 4733, 4734 e 4735 vengono generati quando un gruppo SMB o NFS locale viene creato o cancellato dal sistema e l'utente locale viene aggiunto o rimosso dal gruppo. Gli eventi-gruppo-sicurezza vengono generati quando un account utente viene modificato utilizzando `vserver cifs users-and-groups <local-group> e vserver services name-service <unix-group>` comandi.

Nell'esempio seguente viene visualizzato un evento del gruppo di protezione con l'ID 4731 generato quando viene creato un gruppo di protezione UNIX locale:



```

netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4731
  EventName Local Unix Security Group Created
  ...
  ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~

```

### Gestire l'evento Authorization-policy-change

Quando l'evento Authorization-policy-change viene configurato per una macchina virtuale di storage (SVM) e viene attivato un audit, vengono generati eventi di audit.

Gli eventi Authorization-policy-change con ID evento 4704 e 4705 vengono generati ogni volta che vengono concessi o revocati i diritti di autorizzazione per un utente SMB e un gruppo SMB. Gli eventi Authorization-policy-change vengono generati quando i diritti di autorizzazione vengono assegnati o revocati utilizzando `vserver cifs users-and-groups privilege` comandi correlati.

Nell'esempio seguente viene visualizzato un evento del criterio di autorizzazione con l'ID 4704 generato, quando vengono assegnati i diritti di autorizzazione per un gruppo di utenti SMB:

```

netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
- Provider
  [ Name]   NetApp-Security-Auditing
  [ Guid]   {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
  EventID  4704
  EventName User Right Assigned
  ...
  ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
  SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS

```

## Gestire le configurazioni di controllo

### Ruotare manualmente i registri degli eventi di audit

Prima di poter visualizzare i registri degli eventi di audit, è necessario convertirli in formati leggibili dall'utente. Se si desidera visualizzare i registri degli eventi per una specifica macchina virtuale di storage prima che ONTAP ruoti automaticamente il registro, è possibile ruotare manualmente i registri degli eventi di audit su una SVM.

#### Fase

1. Ruotare i registri degli eventi di audit utilizzando `vserver audit rotate-log` comando.

```
vserver audit rotate-log -vserver vs1
```

Il registro eventi di audit viene salvato nella directory del registro eventi di audit SVM con il formato specificato dalla configurazione di audit (XML oppure EVTX), e possono essere visualizzati utilizzando l'applicazione appropriata.

### Abilitare e disabilitare il controllo sulle SVM

È possibile attivare o disattivare il controllo sulle macchine virtuali di storage (SVM). È possibile interrompere temporaneamente il controllo di file e directory disattivando il controllo. È possibile attivare il controllo in qualsiasi momento (se esiste una configurazione di controllo).

#### Di cosa hai bisogno

Prima di poter attivare il controllo su SVM, la configurazione di controllo di SVM deve già esistere.

## "Creare la configurazione di controllo"

### A proposito di questa attività

La disattivazione del controllo non elimina la configurazione del controllo.

### Fasi

1. Eseguire il comando appropriato:

Se si desidera che il controllo sia...	Immettere il comando...
Attivato	<code>vserver audit enable -vserver vserver_name</code>
Disattivato	<code>vserver audit disable -vserver vserver_name</code>

2. Verificare che il controllo si trovi nello stato desiderato:

```
vserver audit show -vserver vserver_name
```

### Esempi

Nell'esempio seguente viene attivato il controllo per SVM vs1:

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                Vserver: vs1
        Auditing state: true
    Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtv
        Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
                Rotation Schedules: -
        Log Files Rotation Limit: 10
```

Nell'esempio seguente viene disattivato il controllo per SVM vs1:

```
cluster1::> vserver audit disable -vserver vs1
```

```

                Vserver: vs1
            Auditing state: false
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops, cifs-logon-logoff
                Log Format: evtX
            Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
            Log Rotation Schedule: Day: -
            Log Rotation Schedule: Hour: -
        Log Rotation Schedule: Minute: -
                Rotation Schedules: -
            Log Files Rotation Limit: 10
```

## Visualizzare le informazioni relative al controllo delle configurazioni

È possibile visualizzare le informazioni relative al controllo delle configurazioni. Le informazioni consentono di determinare se la configurazione è quella desiderata per ogni SVM. Le informazioni visualizzate consentono inoltre di verificare se è attivata una configurazione di controllo.

### A proposito di questa attività

È possibile visualizzare informazioni dettagliate sulle configurazioni di controllo su tutte le SVM oppure personalizzare le informazioni visualizzate nell'output specificando i parametri opzionali. Se non si specifica alcun parametro opzionale, viene visualizzato quanto segue:

- Nome SVM a cui si applica la configurazione di controllo
- Lo stato di audit, che può essere `true` oppure `false`

Se lo stato di audit è `true`, il controllo è attivato. Se lo stato di audit è `false`, il controllo è disattivato.

- Le categorie di eventi da controllare
- Il formato del registro di controllo
- La directory di destinazione in cui il sottosistema di controllo memorizza i registri di controllo consolidati e convertiti

### Fase

1. Visualizzare le informazioni sulla configurazione di controllo utilizzando `vserver audit show` comando.

Per ulteriori informazioni sull'utilizzo del comando, vedere le pagine `man`.

### Esempi

Nell'esempio seguente viene visualizzato un riepilogo della configurazione di controllo per tutte le SVM:

```
cluster1::> vserver audit show
```

Vserver	State	Event Types	Log Format	Target Directory
vs1	false	file-ops	evtx	/audit_log

Nell'esempio seguente vengono visualizzate, sotto forma di elenco, tutte le informazioni di configurazione per il controllo di tutte le SVM:

```
cluster1::> vserver audit show -instance
```

```

                Vserver: vs1
            Auditing state: true
        Log Destination Path: /audit_log
Categories of Events to Audit: file-ops
            Log Format: evtx
        Log File Size Limit: 100MB
    Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
            Log Rotation Schedule: Hour: -
    Log Rotation Schedule: Minute: -
        Rotation Schedules: -
        Log Files Rotation Limit: 0
```

### Comandi per la modifica delle configurazioni di controllo

Se si desidera modificare un'impostazione di controllo, è possibile modificare la configurazione corrente in qualsiasi momento, tra cui la modifica della destinazione del percorso di log e del formato di log, la modifica delle categorie di eventi da controllare, la modalità di salvataggio automatico dei file di log e il numero massimo di file di log da salvare.

Se si desidera...	Utilizzare questo comando...
Modificare il percorso di destinazione del log	<code>vserver audit modify</code> con <code>-destination</code> parametro

Modificare la categoria di eventi da controllare	vserver audit modify con <b>-events</b> parametro  <div>  <p>Per controllare gli eventi di staging dei criteri di accesso centrale, è necessario attivare l'opzione del server SMB DAC (Dynamic Access Control) sulla macchina virtuale di storage (SVM).</p> </div>
Modificare il formato del registro	vserver audit modify con <b>-format</b> parametro
Attivazione dei salvataggi automatici in base alle dimensioni interne del file di log	vserver audit modify con <b>-rotate-size</b> parametro
Attivazione dei salvataggi automatici in base a un intervallo di tempo	vserver audit modify con <b>-rotate-schedule-month, -rotate-schedule-dayofweek, -rotate-schedule-day, -rotate-schedule-hour, e. -rotate-schedule-minute</b> parametri
Specifica del numero massimo di file di log salvati	vserver audit modify con <b>-rotate-limit</b> parametro

## Eliminare una configurazione di controllo

Se non si desidera più controllare gli eventi di file e directory sulla macchina virtuale di storage (SVM) e non si desidera mantenere una configurazione di controllo sulla SVM, è possibile eliminare la configurazione di controllo.

### Fasi

1. Disattivare la configurazione di controllo:

```
vserver audit disable -vserver vserver_name
```

```
vserver audit disable -vserver vs1
```

2. Eliminare la configurazione di controllo:

```
vserver audit delete -vserver vserver_name
```

```
vserver audit delete -vserver vs1
```

## Comprendere le implicazioni del ripristino del cluster

Se si prevede di ripristinare il cluster, è necessario conoscere il processo di revert che ONTAP segue quando nel cluster sono presenti macchine virtuali di storage abilitate per l'auditing. È necessario eseguire determinate azioni prima di eseguire il ripristino.

## Ripristino di una versione di ONTAP che non supporta il controllo degli eventi di logon e logoff SMB e degli eventi di staging dei criteri di accesso centrale

Il supporto per il controllo degli eventi di logon e logoff SMB e per gli eventi di staging dei criteri di accesso centrale inizia con Clustered Data ONTAP 8.3. Se si ripristina una versione di ONTAP che non supporta questi tipi di eventi e si dispone di configurazioni di controllo che monitorano questi tipi di eventi, è necessario modificare la configurazione di controllo per tali SVM abilitate all'audit prima di eseguire il ripristino. È necessario modificare la configurazione in modo che vengano controllati solo gli eventi del file-op.

## Risolvere i problemi di auditing e di gestione dello spazio dei volumi

Possono verificarsi problemi quando lo spazio disponibile sui volumi di staging o sul volume contenente i registri degli eventi di audit è insufficiente. Se lo spazio è insufficiente, non è possibile creare nuovi record di audit, impedendo ai client di accedere ai dati e impedendo l'esecuzione delle richieste di accesso. Dovresti sapere come risolvere questi problemi di spazio del volume.

### Risolvere i problemi di spazio relativi ai volumi del registro eventi

Se i volumi contenenti file di log degli eventi esauriranno lo spazio, il controllo non potrà convertire i record di log in file di log. Ciò comporta errori di accesso al client. È necessario sapere come risolvere i problemi di spazio relativi ai volumi del registro eventi.

- Gli amministratori delle macchine virtuali di storage (SVM) e dei cluster possono determinare se lo spazio dei volumi è insufficiente visualizzando informazioni sull'utilizzo e la configurazione dei volumi e degli aggregati.
- Se lo spazio disponibile nei volumi contenenti registri eventi è insufficiente, gli amministratori di SVM e cluster possono risolvere i problemi di spazio rimuovendo alcuni file di registro eventi o aumentando le dimensioni del volume.



Se l'aggregato che contiene il volume del registro eventi è pieno, è necessario aumentare le dimensioni dell'aggregato prima di poter aumentare le dimensioni del volume. Solo un amministratore del cluster può aumentare le dimensioni di un aggregato.

- Il percorso di destinazione dei file di registro eventi può essere modificato in una directory di un altro volume modificando la configurazione di controllo.



L'accesso ai dati viene negato nei seguenti casi:

- Se la directory di destinazione viene eliminata.
- Se il limite di file su un volume, che ospita la directory di destinazione, raggiunge il livello massimo.

Scopri di più su:

- ["Come visualizzare informazioni sui volumi e aumentare le dimensioni del volume"](#).
- ["Come visualizzare informazioni sugli aggregati e sulla gestione degli aggregati"](#).

## Risolvere i problemi di spazio relativi ai volumi di staging

Se uno dei volumi contenenti file di staging per la macchina virtuale di storage (SVM) esaurisce lo spazio, il controllo non può scrivere record di log nei file di staging. Ciò comporta errori di accesso al client. Per risolvere questo problema, è necessario determinare se uno dei volumi di staging utilizzati nella SVM è pieno visualizzando le informazioni sull'utilizzo del volume.

Se il volume contenente i file di registro eventi consolidati dispone di spazio sufficiente ma si verificano ancora errori di accesso del client a causa di spazio insufficiente, i volumi di staging potrebbero essere fuori spazio. L'amministratore di SVM deve contattare l'utente per determinare se i volumi di staging che contengono file di staging per SVM hanno spazio insufficiente. Il sottosistema di controllo genera un evento EMS se non è possibile generare eventi di controllo a causa dello spazio insufficiente in un volume di staging. Viene visualizzato il seguente messaggio: `No space left on device`. Solo gli amministratori SVM possono visualizzare informazioni sui volumi di staging.

Tutti i nomi dei volumi di staging iniziano con `MDV_aud_` Seguito dall'UUID dell'aggregato contenente il volume di staging. L'esempio seguente mostra quattro volumi di sistema sulla SVM amministrativa, creati automaticamente quando è stata creata una configurazione di controllo dei file service per una SVM di dati nel cluster:

```
cluster1::> volume show -vserver cluster1
```

Vserver	Volume	Aggregate	State	Type	Size	Available
Used%						
-----	-----	-----	-----	-----	-----	-----
-----						
cluster1	MDV_aud_1d0131843d4811e296fc123478563412	aggr0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_8be27f813d7311e296fc123478563412	root_vs0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_9dc4ad503d7311e296fc123478563412	aggr1	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_a4b887ac3d7311e296fc123478563412	aggr2	online	RW	2GB	1.90GB
5%						

4 entries were displayed.

Se lo spazio disponibile nei volumi di staging è insufficiente, è possibile risolvere i problemi di spazio aumentando le dimensioni del volume.



Se l'aggregato che contiene il volume di staging è pieno, è necessario aumentare le dimensioni dell'aggregato prima di poter aumentare le dimensioni del volume. Solo gli amministratori di SVM possono aumentare le dimensioni di un aggregato.

Se uno o più aggregati hanno uno spazio disponibile inferiore a 2 GB, la creazione dell'audit SVM non riesce. Quando la creazione dell'audit SVM non riesce, i volumi di staging creati vengono cancellati.



# Utilizzare FPolicy per il monitoraggio e la gestione dei file su SVM

## Comprendere FPolicy

### Quali sono le due parti della soluzione FPolicy

FPolicy è un framework di notifica dell'accesso ai file utilizzato per monitorare e gestire gli eventi di accesso ai file sulle macchine virtuali di storage (SVM) attraverso le soluzioni dei partner. Le soluzioni dei partner ti aiutano a risolvere diversi casi di utilizzo, ad esempio governance e conformità dei dati, protezione ransomware e mobilità dei dati.

Le soluzioni dei partner includono soluzioni di terze parti supportate da NetApp e prodotti NetApp per la sicurezza del carico di lavoro e il rilevamento dei dati nel cloud.

Una soluzione FPolicy è composta da due parti. Il framework FPolicy di ONTAP gestisce le attività sul cluster e invia notifiche all'applicazione partner (alias server FPolicy esterni). I server FPolicy esterni elaborano le notifiche inviate da ONTAP FPolicy per soddisfare i casi di utilizzo dei clienti.

Il framework ONTAP crea e gestisce la configurazione di FPolicy, monitora gli eventi dei file e invia notifiche ai server FPolicy esterni. ONTAP FPolicy fornisce l'infrastruttura che consente la comunicazione tra server FPolicy esterni e nodi SVM (Storage Virtual Machine).

Il framework FPolicy si connette ai server FPolicy esterni e invia notifiche per determinati eventi del file system ai server FPolicy quando questi eventi si verificano in seguito all'accesso del client. I server FPolicy esterni elaborano le notifiche e inviano le risposte al nodo. Ciò che accade in seguito all'elaborazione delle notifiche dipende dall'applicazione e dal fatto che la comunicazione tra il nodo e i server esterni sia asincrona o sincrona.

### Quali sono le notifiche sincrone e asincrone

FPolicy invia notifiche ai server FPolicy esterni tramite l'interfaccia FPolicy. Le notifiche vengono inviate in modalità sincrona o asincrona. La modalità di notifica determina le operazioni di ONTAP dopo l'invio di notifiche ai server FPolicy.

- **Notifiche asincrone**

Con le notifiche asincrone, il nodo non attende una risposta dal server FPolicy, che migliora il throughput complessivo del sistema. Questo tipo di notifica è adatto alle applicazioni in cui il server FPolicy non richiede che venga intrapresa alcuna azione in seguito alla valutazione della notifica. Ad esempio, le notifiche asincrone vengono utilizzate quando l'amministratore della macchina virtuale di storage (SVM) desidera monitorare e controllare l'attività di accesso ai file.

Se un server FPolicy che opera in modalità asincrona subisce un'interruzione di rete, le notifiche FPolicy generate durante l'interruzione vengono memorizzate nel nodo di storage. Quando il server FPolicy torna in linea, viene avvisato delle notifiche memorizzate e può recuperarle dal nodo di storage. Il periodo di tempo in cui le notifiche possono essere memorizzate durante un'interruzione è configurabile fino a 10 minuti.

A partire da ONTAP 9.14.1, FPolicy consente di configurare un archivio persistente per acquisire eventi di accesso ai file per policy asincrone non obbligatorie nella SVM. Gli archivi persistenti possono aiutare a separare l'elaborazione i/o dei client dall'elaborazione delle notifiche FPolicy per ridurre la latenza dei

client. Le configurazioni obbligatorie sincrone (obbligatorie o non obbligatorie) e asincrone non sono supportate.

- **Notifiche sincrone**

Se configurato per l'esecuzione in modalità sincrone, il server FPolicy deve riconoscere ogni notifica prima che l'operazione del client possa continuare. Questo tipo di notifica viene utilizzato quando è richiesta un'azione in base ai risultati della valutazione della notifica. Ad esempio, le notifiche sincrone vengono utilizzate quando l'amministratore SVM desidera consentire o negare le richieste in base ai criteri specificati sul server FPolicy esterno.

### **Applicazioni sincrone e asincrone**

Esistono molti possibili utilizzi per le applicazioni FPolicy, sia asincrone che sincrone.

Le applicazioni asincrone sono quelle in cui il server FPolicy esterno non altera l'accesso a file o directory o non modifica i dati sulla macchina virtuale di storage (SVM). Ad esempio:

- Accesso al file e registrazione dell'audit
- Gestione delle risorse dello storage

Le applicazioni sincrone sono quelle in cui l'accesso ai dati viene alterato o i dati vengono modificati dal server FPolicy esterno. Ad esempio:

- Gestione delle quote
- Blocco dell'accesso al file
- Archiviazione dei file e gestione dello storage gerarchico
- Servizi di crittografia e decrittografia
- Servizi di compressione e decompressione

### **Archivi persistenti di FPolicy**

A partire da ONTAP 9.14.1, FPolicy consente di configurare un archivio persistente per acquisire eventi di accesso ai file per policy asincrone non obbligatorie nella SVM. Gli archivi persistenti possono aiutare a separare l'elaborazione i/o dei client dall'elaborazione delle notifiche FPolicy per ridurre la latenza dei client. Le configurazioni obbligatorie sincrone (obbligatorie o non obbligatorie) e asincrone non sono supportate.

Questa funzione è disponibile solo in modalità FPolicy esterna. L'applicazione partner utilizzata deve supportare questa funzione. È necessario collaborare con il proprio partner per assicurarsi che questa configurazione FPolicy sia supportata.

### **Best practice**

Gli amministratori del cluster devono configurare un volume per l'archivio persistente in ciascuna SVM dove FPolicy è abilitato. Una volta configurato, un archivio persistente acquisisce tutti gli eventi FPolicy corrispondenti, che vengono ulteriormente elaborati nella pipeline FPolicy e inviati al server esterno.

L'archivio persistente rimane invariato quando è stato ricevuto l'ultimo evento quando si verifica un riavvio imprevisto o FPolicy viene disattivato e riattivato. Dopo un'operazione di takeover, i nuovi eventi verranno memorizzati ed elaborati dal nodo partner. Dopo un'operazione di giveback, l'archivio persistente riprende

l'elaborazione degli eventi non elaborati che potrebbero rimanere dal momento in cui si è verificato il takeover del nodo. Gli eventi live avrebbero la priorità rispetto agli eventi non elaborati.

Se il volume dell'archivio persistente si sposta da un nodo a un altro nella stessa SVM, le notifiche che non sono ancora state elaborate verranno spostate anche nel nuovo nodo. Sarà necessario eseguire nuovamente `fpolicy persistent-store create` su uno dei nodi dopo lo spostamento del volume, per garantire che la notifica in sospeso venga inviata al server esterno.

Il volume dello storage persistente viene configurato in base alle singole SVM. Per ogni SVM abilitata per FPolicy dovrai creare un volume archivio persistente.

Crea il volume di archivio persistente sul nodo con LIF che prevedono il monitoraggio del traffico massimo da parte di Fpolicy.

Se le notifiche accumulate nell'archivio permanente superano le dimensioni del volume fornito, FPolicy inizia a interrompere la notifica in arrivo con i messaggi EMS appropriati.

Il nome del volume di archiviazione persistente e il percorso di giunzione specificati al momento della creazione del volume dovrebbero corrispondere.

Impostare il criterio snapshot su `none` per quel volume invece di `default`. In questo modo si garantisce che non vi sia alcun ripristino accidentale dello snapshot che causa la perdita degli eventi correnti e per impedire un'eventuale elaborazione di eventi duplicati.

Rendere il volume dell'archivio persistente inaccessibile per l'accesso al protocollo utente esterno (CIFS/NFS) per evitare il danneggiamento accidentale o l'eliminazione dei record di eventi persistenti. Per ottenere questo risultato, dopo aver attivato FPolicy, smontare il volume in ONTAP per rimuovere il percorso di giunzione; ciò lo rende inaccessibile per l'accesso al protocollo utente.

Per ulteriori informazioni, vedere ["Creare archivi persistenti"](#).

## Tipi di configurazione FPolicy

Esistono due tipi di configurazione FPolicy di base. Una configurazione utilizza server FPolicy esterni per elaborare e agire in base alle notifiche. L'altra configurazione non utilizza server FPolicy esterni, ma utilizza il server FPolicy nativo interno di ONTAP per un semplice blocco dei file basato sulle estensioni.

- **Configurazione del server FPolicy esterno**

La notifica viene inviata al server FPolicy, che vaglia la richiesta e applica le regole per determinare se il nodo deve consentire l'operazione di file richiesta. Per i criteri sincroni, il server FPolicy invia quindi una risposta al nodo per consentire o bloccare l'operazione di file richiesta.

- **Configurazione del server FPolicy nativo**

La notifica viene sottoposta a screening interno. La richiesta viene consentita o negata in base alle impostazioni di estensione del file configurate nell'ambito FPolicy.

**Nota:** Le richieste di estensione del file negate non vengono registrate.

## Quando creare una configurazione FPolicy nativa

Le configurazioni FPolicy native utilizzano il motore FPolicy interno di ONTAP per monitorare e bloccare le

operazioni dei file in base all'estensione del file. Questa soluzione non richiede server FPolicy esterni (server FPolicy). L'utilizzo di una configurazione nativa per il blocco dei file è appropriato quando questa semplice soluzione è tutto ciò che serve.

Il blocco nativo dei file consente di monitorare le operazioni dei file che corrispondono alle operazioni configurate e agli eventi di filtraggio, negando quindi l'accesso ai file con estensioni particolari. Questa è la configurazione predefinita.

Questa configurazione consente di bloccare l'accesso al file solo in base all'estensione del file. Ad esempio, per bloccare i file che contengono `mp3` extensions (estensioni), viene configurato un criterio per fornire notifiche per determinate operazioni con estensioni file di destinazione di `mp3`. Il criterio è configurato per negare `mp3` richieste di file per operazioni che generano notifiche.

Quanto segue si applica alle configurazioni FPolicy native:

- Lo stesso set di filtri e protocolli supportati dallo screening dei file basato su server FPolicy è supportato anche per il blocco dei file nativi.
- È possibile configurare contemporaneamente le applicazioni di blocco dei file nativi e di screening dei file basate su server FPolicy.

A tale scopo, è possibile configurare due policy FPolicy separate per la macchina virtuale di storage (SVM), una configurata per il blocco dei file nativi e una configurata per lo screening dei file basato su server FPolicy.

- La funzione di blocco dei file nativi consente di visualizzare solo i file in base alle estensioni e non in base al contenuto del file.
- Nel caso di collegamenti simbolici, il blocco dei file nativi utilizza l'estensione del file root.

Scopri di più ["FPolicy: Blocco dei file nativi"](#).

#### **Quando creare una configurazione che utilizza server FPolicy esterni**

Le configurazioni FPolicy che utilizzano server FPolicy esterni per elaborare e gestire le notifiche offrono soluzioni efficaci per i casi di utilizzo in cui è necessario un blocco dei file più semplice basato sull'estensione dei file.

È necessario creare una configurazione che utilizzi server FPolicy esterni quando si desidera eseguire operazioni quali il monitoraggio e la registrazione degli eventi di accesso ai file, fornire servizi di quota, eseguire il blocco dei file in base a criteri diversi dalle semplici estensioni dei file, fornire servizi di migrazione dei dati utilizzando applicazioni di gestione dello storage gerarchiche. In alternativa, è possibile fornire un insieme di policy dettagliato che monitorano solo un sottoinsieme di dati nella macchina virtuale di storage (SVM).

#### **Ruoli che i componenti del cluster giocano con l'implementazione di FPolicy**

Il cluster, le SVM (Storage Virtual Machine) contenute e le LIF dei dati svolgono un ruolo fondamentale in un'implementazione FPolicy.

- **cluster**

Il cluster contiene il framework di gestione FPolicy e gestisce e gestisce le informazioni su tutte le configurazioni FPolicy nel cluster.

- **SVM**

Viene definita una configurazione FPolicy a livello di SVM. L'ambito della configurazione è SVM e funziona solo con le risorse SVM. Una configurazione SVM non è in grado di monitorare e inviare notifiche per le richieste di accesso ai file effettuate per i dati che risiedono su un'altra SVM.

Le configurazioni FPolicy possono essere definite sulla SVM amministrativa. Una volta definite le configurazioni sulla SVM amministrativa, queste possono essere visualizzate e utilizzate in tutte le SVM.

- **LIF dati**

Le connessioni ai server FPolicy vengono effettuate tramite i LIF dei dati appartenenti a SVM con la configurazione FPolicy. I dati LIF utilizzati per queste connessioni possono eseguire il failover nello stesso modo dei dati LIF utilizzati per il normale accesso client.

## **Funzionamento di FPolicy con i server FPolicy esterni**

Dopo aver configurato e attivato FPolicy sulla macchina virtuale di storage (SVM), FPolicy viene eseguito su ogni nodo a cui partecipa SVM. FPolicy è responsabile della creazione e della gestione delle connessioni con server FPolicy esterni (server FPolicy), dell'elaborazione delle notifiche e della gestione dei messaggi di notifica da e verso i server FPolicy.

Inoltre, nell'ambito della gestione delle connessioni, FPolicy ha le seguenti responsabilità:

- Garantisce che la notifica del file scorra attraverso la LIF corretta al server FPolicy.
- Garantisce che quando più server FPolicy sono associati a un criterio, il bilanciamento del carico viene eseguito quando si inviano notifiche ai server FPolicy.
- Tenta di ristabilire la connessione in caso di interruzione della connessione a un server FPolicy.
- Invia le notifiche ai server FPolicy in una sessione autenticata.
- Gestisce la connessione dati pass-through-Read stabilita dal server FPolicy per gestire le richieste del client quando è attivata la funzione pass-through-Read.

## **Come vengono utilizzati i canali di controllo per la comunicazione FPolicy**

FPolicy avvia una connessione del canale di controllo a un server FPolicy esterno dalle LIF dei dati di ciascun nodo che partecipa a una macchina virtuale di storage (SVM). FPolicy utilizza canali di controllo per la trasmissione delle notifiche dei file; pertanto, un server FPolicy potrebbe visualizzare più connessioni dei canali di controllo in base alla topologia SVM.

## **Come vengono utilizzati i canali di accesso privilegiato ai dati per le comunicazioni sincrone**

Con i casi di utilizzo sincroni, il server FPolicy accede ai dati che risiedono sulla macchina virtuale di storage (SVM) attraverso un percorso di accesso privilegiato ai dati. L'accesso attraverso il percorso privilegiato espone l'intero file system al server FPolicy. Il reparto IT può accedere ai file di dati per raccogliere informazioni, scansare file, leggere file o scrivere in file.

Poiché il server FPolicy esterno può accedere all'intero file system dalla directory principale di SVM attraverso il canale dati privilegiato, la connessione del canale dati privilegiato deve essere sicura.

## **Modalità di utilizzo delle credenziali di connessione FPolicy con i canali di accesso privilegiato ai dati**

Il server FPolicy effettua connessioni privilegiate di accesso ai dati ai nodi del cluster utilizzando una specifica credenziale utente Windows che viene salvata con la configurazione FPolicy. SMB è l'unico protocollo

supportato per la connessione di un canale di accesso privilegiato ai dati.

Se il server FPolicy richiede un accesso privilegiato ai dati, devono essere soddisfatte le seguenti condizioni:

- Sul cluster deve essere attivata una licenza SMB.
- Il server FPolicy deve essere eseguito con le credenziali configurate nella configurazione FPolicy.

Quando si effettua una connessione al canale dati, FPolicy utilizza la credenziale per il nome utente Windows specificato. L'accesso ai dati avviene tramite la condivisione amministrativa ONTAP\_ADMIN.

#### **Cosa significa concedere credenziali super utente per l'accesso privilegiato ai dati**

ONTAP utilizza la combinazione dell'indirizzo IP e della credenziale utente configurata nella configurazione FPolicy per assegnare credenziali super utente al server FPolicy.

Quando il server FPolicy accede ai dati, lo stato di Super User concede i seguenti privilegi:

- Evitare controlli delle autorizzazioni

L'utente evita di controllare i file e l'accesso alla directory.

- Speciali privilegi di blocco

ONTAP consente l'accesso in lettura, scrittura o modifica a qualsiasi file, indipendentemente dai blocchi esistenti. Se il server FPolicy utilizza blocchi di intervallo di byte sul file, si ottiene la rimozione immediata dei blocchi esistenti sul file.

- Ignorare eventuali controlli FPolicy

Access non genera alcuna notifica FPolicy.

#### **In che modo FPolicy gestisce l'elaborazione delle policy**

Alla macchina virtuale di storage (SVM) potrebbero essere assegnati più criteri FPolicy, ciascuno con una priorità diversa. Per creare una configurazione FPolicy appropriata sulla SVM, è importante comprendere come FPolicy gestisce l'elaborazione delle policy.

Ogni richiesta di accesso al file viene inizialmente valutata per determinare quali policy monitorano questo evento. Se si tratta di un evento monitorato, le informazioni sull'evento monitorato e le policy interessate vengono trasmesse a FPolicy, dove vengono valutate. Ogni policy viene valutata in base alla priorità assegnata.

Durante la configurazione dei criteri, è necessario prendere in considerazione i seguenti consigli:

- Se si desidera che un criterio venga sempre valutato prima di altri criteri, configurarlo con una priorità più alta.
- Se il successo dell'operazione di accesso al file richiesta in un evento monitorato è un prerequisito per una richiesta di file che viene valutata in base a un altro criterio, assegnare una priorità maggiore alla policy che controlla il successo o l'errore della prima operazione di file.

Ad esempio, se un criterio gestisce la funzionalità di archiviazione e ripristino dei file FPolicy e un secondo criterio gestisce le operazioni di accesso ai file sul file online, il criterio che gestisce il ripristino dei file deve avere una priorità più alta in modo che il file venga ripristinato prima di poter consentire l'operazione gestita dal secondo criterio.

- Se si desidera valutare tutti i criteri applicabili a un'operazione di accesso ai file, assegnare una priorità inferiore ai criteri sincroni.

È possibile riordinare le priorità dei criteri per i criteri esistenti modificando il numero di sequenza dei criteri. Tuttavia, per fare in modo che FPolicy valuti i criteri in base all'ordine di priorità modificato, è necessario disattivare e riabilitare il criterio con il numero di sequenza modificato.

### **Qual è il processo di comunicazione da nodo a server FPolicy esterno**

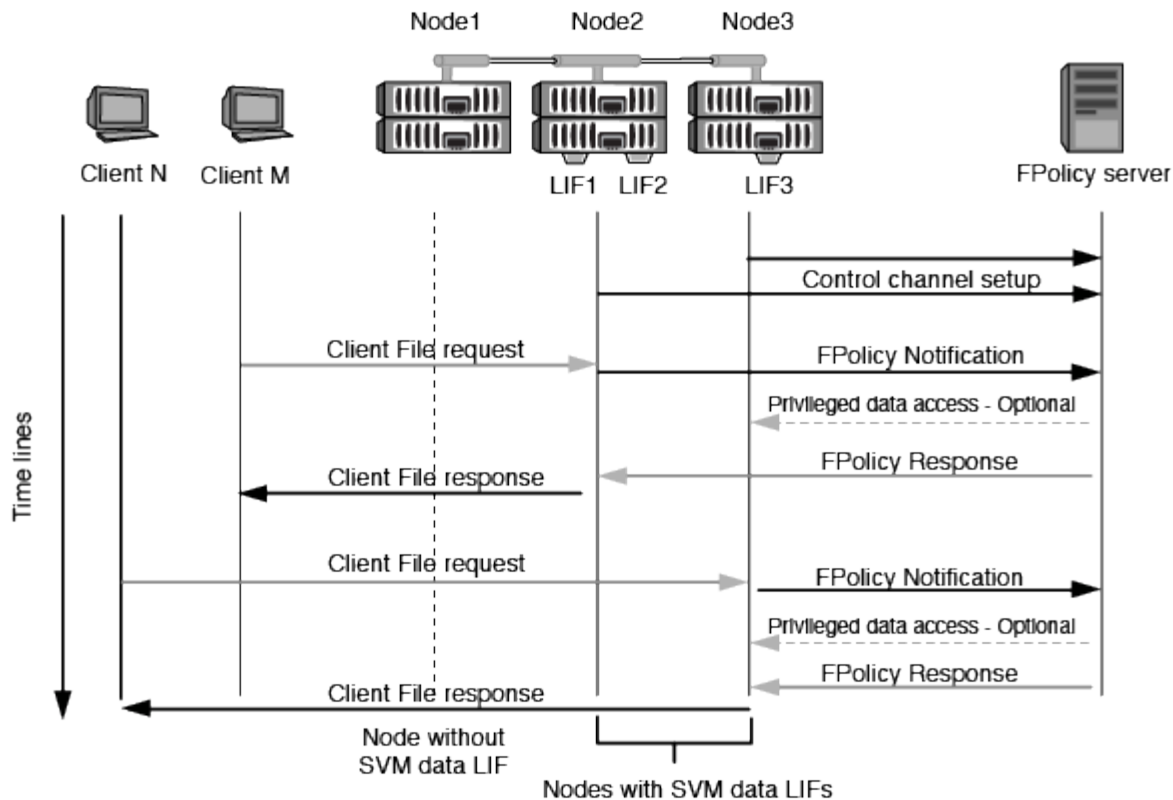
Per pianificare correttamente la configurazione di FPolicy, è necessario comprendere il processo di comunicazione da nodo a server FPolicy esterno.

Ogni nodo che partecipa a ciascuna macchina virtuale di storage (SVM) avvia una connessione a un server FPolicy esterno (server FPolicy) utilizzando TCP/IP. Le connessioni ai server FPolicy vengono configurate utilizzando LIF dei dati dei nodi; pertanto, un nodo partecipante può impostare una connessione solo se il nodo dispone di una LIF dei dati operativi per SVM.

Ogni processo FPolicy sui nodi partecipanti tenta di stabilire una connessione con il server FPolicy quando il criterio è attivato. Utilizza l'indirizzo IP e la porta del motore esterno FPolicy specificato nella configurazione del criterio.

La connessione stabilisce un canale di controllo da ciascuno dei nodi che partecipano a ciascuna SVM al server FPolicy attraverso la LIF dei dati. Inoltre, se gli indirizzi LIF dei dati IPv4 e IPv6 sono presenti sullo stesso nodo partecipante, FPolicy tenta di stabilire connessioni sia per IPv4 che per IPv6. Pertanto, in uno scenario in cui la SVM si estende su più nodi o se sono presenti entrambi gli indirizzi IPv4 e IPv6, il server FPolicy deve essere pronto per più richieste di configurazione del canale di controllo dal cluster dopo che la policy FPolicy è stata attivata sulla SVM.

Ad esempio, se un cluster ha tre nodi - Node1, Node2 e node3 - e le LIF dei dati SVM sono distribuite solo su Node2 e node3, i canali di controllo vengono avviati solo da Node2 e node3, indipendentemente dalla distribuzione dei volumi di dati. Si supponga che Node2 abbia due LIF di dati (LIF e LF2) che appartengono alla SVM e che la connessione iniziale sia da LIF. In caso di errore di LIF, FPolicy tenta di stabilire un canale di controllo da LIE2.



#### Come FPolicy gestisce le comunicazioni esterne durante la migrazione LIF o il failover

È possibile migrare le LIF dei dati nelle porte dati dello stesso nodo o nelle porte dati di un nodo remoto.

Quando si esegue il failover o la migrazione di una LIF dati, viene stabilita una nuova connessione del canale di controllo al server FPolicy. FPolicy può quindi riprovare le richieste dei client SMB e NFS in timeout, con il risultato che le nuove notifiche vengono inviate ai server FPolicy esterni. Il nodo rifiuta le risposte del server FPolicy alle richieste SMB e NFS originali, con timeout.

#### Come FPolicy gestisce le comunicazioni esterne durante il failover del nodo

Se il nodo del cluster che ospita le porte dati utilizzate per la comunicazione FPolicy non riesce, ONTAP interrompe la connessione tra il server FPolicy e il nodo.

L'impatto del failover del cluster sul server FPolicy può essere mitigato configurando il criterio di failover per migrare la porta dati utilizzata nella comunicazione FPolicy a un altro nodo attivo. Una volta completata la migrazione, viene stabilita una nuova connessione utilizzando la nuova porta dati.

Se il criterio di failover non è configurato per migrare la porta dati, il server FPolicy deve attendere che venga visualizzato il nodo guasto. Una volta attivato il nodo, viene avviata una nuova connessione da quel nodo con un nuovo ID sessione.



Il server FPolicy rileva le connessioni interrotte con il messaggio del protocollo Keep-alive. Il timeout per l'eliminazione dell'ID sessione viene determinato durante la configurazione di FPolicy. Il timeout di mantenimento predefinito è di due minuti.

#### Come funzionano i servizi FPolicy negli spazi dei nomi SVM

ONTAP offre uno spazio dei nomi di una macchina virtuale di storage unificata (SVM). I



volumi nel cluster vengono Uniti da giunzioni per fornire un singolo file system logico. Il server FPolicy è a conoscenza della topologia dello spazio dei nomi e fornisce i servizi FPolicy attraverso lo spazio dei nomi.

Lo spazio dei nomi è specifico e contenuto all'interno di SVM; pertanto, è possibile visualizzare lo spazio dei nomi solo dal contesto SVM. Gli spazi dei nomi hanno le seguenti caratteristiche:

- In ogni SVM esiste un singolo namespace, con la radice dello spazio dei nomi come volume root, rappresentata nello spazio dei nomi come barra (/).
- Tutti gli altri volumi hanno punti di giunzione sotto la radice (/).
- Le giunzioni dei volumi sono trasparenti per i client.
- Una singola esportazione NFS può fornire l'accesso all'intero namespace; in caso contrario, le policy di esportazione possono esportare volumi specifici.
- Le condivisioni SMB possono essere create sul volume o su qtree all'interno del volume o su qualsiasi directory all'interno dello spazio dei nomi.
- L'architettura dello spazio dei nomi è flessibile.

Di seguito sono riportati alcuni esempi di architetture di namespace tipiche:

- Uno spazio dei nomi con una singola diramazione fuori dalla directory principale
- Uno spazio dei nomi con più diramazioni al di fuori della radice
- Uno spazio dei nomi con più volumi non ramificati fuori dalla directory principale

### **In che modo FPolicy pass-through-Read migliora l'usabilità per la gestione dello storage gerarchico**

La funzione pass-through-Read consente al server FPolicy (che funge da server HSM) di fornire l'accesso in lettura ai file offline senza dover richiamare il file dal sistema di storage secondario al sistema di storage primario.

Quando un server FPolicy è configurato per fornire HSM ai file che risiedono su un server SMB, si verifica una migrazione dei file basata su policy in cui i file sono memorizzati offline sullo storage secondario e solo un file stub rimane sullo storage primario. Anche se un file stub viene visualizzato come un file normale per i client, in realtà è un file sparse che ha le stesse dimensioni del file originale. Il file sparse ha il bit SMB offline impostato e punta al file effettivo che è stato migrato allo storage secondario.

In genere, quando si riceve una richiesta di lettura per un file offline, il contenuto richiesto deve essere richiamato allo storage primario e quindi accessibile attraverso lo storage primario. La necessità di richiamare i dati sullo storage primario ha diversi effetti indesiderati. Tra gli effetti indesiderati vi è la maggiore latenza per le richieste dei client causata dalla necessità di richiamare il contenuto prima di rispondere alla richiesta e l'aumento del consumo di spazio necessario per i file richiamati sullo storage primario.

FPolicy pass-through-Read consente al server HSM (il server FPolicy) di fornire l'accesso in lettura ai file migrati offline senza dover richiamare il file dal sistema di storage secondario al sistema di storage primario. Invece di richiamare i file sullo storage primario, le richieste di lettura possono essere gestite direttamente dallo storage secondario.



L'offload della copia (ODX) non è supportato con l'operazione di pass-through-lettura FPolicy.

La lettura pass-through migliora l'usabilità fornendo i seguenti vantaggi:

- Le richieste di lettura possono essere gestite anche se lo storage primario non dispone di spazio sufficiente per richiamare i dati richiesti nello storage primario.
- Migliore gestione della capacità e delle performance in caso di aumento del richiamo dei dati, ad esempio se uno script o una soluzione di backup necessita di accedere a molti file offline.
- Le richieste di lettura per i file offline nelle copie Snapshot possono essere gestite.

Poiché le copie Snapshot sono di sola lettura, il server FPolicy non può ripristinare il file originale se il file stub si trova in una copia Snapshot. L'utilizzo di pass-through-Read elimina questo problema.

- È possibile impostare policy che controllano quando le richieste di lettura vengono gestite attraverso l'accesso al file sullo storage secondario e quando il file offline deve essere richiamato sullo storage primario.

Ad esempio, è possibile creare un criterio sul server HSM che specifica il numero di volte in cui è possibile accedere al file offline in un determinato periodo di tempo prima che il file venga nuovamente migrato nello storage primario. Questo tipo di policy evita di richiamare i file a cui si accede raramente.

### **Come vengono gestite le richieste di lettura quando FPolicy pass-through-Read è attivato**

È necessario comprendere come vengono gestite le richieste di lettura quando FPolicy pass-through-Read è attivato, in modo da poter configurare in modo ottimale la connettività tra la macchina virtuale di storage (SVM) e i server FPolicy.

Quando FPolicy pass-through-Read è attivato e la SVM riceve una richiesta di un file offline, FPolicy invia una notifica al server FPolicy (server HSM) attraverso il canale di connessione standard.

Dopo aver ricevuto la notifica, il server FPolicy legge i dati dal percorso del file inviato nella notifica e invia i dati richiesti alla SVM attraverso la connessione dati privilegiata pass-through-Read stabilita tra la SVM e il server FPolicy.

Una volta inviati i dati, il server FPolicy risponde alla richiesta di lettura come ALLOW (CONSENTI) o DENY (RIFIUTA). A seconda che la richiesta di lettura sia consentita o rifiutata, ONTAP invia le informazioni richieste o invia un messaggio di errore al client.

## **Pianificare la configurazione di FPolicy**

### **Requisiti, considerazioni e Best practice per la configurazione di FPolicy**

Prima di creare e configurare le configurazioni FPolicy sulle SVM, è necessario conoscere alcuni requisiti, considerazioni e Best practice per la configurazione di FPolicy.

Le funzionalità di FPolicy sono configurate tramite l'interfaccia a riga di comando (CLI) o tramite API REST.

#### **Requisiti per la configurazione di FPolicy**

Prima di configurare e abilitare FPolicy sulla macchina virtuale di storage (SVM), è necessario conoscere alcuni requisiti.

- Tutti i nodi del cluster devono eseguire una versione di ONTAP che supporti FPolicy.
- Se non si utilizza il motore FPolicy nativo di ONTAP, è necessario che siano installati server FPolicy esterni.
- I server FPolicy devono essere installati su un server accessibile dalle LIF dei dati di SVM in cui sono

attivati i criteri FPolicy.



A partire da ONTAP 9.8, ONTAP fornisce un servizio LIF client per le connessioni FPolicy in uscita con l'aggiunta di `data-fpolicy-client` servizio. ["Scopri di più sui LIF e sulle policy di servizio"](#).

- L'indirizzo IP del server FPolicy deve essere configurato come server primario o secondario nella configurazione del motore esterno del criterio FPolicy.
- Se i server FPolicy accedono ai dati su un canale dati privilegiato, devono essere soddisfatti i seguenti requisiti aggiuntivi:
  - SMB deve essere concesso in licenza sul cluster.

L'accesso privilegiato ai dati viene eseguito utilizzando connessioni SMB.

- È necessario configurare una credenziale utente per accedere ai file sul canale dati privilegiato.
- Il server FPolicy deve essere eseguito con le credenziali configurate nella configurazione FPolicy.
- Tutti i dati LIF utilizzati per comunicare con i server FPolicy devono essere configurati in modo da avere `cifs` come uno dei protocolli consentiti.

Sono inclusi i LIF utilizzati per le connessioni pass-through-Read.

- A partire da ONTAP 9.14.1, FPolicy consente di configurare un archivio persistente per acquisire eventi di accesso ai file per policy asincrone non obbligatorie nella SVM. Gli archivi persistenti possono aiutare a separare l'elaborazione i/o dei client dall'elaborazione delle notifiche FPolicy per ridurre la latenza dei client. Le configurazioni obbligatorie sincrone (obbligatorie o non obbligatorie) e asincrone non sono supportate.

### Best practice e consigli per la configurazione di FPolicy

Durante la configurazione di FPolicy su macchine virtuali di storage (SVM), acquisire familiarità con le Best practice e i consigli generali per la configurazione di FPolicy per garantire performance di monitoraggio e risultati affidabili che soddisfino i requisiti.

Per le linee guida specifiche relative a performance, dimensionamento e configurazione, utilizzare l'applicazione partner FPolicy.

### Configurazione dei criteri

La configurazione del motore esterno FPolicy, gli eventi e l'ambito per le SVM possono migliorare la tua esperienza e la sicurezza generale.

- Configurazione del motore esterno FPolicy per SVM:
  - Fornire una maggiore sicurezza implica un costo in termini di performance. L'abilitazione della comunicazione SSL (Secure Sockets Layer) ha un effetto sulle performance di accesso alle condivisioni.
  - Il motore esterno FPolicy deve essere configurato con più di un server FPolicy per garantire resilienza e alta disponibilità dell'elaborazione delle notifiche del server FPolicy.
- Configurazione degli eventi FPolicy per SVM:

Il monitoraggio delle operazioni dei file influenza l'esperienza complessiva. Ad esempio, il filtraggio delle operazioni di file indesiderate sul lato dello storage migliora l'esperienza. NetApp consiglia di configurare la

seguente configurazione:

- Monitoraggio dei tipi minimi di operazioni di file e abilitazione del numero massimo di filtri senza interrompere il caso d'utilizzo.
- Utilizzo di filtri per operazioni di getattr, lettura, scrittura, apertura e chiusura. Gli ambienti di home directory SMB e NFS hanno un'elevata percentuale di queste operazioni.
- Configurazione dell'ambito FPolicy per le SVM:

Limitare l'ambito delle policy agli oggetti di storage rilevanti, come condivisioni, volumi ed esportazioni, invece di abilitarli nell'intera SVM. NetApp consiglia di controllare le estensioni di directory. Se il `is-file-extension-check-on-directories-enabled` il parametro è impostato su `true`, gli oggetti di directory sono sottoposti agli stessi controlli di estensione dei file normali.

## Configurazione di rete

La connettività di rete tra il server FPolicy e il controller deve essere di bassa latenza. NetApp consiglia di separare il traffico FPolicy dal traffico client utilizzando una rete privata.

Inoltre, è necessario posizionare server FPolicy esterni (server FPolicy) nelle immediate vicinanze del cluster con connettività a elevata larghezza di banda per fornire una latenza minima e una connettività a elevata larghezza di banda.



Per uno scenario in cui il traffico LIF per FPolicy viene configurato su una porta diversa da LIF per il traffico client, FPolicy LIF potrebbe eseguire il failover sull'altro nodo a causa di un errore della porta. Di conseguenza, il server FPolicy diventa irraggiungibile dal nodo, il che causa un errore nelle notifiche FPolicy per le operazioni sui file sul nodo. Per evitare questo problema, verificare che il server FPolicy possa essere raggiunto attraverso almeno un LIF sul nodo per elaborare le richieste FPolicy per le operazioni file eseguite su quel nodo.

## Configurazione dell'hardware

Il server FPolicy può essere installato su un server fisico o virtuale. Se il server FPolicy si trova in un ambiente virtuale, è necessario allocare risorse dedicate (CPU, rete e memoria) al server virtuale.

Il rapporto nodo-server FPolicy del cluster deve essere ottimizzato per garantire che i server FPolicy non siano sovraccarichi, il che può introdurre latenze quando la SVM risponde alle richieste del client. Il rapporto ottimale dipende dall'applicazione del partner per cui viene utilizzato il server FPolicy. NetApp consiglia di collaborare con i partner per determinare il valore appropriato.

## Configurazione a più policy

La policy FPolicy per il blocco nativo ha la priorità più alta, indipendentemente dal numero di sequenza, e le policy di modifica delle decisioni hanno una priorità più alta rispetto ad altre. La priorità della policy dipende dal caso d'utilizzo. NetApp consiglia di collaborare con i partner per determinare la priorità appropriata.

## Considerazioni sulle dimensioni

FPolicy esegue il monitoraggio in linea delle operazioni SMB e NFS, invia notifiche al server esterno e attende una risposta, a seconda della modalità di comunicazione esterna del motore (sincrona o asincrona). Questo processo influisce sulle prestazioni dell'accesso SMB e NFS e sulle risorse della CPU.

Per mitigare eventuali problemi, NetApp consiglia di collaborare con i partner per valutare e dimensionare l'ambiente prima di abilitare FPolicy. Le performance sono influenzate da diversi fattori, tra cui il numero di

utenti, le caratteristiche dei carichi di lavoro, come le operazioni per utente e le dimensioni dei dati, la latenza di rete e la lentezza dei guasti o dei server.

**Monitorare le performance**

FPolicy è un sistema basato su notifiche. Le notifiche vengono inviate a un server esterno per l'elaborazione e la generazione di una risposta a ONTAP. Questo processo di andata e ritorno aumenta la latenza per l'accesso al client.

Il monitoraggio dei contatori delle performance sul server FPolicy e in ONTAP consente di identificare i colli di bottiglia nella soluzione e di ottimizzare i parametri in base alle necessità per una soluzione ottimale. Ad esempio, un aumento della latenza di FPolicy ha un effetto a cascata sulla latenza di accesso SMB e NFS. Pertanto, è necessario monitorare sia il carico di lavoro (SMB e NFS) che la latenza di FPolicy. Inoltre, è possibile utilizzare le policy di qualità del servizio in ONTAP per impostare un carico di lavoro per ogni volume o SVM abilitato per FPolicy.

NetApp consiglia di eseguire `statistics show -object workload` per visualizzare le statistiche del carico di lavoro. Inoltre, è necessario monitorare i seguenti parametri:

- Latenze medie, di lettura e di scrittura
- Numero totale di operazioni
- Contatori di lettura e scrittura

È possibile monitorare le performance dei sottosistemi FPolicy utilizzando i seguenti contatori FPolicy.



Per raccogliere le statistiche relative a FPolicy, è necessario essere in modalità diagnostica.

**Fasi**

1. Raccogliere i contatori FPolicy:

- a. `statistics start -object fpolicy -instance instance_name -sample-id ID`
- b. `statistics start -object fpolicy_policy -instance instance_name -sample-id ID`

2. Visualizza contatori FPolicy:

- a. `statistics show -object fpolicy -instance instance_name -sample-id ID`
- b. `statistics show -object fpolicy_server -instance instance_name -sample-id ID`

Il `fpolicy` e `fpolicy_server` i contatori forniscono informazioni su diversi parametri delle prestazioni descritti nella tabella seguente.

Contatori	Descrizione
• contatori "fpolicy"*	richieste_interrotte
Numero di richieste sullo schermo per le quali l'elaborazione viene interrotta sulla SVM	conteggio_eventi
Elenco degli eventi risultanti dalla notifica	latenza_richiesta_massima

Contatori	Descrizione
Latenza massima richiesta dallo schermo	richieste_in_sospeso
Numero totale di richieste di schermate in corso	processed_requests
Numero totale di richieste eseguite tramite l'elaborazione di fpolicy nella SVM	request_latency_hist
Istogramma della latenza per le richieste dello schermo	requests_dispatched_rate
Numero di richieste di videata inviate al secondo	requests_received_rate
Numero di richieste di videata ricevute al secondo	<ul style="list-style-type: none"> <li>contatori "fpolicy_server"</li> </ul>
latenza_richiesta_massima	Latenza massima per una richiesta dello schermo
richieste_in_sospeso	Numero totale di richieste sullo schermo in attesa di risposta
request_latency	Latenza media per la richiesta dello schermo
request_latency_hist	Istogramma della latenza per le richieste dello schermo
request_sent_rate	Numero di screen request inviate al server FPolicy al secondo
response_received_rate	Numero di risposte sullo schermo ricevute dal server FPolicy al secondo

## Gestire il workflow FPolicy e la dipendenza da altre tecnologie

NetApp consiglia di disattivare un criterio FPolicy prima di apportare modifiche alla configurazione. Ad esempio, se si desidera aggiungere o modificare un indirizzo IP nel motore esterno configurato per il criterio Enabled (attivato), disattivare prima il criterio.

Se si configura FPolicy per il monitoraggio dei volumi NetApp FlexCache, NetApp consiglia di non configurare FPolicy per monitorare le operazioni di lettura e getattr dei file. Il monitoraggio di queste operazioni in ONTAP richiede il recupero dei dati inode-to-path (I2P). Poiché i dati I2P non possono essere recuperati dai volumi FlexCache, devono essere recuperati dal volume di origine. Pertanto, il monitoraggio di queste operazioni elimina i benefici in termini di performance che FlexCache può offrire.

Quando vengono implementate sia FPolicy che una soluzione antivirus off-box, la soluzione antivirus riceve prima le notifiche. L'elaborazione di FPolicy viene avviata solo al termine della scansione antivirus. È importante dimensionare correttamente le soluzioni antivirus perché un programma antivirus lento può influire sulle prestazioni generali.

## Considerazioni su upgrade e revert in lettura passthrough

Prima di eseguire l'aggiornamento a una release di ONTAP che supporta la lettura pass-through o prima di tornare a una release che non supporta la lettura pass-through, è necessario conoscere alcune considerazioni

relative all'aggiornamento e al ripristino.

## **Aggiornamento in corso**

Dopo l'aggiornamento di tutti i nodi a una versione di ONTAP che supporta FPolicy pass-through-Read, il cluster è in grado di utilizzare la funzionalità pass-through-Read; tuttavia, il pass-through-Read viene disattivato per impostazione predefinita nelle configurazioni FPolicy esistenti. Per utilizzare pass-through-Read sulle configurazioni FPolicy esistenti, è necessario disattivare il criterio FPolicy e modificare la configurazione, quindi riattivarla.

## **In corso**

Prima di ripristinare una versione di ONTAP che non supporta FPolicy pass-through-Read, è necessario soddisfare le seguenti condizioni:

- Disattivare tutti i criteri utilizzando pass-through-Read, quindi modificare le configurazioni interessate in modo che non utilizzino pass-through-Read.
- Disattivare la funzionalità FPolicy sul cluster disattivando tutti i criteri FPolicy sul cluster.

Prima di tornare a una versione di ONTAP che non supporta gli archivi persistenti, assicurarsi che nessuno dei criteri FPolicy disponga di un archivio persistente configurato. Se è configurato un archivio persistente, l'indirizzamento non riesce.

## **Quali sono i passaggi per configurare una configurazione FPolicy**

Prima che FPolicy possa monitorare l'accesso ai file, è necessario creare e abilitare una configurazione FPolicy sulla macchina virtuale di storage (SVM) per la quale sono richiesti i servizi FPolicy.

Di seguito sono riportati i passaggi per impostare e abilitare una configurazione FPolicy su SVM:

### **1. Creare un motore esterno FPolicy.**

Il motore esterno FPolicy identifica i server FPolicy esterni (server FPolicy) associati a una specifica configurazione FPolicy. Se il motore FPolicy interno "nativo" viene utilizzato per creare una configurazione di blocco dei file nativa, non è necessario creare un motore esterno FPolicy.

### **2. Creare un evento FPolicy.**

Un evento FPolicy descrive ciò che la policy FPolicy deve monitorare. Gli eventi sono costituiti dai protocolli e dalle operazioni dei file da monitorare e possono contenere un elenco di filtri. Gli eventi utilizzano filtri per limitare l'elenco degli eventi monitorati per i quali il motore esterno FPolicy deve inviare notifiche. Gli eventi specificano anche se il criterio monitora le operazioni del volume.

### **3. Creare una policy FPolicy.**

Il criterio FPolicy è responsabile dell'associazione, con l'ambito appropriato, dell'insieme di eventi da monitorare e per i quali le notifiche degli eventi monitorati devono essere inviate al server FPolicy designato (o al motore nativo se non sono configurati server FPolicy). Il criterio definisce inoltre se al server FPolicy è consentito l'accesso privilegiato ai dati per i quali riceve le notifiche. Un server FPolicy ha bisogno di un accesso privilegiato se il server ha bisogno di accedere ai dati. I casi di utilizzo tipici in cui è necessario un accesso privilegiato includono il blocco dei file, la gestione delle quote e la gestione dello storage gerarchico. Il criterio consente di specificare se la configurazione di questo criterio utilizza un server FPolicy o il server FPolicy interno "nativo".

Un criterio specifica se lo screening è obbligatorio. Se lo screening è obbligatorio e tutti i server FPolicy non sono attivi o non viene ricevuta alcuna risposta dai server FPolicy entro un periodo di timeout definito, l'accesso al file viene negato.

I limiti di una policy sono la SVM. Un criterio non può essere applicato a più di una SVM. Tuttavia, una SVM specifica può avere più policy FPolicy, ciascuna con la stessa o diversa combinazione di ambito, evento e configurazioni di server esterni.

#### 4. Configurare l'ambito del criterio.

L'ambito di FPolicy determina i volumi, le condivisioni o le policy di esportazione su cui la policy agisce o esclude dal monitoraggio. Un ambito determina anche quali estensioni di file devono essere incluse o escluse dal monitoraggio di FPolicy.



Gli elenchi di esclusione hanno la precedenza sugli elenchi di inclusione.

#### 5. Attivare il criterio FPolicy.

Quando il criterio è attivato, i canali di controllo e, facoltativamente, i canali dati privilegiati sono connessi. Il processo FPolicy sui nodi a cui partecipa SVM inizia a monitorare l'accesso a file e cartelle e, per gli eventi che corrispondono ai criteri configurati, invia notifiche ai server FPolicy (o al motore nativo se non sono configurati server FPolicy).



Se il criterio utilizza il blocco dei file nativi, un motore esterno non viene configurato o associato al criterio.

### Pianificare la configurazione del motore esterno FPolicy

#### Pianificare la configurazione del motore esterno FPolicy

Prima di configurare il motore esterno FPolicy (motore esterno), è necessario comprendere il significato della creazione di un motore esterno e quali parametri di configurazione sono disponibili. Queste informazioni consentono di determinare i valori da impostare per ciascun parametro.

#### Informazioni definite durante la creazione del motore esterno FPolicy

La configurazione del motore esterno definisce le informazioni necessarie a FPolicy per effettuare e gestire le connessioni ai server FPolicy esterni (server FPolicy), incluse le seguenti informazioni:

- Nome SVM
- Nome del motore
- Gli indirizzi IP dei server FPolicy primario e secondario e il numero di porta TCP da utilizzare per la connessione ai server FPolicy
- Se il tipo di motore è asincrono o sincrono
- Come autenticare la connessione tra il nodo e il server FPolicy

Se si sceglie di configurare l'autenticazione SSL reciproca, è necessario configurare anche i parametri che forniscono le informazioni del certificato SSL.




- Come gestire la connessione utilizzando diverse impostazioni avanzate dei privilegi

Sono inclusi parametri che definiscono valori di timeout, valori di tentativi, valori di mantenimento, valori di richiesta massimi, valori di dimensione buffer inviati e ricevuti e valori di timeout della sessione.

Il `vserver fpolicy policy external-engine create` Il comando viene utilizzato per creare un motore esterno FPolicy.

**Quali sono i parametri esterni di base del motore**

È possibile utilizzare la seguente tabella dei parametri di configurazione di base di FPolicy per pianificare la configurazione:

Tipo di informazione	Opzione
<p><i>SVM</i></p> <p>Specifica il nome SVM che si desidera associare a questo motore esterno.</p> <p>Ogni configurazione FPolicy viene definita all'interno di una singola SVM. Il motore esterno, l'evento del criterio, l'ambito del criterio e il criterio che si combinano insieme per creare una configurazione del criterio FPolicy devono essere tutti associati alla stessa SVM.</p>	<p><code>-vserver vserver_name</code></p>
<p><i>Nome motore</i></p> <p>Specifica il nome da assegnare alla configurazione esterna del motore. È necessario specificare il nome del motore esterno in un secondo momento quando si crea il criterio FPolicy. In questo modo, il motore esterno viene associato alla policy.</p> <p>Il nome può contenere fino a 256 caratteri.</p> <div><p>Se si configura il nome del motore esterno in una configurazione di disaster recovery MetroCluster o SVM, il nome deve essere composto da un massimo di 200 caratteri.</p></div> <p>Il nome può contenere qualsiasi combinazione dei seguenti caratteri ASCII:</p> <ul style="list-style-type: none"><li>• a attraverso z</li><li>• A attraverso Z</li><li>• 0 attraverso 9</li><li>• “_”, “-”, and “`”</li></ul>	<p><code>-engine-name engine_name</code></p>

<p><i>Server FPolicy primari</i></p> <p>Specifica i server FPolicy primari a cui il nodo invia le notifiche per un dato criterio FPolicy. Il valore viene specificato come elenco di indirizzi IP delimitato da virgole.</p> <p>Se viene specificato più di un indirizzo IP del server primario, ogni nodo a cui partecipa SVM crea una connessione di controllo a ogni server FPolicy primario specificato al momento dell'attivazione del criterio. Se si configurano più server FPolicy primari, le notifiche vengono inviate ai server FPolicy in modo round-robin.</p> <p>Se il motore esterno viene utilizzato in una configurazione di disaster recovery MetroCluster o SVM, è necessario specificare gli indirizzi IP dei server FPolicy nel sito di origine come server primari. Gli indirizzi IP dei server FPolicy nel sito di destinazione devono essere specificati come server secondari.</p>	<p>-primary-servers IP_address,...</p>
<p><i>Numero porta</i></p> <p>Specifica il numero di porta del servizio FPolicy.</p>	<p>-port integer</p>
<p><i>Server FPolicy secondari</i></p> <p>Specifica i server FPolicy secondari a cui inviare gli eventi di accesso ai file per un determinato criterio FPolicy. Il valore viene specificato come elenco di indirizzi IP delimitato da virgole.</p> <p>I server secondari vengono utilizzati solo quando nessuno dei server primari è raggiungibile. Le connessioni ai server secondari vengono stabilite quando il criterio è attivato, ma le notifiche vengono inviate ai server secondari solo se nessuno dei server primari è raggiungibile. Se si configurano più server secondari, le notifiche vengono inviate ai server FPolicy in modo round-robin.</p>	<p>-secondary-servers IP_address,...</p>
<p><i>Tipo di motore esterno</i></p> <p>Specifica se il motore esterno funziona in modalità sincrona o asincrona. Per impostazione predefinita, FPolicy opera in modalità sincrona.</p> <p>Quando è impostato su <i>synchronous</i>, L'elaborazione della richiesta di file invia una notifica al server FPolicy, ma non continua fino a quando non riceve una risposta dal server FPolicy. A questo punto, il flusso della richiesta continua o l'elaborazione comporta un rifiuto, a seconda che la risposta dal server FPolicy consenta l'azione richiesta.</p> <p>Quando è impostato su <i>asynchronous</i>, L'elaborazione della richiesta di file invia una notifica al server FPolicy, quindi continua.</p>	<p>-extern-engine-type external_engine_type Il valore di questo parametro può essere uno dei seguenti:</p> <ul style="list-style-type: none"> <li>• synchronous</li> <li>• asynchronous</li> </ul>

<p><b>Opzione SSL per la comunicazione con il server FPolicy</b></p> <p>Specifica l'opzione SSL per la comunicazione con il server FPolicy. Questo è un parametro obbligatorio. È possibile scegliere una delle opzioni in base alle seguenti informazioni:</p> <ul style="list-style-type: none"> <li>• Quando è impostato su <code>no-auth</code>, non viene eseguita alcuna autenticazione.</li> </ul> <p>Il collegamento di comunicazione viene stabilito tramite TCP.</p> <ul style="list-style-type: none"> <li>• Quando è impostato su <code>server-auth</code>, SVM autentica il server FPolicy utilizzando l'autenticazione del server SSL.</li> <li>• Quando è impostato su <code>mutual-auth</code>, L'autenticazione reciproca avviene tra SVM e il server FPolicy; SVM autentica il server FPolicy e il server FPolicy autentica SVM.</li> </ul> <p>Se si sceglie di configurare l'autenticazione SSL reciproca, è necessario configurare anche <code>-certificate-common-name</code>, <code>-certificate-serial</code>, e. <code>-certificate-ca</code> parametri.</p>	<p><code>-ssl-option {no-auth</code></p>
<p><code>server-auth</code></p>	<p><code>mutual-auth}</code></p>
<p><b>FQDN certificato o nome comune personalizzato</b></p> <p>Specifica il nome del certificato utilizzato se è configurata l'autenticazione SSL tra SVM e il server FPolicy. È possibile specificare il nome del certificato come FQDN o come nome comune personalizzato.</p> <p>Se si specifica <code>mutual-auth</code> per <code>-ssl-option</code> specificare un valore per <code>-certificate-common-name</code> parametro.</p>	<p><code>-certificate-common-name text</code></p>
<p><b>Numero di serie del certificato</b></p> <p>Specifica il numero di serie del certificato utilizzato per l'autenticazione se è configurata l'autenticazione SSL tra SVM e il server FPolicy.</p> <p>Se si specifica <code>mutual-auth</code> per <code>-ssl-option</code> specificare un valore per <code>-certificate-serial</code> parametro.</p>	<p><code>-certificate-serial text</code></p>
<p><b>Autorità di certificazione</b></p> <p>Specifica il nome della CA del certificato utilizzato per l'autenticazione se è configurata l'autenticazione SSL tra SVM e il server FPolicy.</p> <p>Se si specifica <code>mutual-auth</code> per <code>-ssl-option</code> specificare un valore per <code>-certificate-ca</code> parametro.</p>	<p><code>-certificate-ca text</code></p>

## Quali sono le opzioni avanzate dei motori esterni

È possibile utilizzare la seguente tabella di parametri di configurazione FPolicy avanzati quando si prevede di

personalizzare la configurazione con parametri avanzati. Questi parametri vengono utilizzati per modificare il comportamento delle comunicazioni tra i nodi del cluster e i server FPolicy:

Tipo di informazione	Opzione
<p><i>Timeout per l'annullamento di una richiesta</i></p> <p>Specifica l'intervallo di tempo in ore (h), minuti (m), o secondi (s) Che il nodo attende una risposta dal server FPolicy.</p> <p>Se l'intervallo di timeout viene superato, il nodo invia una richiesta di annullamento al server FPolicy. Il nodo invia quindi la notifica a un server FPolicy alternativo. Questo timeout consente di gestire un server FPolicy che non risponde, migliorando la risposta del client SMB/NFS. Inoltre, l'annullamento delle richieste dopo un periodo di timeout può aiutare a rilasciare le risorse di sistema perché la richiesta di notifica viene spostata da un server FPolicy inattivo/non funzionante a un server FPolicy alternativo.</p> <p>L'intervallo per questo valore è 0 attraverso 100. Se il valore è impostato su 0, L'opzione è disattivata e i messaggi di richiesta di annullamento non vengono inviati al server FPolicy. L'impostazione predefinita è 20s.</p>	<p>-reqs-cancel-timeout integer[h]</p>
m	s]
<p><i>Timeout per l'interruzione di una richiesta</i></p> <p>Specifica il timeout in ore (h), minuti (m), o secondi (s) per interrompere una richiesta.</p> <p>L'intervallo per questo valore è 0 attraverso 200.</p>	<p>-reqs-abort-timeout ` integer[h]</p>
m	s]
<p><i>Intervallo per l'invio delle richieste di stato</i></p> <p>Specifica l'intervallo in ore (h), minuti (m), o secondi (s) Dopo di che viene inviata una richiesta di stato al server FPolicy.</p> <p>L'intervallo per questo valore è 0 attraverso 50. Se il valore è impostato su 0, L'opzione è disattivata e i messaggi di richiesta di stato non vengono inviati al server FPolicy. L'impostazione predefinita è 10s.</p>	<p>-status-req-interval integer[h]</p>
m	s]
<p><i>Numero massimo di richieste in sospeso sul server FPolicy</i></p> <p>Specifica il numero massimo di richieste in sospeso che è possibile mettere in coda sul server FPolicy.</p> <p>L'intervallo per questo valore è 1 attraverso 10000. L'impostazione predefinita è 500.</p>	<p>-max-server-reqs integer</p>

<p><i>Timeout per la disconnessione di un server FPolicy che non risponde</i></p> <p>Specifica l'intervallo di tempo in ore (h), minuti (m), o secondi (s) Dopo di che la connessione al server FPolicy viene interrotta.</p> <p>La connessione viene interrotta dopo il periodo di timeout solo se la coda del server FPolicy contiene il numero massimo consentito di richieste e non viene ricevuta alcuna risposta entro il periodo di timeout. Il numero massimo consentito di richieste è 50 (impostazione predefinita) o il numero specificato da <code>max-server-reqs</code> parametro.</p> <p>L'intervallo per questo valore è 1 attraverso 100. L'impostazione predefinita è 60s.</p>	<p>-server-progress -timeout integer[h</p>
m	s]
<p><i>Intervallo per l'invio di messaggi keep-alive al server FPolicy</i></p> <p>Specifica l'intervallo di tempo in ore (h), minuti (m), o secondi (s) In cui i messaggi keep-alive vengono inviati al server FPolicy.</p> <p>I messaggi keep-alive rilevano connessioni half-open.</p> <p>L'intervallo per questo valore è 10 attraverso 600. Se il valore è impostato su 0, L'opzione è disattivata e non è possibile inviare messaggi keep-alive ai server FPolicy. L'impostazione predefinita è 120s.</p>	<p>-keep-alive-interval-integer[h</p>
m	s]
<p><i>Numero massimo di tentativi di riconnessione</i></p> <p>Specifica il numero massimo di tentativi di riconnessione da parte di SVM al server FPolicy dopo l'interruzione della connessione.</p> <p>L'intervallo per questo valore è 0 attraverso 20. L'impostazione predefinita è 5.</p>	<p>-max-connection-retries integer</p>
<p><i>Dimensione buffer di ricezione</i></p> <p>Specifica la dimensione del buffer di ricezione del socket connesso per il server FPolicy.</p> <p>Il valore predefinito è 256 kilobyte (Kb). Quando il valore è impostato su 0, la dimensione del buffer di ricezione viene impostata su un valore definito dal sistema.</p> <p>Ad esempio, se la dimensione predefinita del buffer di ricezione del socket è 65536 byte, impostando il valore sintonizzabile su 0, la dimensione del buffer del socket viene impostata su 65536 byte. È possibile utilizzare qualsiasi valore non predefinito per impostare la dimensione (in byte) del buffer di ricezione.</p>	<p>-recv-buffer-size integer</p>

<p><i>Invia dimensione buffer</i></p> <p>Specifica la dimensione del buffer di invio del socket connesso per il server FPolicy.</p> <p>Il valore predefinito è 256 kilobyte (Kb). Quando il valore è impostato su 0, la dimensione del buffer di invio viene impostata su un valore definito dal sistema.</p> <p>Ad esempio, se la dimensione predefinita del buffer di invio del socket è impostata su 65536 byte, impostando il valore sintonizzabile su 0, la dimensione del buffer del socket viene impostata su 65536 byte. È possibile utilizzare qualsiasi valore non predefinito per impostare la dimensione (in byte) del buffer di invio.</p>	<p><code>-send-buffer-size</code> integer</p>
<p><i>Timeout per l'eliminazione di un ID sessione durante la riconnessione</i></p> <p>Specifica l'intervallo in ore (h), minuti (m), o secondi (s) Dopo di che viene inviato un nuovo ID di sessione al server FPolicy durante i tentativi di riconnessione.</p> <p>Se la connessione tra il controller di storage e il server FPolicy viene interrotta e la riconnessione viene effettuata all'interno di <code>-session-timeout</code> Intervallo, il vecchio ID sessione viene inviato al server FPolicy in modo che possa inviare le risposte per le vecchie notifiche.</p> <p>Il valore predefinito è impostato su 10 secondi.</p>	<p><code>-session-timeout</code> [.integerh][integerm][integer s]</p>

#### Ulteriori informazioni sulla configurazione dei motori esterni FPolicy per l'utilizzo di connessioni autenticate SSL

Per configurare il motore esterno FPolicy in modo che utilizzi SSL durante la connessione ai server FPolicy, è necessario conoscere alcune informazioni aggiuntive.

#### Autenticazione del server SSL

Se si sceglie di configurare il motore esterno FPolicy per l'autenticazione del server SSL, prima di creare il motore esterno, è necessario installare il certificato pubblico dell'autorità di certificazione (CA) che ha firmato il certificato del server FPolicy.

#### Autenticazione reciproca

Se si configurano i motori esterni di FPolicy in modo che utilizzino l'autenticazione reciproca SSL quando si collegano i LIF dei dati delle macchine virtuali di storage (SVM) ai server FPolicy esterni, prima di creare il motore esterno, È necessario installare il certificato pubblico della CA che ha firmato il certificato del server FPolicy insieme al certificato pubblico e al file delle chiavi per l'autenticazione della SVM. Non è necessario eliminare questo certificato mentre i criteri FPolicy utilizzano il certificato installato.

Se il certificato viene eliminato mentre FPolicy lo utilizza per l'autenticazione reciproca durante la connessione a un server FPolicy esterno, non è possibile riabilitare un criterio FPolicy disattivato che utilizza tale certificato. Non è possibile riabilitare il criterio FPolicy in questa situazione anche se viene creato e installato un nuovo certificato con le stesse impostazioni sulla SVM.

Se il certificato è stato eliminato, è necessario installare un nuovo certificato, creare nuovi motori esterni

FPolicy che utilizzano il nuovo certificato e associare i nuovi motori esterni al criterio FPolicy che si desidera riabilitare modificando il criterio FPolicy.

## Installare i certificati per SSL

Il certificato pubblico della CA utilizzato per firmare il certificato del server FPolicy viene installato utilizzando `security certificate install` con il `-type` parametro impostato su `client-ca`. La chiave privata e il certificato pubblico richiesti per l'autenticazione della SVM vengono installati utilizzando `security certificate install` con il `-type` parametro impostato su `server`.

### I certificati non vengono replicati nelle relazioni di disaster recovery SVM con una configurazione non-ID-preserve

I certificati di sicurezza utilizzati per l'autenticazione SSL durante le connessioni ai server FPolicy non replicano nelle destinazioni di disaster recovery SVM con configurazioni non ID-preserve. Sebbene la configurazione del motore esterno FPolicy sulla SVM sia replicata, i certificati di sicurezza non vengono replicati. È necessario installare manualmente i certificati di protezione sulla destinazione.

Quando si imposta la relazione di disaster recovery SVM, il valore selezionato per `-identity-preserve` opzione di `snapmirror create` Determina i dettagli di configurazione replicati nella SVM di destinazione.

Se si imposta `-identity-preserve` opzione a `true` (ID-Preserve), vengono replicati tutti i dettagli di configurazione di FPolicy, incluse le informazioni del certificato di sicurezza. È necessario installare i certificati di protezione sulla destinazione solo se si imposta l'opzione su `false` (Non-ID-Preserve).

### Restrizioni per motori esterni FPolicy con ambito cluster con configurazioni di disaster recovery MetroCluster e SVM

È possibile creare un motore esterno FPolicy con ambito cluster assegnando la SVM (Cluster Storage Virtual Machine) al motore esterno. Tuttavia, quando si crea un motore esterno con ambito cluster in una configurazione di disaster recovery MetroCluster o SVM, esistono alcune restrizioni quando si sceglie il metodo di autenticazione utilizzato da SVM per la comunicazione esterna con il server FPolicy.

Quando si creano server FPolicy esterni, è possibile scegliere tre opzioni di autenticazione: Nessuna autenticazione, autenticazione del server SSL e autenticazione reciproca SSL. Sebbene non vi siano restrizioni quando si sceglie l'opzione di autenticazione se il server FPolicy esterno è assegnato a una SVM di dati, esistono restrizioni quando si crea un motore esterno FPolicy con ambito cluster:

Configurazione	Consentito?
Disaster recovery MetroCluster o SVM e motore esterno FPolicy con ambito cluster senza autenticazione (SSL non configurato)	Sì
Disaster recovery MetroCluster o SVM e motore esterno FPolicy con ambito cluster con server SSL o autenticazione reciproca SSL	No

- Se esiste un motore esterno FPolicy con ambito cluster con autenticazione SSL e si desidera creare una configurazione di disaster recovery MetroCluster o SVM, è necessario modificare questo motore esterno in modo che non utilizzi alcuna autenticazione o rimuovere il motore esterno prima di poter creare la configurazione di disaster recovery MetroCluster o SVM.

- Se la configurazione di disaster recovery MetroCluster o SVM esiste già, ONTAP impedisce di creare un motore esterno FPolicy con ambito cluster e autenticazione SSL.

#### Completare il foglio di lavoro di configurazione del motore esterno FPolicy

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione del motore esterno FPolicy. Se è richiesto un valore di parametro, è necessario determinare quale valore utilizzare per tali parametri prima di configurare il motore esterno.

#### Informazioni per una configurazione di base del motore esterno

Registrare se si desidera includere ogni impostazione di parametro nella configurazione esterna del motore e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	Sì	
Nome del motore	Sì	Sì	
Server FPolicy primari	Sì	Sì	
Numero di porta	Sì	Sì	
Server FPolicy secondari	No		
Tipo di motore esterno	No		
Opzione SSL per la comunicazione con il server FPolicy esterno	Sì	Sì	
FQDN certificato o nome comune personalizzato	No		
Numero di serie del certificato	No		
Autorità di certificazione	No		

#### Informazioni sui parametri esterni avanzati del motore

Per configurare un motore esterno con parametri avanzati, è necessario immettere il comando di configurazione in modalità avanzata con privilegi.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Timeout per l'annullamento di una richiesta	No		



Timeout per l'interruzione di una richiesta	No		
Intervallo per l'invio delle richieste di stato	No		
Numero massimo di richieste in sospeso sul server FPolicy	No		
Timeout per la disconnessione di un server FPolicy che non risponde	No		
Intervallo per l'invio di messaggi keep-alive al server FPolicy	No		
Numero massimo di tentativi di riconnessione	No		
Dimensione buffer di ricezione	No		
Dimensione buffer di invio	No		
Timeout per l'eliminazione di un ID sessione durante la riconnessione	No		

## Pianificare la configurazione dell'evento FPolicy

### Pianificare la panoramica della configurazione degli eventi FPolicy

Prima di configurare gli eventi FPolicy, è necessario comprendere il significato di creazione di un evento FPolicy. È necessario determinare quali protocolli si desidera monitorare l'evento, quali eventi monitorare e quali filtri eventi utilizzare. Queste informazioni consentono di pianificare i valori che si desidera impostare.

### Cosa significa creare un evento FPolicy

La creazione dell'evento FPolicy implica la definizione delle informazioni necessarie al processo FPolicy per determinare quali operazioni di accesso ai file monitorare e per quali notifiche degli eventi monitorati devono essere inviate al server FPolicy esterno. La configurazione degli eventi FPolicy definisce le seguenti informazioni di configurazione:

- Nome SVM (Storage Virtual Machine)
- Nome dell'evento
- Quali protocolli monitorare

FPolicy può monitorare le operazioni di accesso ai file SMB, NFSv3 e NFSv4.

- Quali operazioni di file monitorare

Non tutte le operazioni sui file sono valide per ciascun protocollo.

- Quali filtri di file configurare

Sono valide solo alcune combinazioni di operazioni e filtri dei file. Ogni protocollo dispone di un proprio set di combinazioni supportate.

- Se monitorare le operazioni di montaggio e smontaggio del volume


Esiste una dipendenza con tre parametri (-protocol, -file-operations, -filters). Le seguenti combinazioni sono valide per i tre parametri:




- È possibile specificare -protocol e. -file-operations parametri.
- È possibile specificare tutti e tre i parametri.
- Non è possibile specificare alcun parametro.

### Contenuto della configurazione dell'evento FPolicy

È possibile utilizzare il seguente elenco di parametri di configurazione degli eventi FPolicy disponibili per pianificare la configurazione:

Tipo di informazione	Opzione
<p><b>SVM</b></p> <p>Specifica il nome SVM che si desidera associare a questo evento FPolicy.</p> <p>Ogni configurazione FPolicy viene definita all'interno di una singola SVM. Il motore esterno, l'evento del criterio, l'ambito del criterio e il criterio che si combinano insieme per creare una configurazione del criterio FPolicy devono essere tutti associati alla stessa SVM.</p>	<p>-vserver vserver_name</p>
<p><b>Nome evento</b></p> <p>Specifica il nome da assegnare all'evento FPolicy. Quando si crea il criterio FPolicy, l'evento FPolicy viene associato al criterio utilizzando il nome dell'evento.</p> <p>Il nome può contenere fino a 256 caratteri.</p> <div>  <p>Se si configura l'evento in una configurazione di disaster recovery MetroCluster o SVM, il nome deve contenere fino a 200 caratteri.</p> </div> <p>Il nome può contenere qualsiasi combinazione dei seguenti caratteri ASCII:</p> <ul style="list-style-type: none"> <li>• a attraverso z</li> <li>• A attraverso Z</li> <li>• 0 attraverso 9</li> <li>• " _ ", "-", and ""</li> </ul>	<p>-event-name event_name</p>

<p><i>Protocollo</i></p> <p>Specifica quale protocollo configurare per l'evento FPolicy. L'elenco per <code>-protocol</code> può includere uno dei seguenti valori:</p> <ul style="list-style-type: none"> <li>• <code>cifs</code></li> <li>• <code>nfsv3</code></li> <li>• <code>nfsv4</code></li> </ul> <div data-bbox="167 510 220 562">  </div> <div data-bbox="282 468 1026 604"> <p>Se si specifica <code>-protocol</code>, quindi specificare un valore valido in <code>-file-operations</code> parametro. Man mano che la versione del protocollo cambia, i valori validi potrebbero cambiare.</p> </div>	<p><code>-protocol protocol</code></p>
--	--

## Operazioni file

Specifica l'elenco delle operazioni del file per l'evento FPolicy.

L'evento controlla le operazioni specificate in questo elenco da tutte le richieste client utilizzando il protocollo specificato in `-protocol` parametro. È possibile elencare una o più operazioni sui file utilizzando un elenco delimitato da virgole. L'elenco per `-file-operations` può includere uno o più dei seguenti valori:

- `close` per le operazioni di chiusura del file
- `create` per le operazioni di creazione dei file
- `create-dir` per le operazioni di creazione directory
- `delete` per le operazioni di eliminazione dei file
- `delete_dir` per le operazioni di eliminazione della directory
- `getattr` per le operazioni get attribute
- `link` per le operazioni di collegamento
- `lookup` per le operazioni di ricerca
- `open` per le operazioni di apertura dei file
- `read` per le operazioni di lettura del file
- `write` per le operazioni di scrittura del file
- `rename` per le operazioni di ridenominazione dei file
- `rename_dir` per le operazioni di ridenominazione della directory
- `setattr` per le operazioni di set attribute
- `symlink` per operazioni di collegamento simbolico



Se si specifica `-file-operations`, quindi specificare un protocollo valido in `-protocol` parametro.

`-file-operations`  
`file_operations,...`

Specifica l'elenco dei filtri per una determinata operazione di file per il protocollo specificato. I valori in `-filters` i parametri vengono utilizzati per filtrare le richieste dei client. L'elenco può includere uno o più dei seguenti elementi:



Se si specifica `-filters` quindi specificare valori validi per `-file-operations` e. `-protocol` parametri.

- `monitor-ads` opzione per filtrare la richiesta del client per un flusso di dati alternativo.
- `close-with-modification` opzione per filtrare la richiesta del client per la chiusura con modifica.
- `close-without-modification` opzione per filtrare la richiesta del client per la chiusura senza modifiche.
- `first-read` opzione per filtrare la richiesta del client per la prima lettura.
- `first-write` opzione per filtrare la richiesta del client per la prima scrittura.
- `offline-bit` opzione per filtrare la richiesta del client per il set di bit offline.

Impostando questo filtro, il server FPolicy riceve una notifica solo quando si accede ai file offline.

- `open-with-delete-intent` opzione per filtrare la richiesta del client per l'apertura con intento di eliminazione.

Se si imposta questo filtro, il server FPolicy riceve una notifica solo quando si tenta di aprire un file con l'intento di eliminarlo. Questo viene utilizzato dai file system quando `FILE_DELETE_ON_CLOSE` flag specificato.

- `open-with-write-intent` opzione per filtrare la richiesta del client per l'apertura con intento di scrittura.

L'impostazione di questo filtro comporta la ricezione di una notifica da parte del server FPolicy solo quando si tenta di aprire un file con l'intento di scriverne qualcosa.

- `write-with-size-change` opzione per filtrare la richiesta del client per la scrittura con la modifica delle dimensioni.

<p><i>Filtri (continua)</i></p> <ul style="list-style-type: none"> <li>• <code>setattr-with-owner-change</code> opzione per filtrare le richieste setattr del client per la modifica del proprietario di un file o di una directory.</li> <li>• <code>setattr-with-group-change</code> opzione per filtrare le richieste setattr del client per la modifica del gruppo di un file o di una directory.</li> <li>• <code>setattr-with-sacl-change</code> Opzione per filtrare le richieste setattr del client per la modifica del SACL in un file o in una directory.</li> </ul> <p>Questo filtro è disponibile solo per i protocolli SMB e NFSv4.</p> <ul style="list-style-type: none"> <li>• <code>setattr-with-dacl-change</code> Opzione per filtrare le richieste setattr del client per la modifica del DACL in un file o in una directory.</li> </ul> <p>Questo filtro è disponibile solo per i protocolli SMB e NFSv4.</p> <ul style="list-style-type: none"> <li>• <code>setattr-with-modify-time-change</code> opzione per filtrare le richieste setattr del client per modificare l'ora di modifica di un file o di una directory.</li> <li>• <code>setattr-with-access-time-change</code> opzione per filtrare le richieste setattr del client per modificare l'ora di accesso di un file o di una directory.</li> <li>• <code>setattr-with-creation-time-change</code> opzione per filtrare le richieste setattr del client per modificare l'ora di creazione di un file o di una directory.</li> </ul> <p>Questa opzione è disponibile solo per il protocollo SMB.</p> <ul style="list-style-type: none"> <li>• <code>setattr-with-mode-change</code> opzione per filtrare le richieste setattr del client per modificare i bit di modalità su un file o una directory.</li> <li>• <code>setattr-with-size-change</code> opzione per filtrare le richieste setattr del client per modificare le dimensioni di un file.</li> <li>• <code>setattr-with-allocation-size-change</code> opzione per filtrare le richieste setattr del client per modificare la dimensione di allocazione di un file.</li> </ul> <p>Questa opzione è disponibile solo per il protocollo SMB.</p> <ul style="list-style-type: none"> <li>• <code>exclude-directory</code> opzione per filtrare le richieste del client per le operazioni di directory.</li> </ul> <p>Quando viene specificato questo filtro, le operazioni della directory non vengono monitorate.</p>	<p><code>-filters filter, ...</code></p>
<p><i>È richiesta l'operazione del volume</i></p> <p>Specifica se il monitoraggio è necessario per le operazioni di montaggio e disinstallazione del volume. L'impostazione predefinita è <code>false</code>.</p>	<p><code>-volume-operation {true</code></p>

<pre>false}  -filters filter,...</pre>	<p><i>Notifica accesso FPolicy negata</i></p> <p>A partire da ONTAP 9.13.1, gli utenti possono ricevere notifiche per operazioni di file non riuscite a causa della mancanza di autorizzazioni. Queste notifiche sono preziose per la sicurezza, la protezione ransomware e la governance. Le notifiche verranno generate per l'operazione del file non riuscita a causa della mancanza di autorizzazione, che include:</p> <ul style="list-style-type: none"> <li>• Errori dovuti alle autorizzazioni NTFS.</li> <li>• Errori dovuti a bit di modalità Unix.</li> <li>• Guasti dovuti a ACL NFSv4.</li> </ul>
<pre>-monitor-fileop-failure {true</pre>	<pre>false}</pre>

#### Operazioni di file supportate e combinazioni di filtri che FPolicy può monitorare per SMB

Quando si configura l'evento FPolicy, è necessario tenere presente che solo alcune combinazioni di operazioni e filtri dei file sono supportate per il monitoraggio delle operazioni di accesso ai file SMB.

L'elenco delle operazioni di file supportate e delle combinazioni di filtri per il monitoraggio FPolicy degli eventi di accesso ai file SMB è riportato nella seguente tabella:

Operazioni di file supportate	Filtri supportati
chiudere	monitor-ads, offline-bit, close-with-modification, close-without-modification, close-with-read, escludi-directory
creare	monitor-ads, offline-bit
crea_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
eliminare	monitor-ads, offline-bit
dir_delete	Attualmente non è supportato alcun filtro per questa operazione di file.

getattr	offline-bit, exclude-dir
aprire	monitor-ads, offline-bit, open-with-delete-intent, open-with-write-intent, exclude-dir
leggi	monitor-ads, offline-bit, first-read
di scrittura	monitor-ads, offline-bit, first-write, write-with-size-change
rinominare	monitor-ads, offline-bit
rinomina_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
setattr	monitor-ads, offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_creation_time_change, setattr_with_size_change, setattr_with_allocation_size_change, exclude_directory

A partire da ONTAP 9.13.1, gli utenti possono ricevere notifiche per operazioni di file non riuscite a causa della mancanza di autorizzazioni. L'elenco delle combinazioni di filtri e operazioni di accesso negato supportate per il monitoraggio FPolicy degli eventi di accesso ai file SMB è riportato nella seguente tabella:

Operazione di accesso supportato con accesso negato	Filtri supportati
aprire	NA

#### Operazioni di file supportate e combinazioni di filtri che FPolicy può monitorare per NFSv3

Quando si configura l'evento FPolicy, è necessario tenere presente che solo alcune combinazioni di operazioni e filtri dei file sono supportate per il monitoraggio delle operazioni di accesso ai file NFSv3.

L'elenco delle operazioni di file supportate e delle combinazioni di filtri per il monitoraggio FPolicy degli eventi di accesso ai file NFSv3 è riportato nella seguente tabella:

Operazioni di file supportate	Filtri supportati
creare	offline-bit
crea_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
eliminare	offline-bit
dir_delete	Attualmente non è supportato alcun filtro per questa operazione di file.



collegamento	offline-bit
ricerca	offline-bit, exclude-dir
leggi	offline-bit, first-read
di scrittura	offline-bit, first-write, write-with-size-change
rinominare	offline-bit
rinomina_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
link simbolico	offline-bit

A partire da ONTAP 9.13.1, gli utenti possono ricevere notifiche per operazioni di file non riuscite a causa della mancanza di autorizzazioni. L'elenco delle combinazioni di filtri e operazioni di accesso negato supportate per il monitoraggio FPolicy degli eventi di accesso al file NFSv3 è riportato nella seguente tabella:

Operazione di accesso supportato con accesso negato	Filtri supportati
accesso	NA
creare	NA
crea_dir	NA
eliminare	NA
dir_delete	NA
collegamento	NA
leggi	NA
rinominare	NA
rinomina_dir	NA
setattr	NA

di scrittura	NA
--------------	----

#### Operazioni di file supportate e combinazioni di filtri che FPolicy può monitorare per NFSv4

Quando si configura l'evento FPolicy, è necessario tenere presente che solo alcune combinazioni di operazioni e filtri dei file sono supportate per il monitoraggio delle operazioni di accesso ai file NFSv4.

L'elenco delle operazioni di file supportate e delle combinazioni di filtri per il monitoraggio FPolicy degli eventi di accesso ai file NFSv4 è riportato nella seguente tabella:

Operazioni di file supportate	Filtri supportati
chiudere	offline-bit, exclude-directory
creare	offline-bit
crea_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
eliminare	offline-bit
dir_delete	Attualmente non è supportato alcun filtro per questa operazione di file.
getattr	offline-bit, exclude-directory
collegamento	offline-bit
ricerca	offline-bit, exclude-directory
aprire	offline-bit, exclude-directory
leggi	offline-bit, first-read
di scrittura	offline-bit, first-write, write-with-size-change
rinominare	offline-bit
rinomina_dir	Attualmente non è supportato alcun filtro per questa operazione di file.
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_sacl_change, setattr_with_dacl_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory
link simbolico	offline-bit

A partire da ONTAP 9.13.1, gli utenti possono ricevere notifiche per operazioni di file non riuscite a causa della mancanza di autorizzazioni. L'elenco delle combinazioni di filtri e operazioni di accesso negato supportate per il monitoraggio FPolicy degli eventi di accesso al file NFSv4 è riportato nella seguente tabella:

Operazione di accesso supportato con accesso negato	Filtri supportati
accesso	NA
creare	NA
crea_dir	NA
eliminare	NA
dir_delete	NA
collegamento	NA
aprire	NA
leggi	NA
rinominare	NA
rinomina_dir	NA
setattr	NA
di scrittura	NA

#### Completare il foglio di lavoro di configurazione degli eventi FPolicy

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione degli eventi FPolicy. Se è richiesto un valore di parametro, è necessario determinare quale valore utilizzare per tali parametri prima di configurare l'evento FPolicy.

Registrare se si desidera includere ogni impostazione di parametro nella configurazione dell'evento FPolicy e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	Sì	
Nome dell'evento	Sì	Sì	

Protocollo	No		
Operazioni sui file	No		
Filtri	No		
Funzionamento del volume	No		
Accesso agli eventi negati + (supporto a partire da ONTAP 9.13)	No		

## Pianificare la configurazione del criterio FPolicy

### Pianificare la panoramica della configurazione dei criteri FPolicy

Prima di configurare il criterio FPolicy, è necessario comprendere quali parametri sono necessari per la creazione del criterio e perché si desidera configurare determinati parametri opzionali. Queste informazioni consentono di determinare i valori da impostare per ciascun parametro.

Quando si crea un criterio FPolicy, si associa il criterio a quanto segue:

- La macchina virtuale per lo storage (SVM)
- Uno o più eventi FPolicy
- Un motore esterno FPolicy

È inoltre possibile configurare diverse impostazioni opzionali dei criteri.

### Contenuto della configurazione del criterio FPolicy

Per pianificare la configurazione, è possibile utilizzare il seguente elenco di criteri FPolicy obbligatori e parametri opzionali:

Tipo di informazione	Opzione	Obbligatorio	Predefinito
<b>Nome SVM</b>  Specifica il nome della SVM su cui si desidera creare un criterio FPolicy.	-vserver vserver_name	Sì	Nessuno

<p><i>Nome policy</i></p> <p>Specifica il nome del criterio FPolicy.</p> <p>Il nome può contenere fino a 256 caratteri.</p> <div data-bbox="167 386 220 441"> </div> <p>Se si configura il criterio in una configurazione di disaster recovery MetroCluster o SVM, il nome deve contenere fino a 200 caratteri.</p> <p>Il nome può contenere qualsiasi combinazione dei seguenti caratteri ASCII:</p> <ul style="list-style-type: none"> <li>• a attraverso z</li> <li>• A attraverso Z</li> <li>• 0 attraverso 9</li> <li>• “_”, “-”, and “`”</li> </ul>	<p>-policy-name policy_name</p>	<p>Sì</p>	<p>Nessuno</p>
<p><i>Nomi eventi</i></p> <p>Specifica un elenco delimitato da virgole di eventi da associare al criterio FPolicy.</p> <ul style="list-style-type: none"> <li>• È possibile associare più di un evento a un criterio.</li> <li>• Un evento è specifico di un protocollo.</li> <li>• È possibile utilizzare un singolo criterio per monitorare gli eventi di accesso ai file per più protocolli creando un evento per ciascun protocollo che si desidera monitorare dal criterio e associando quindi gli eventi al criterio.</li> <li>• Gli eventi devono già esistere.</li> </ul>	<p>-events event_name, ...</p>	<p>Sì</p>	<p>Nessuno</p>

<p><b>Nome motore esterno</b></p> <p>Specifica il nome del motore esterno da associare al criterio FPolicy.</p> <ul style="list-style-type: none"> <li>• Un motore esterno contiene le informazioni richieste dal nodo per inviare le notifiche a un server FPolicy.</li> <li>• È possibile configurare FPolicy per utilizzare il motore esterno nativo di ONTAP per un semplice blocco dei file o per utilizzare un motore esterno configurato per utilizzare server FPolicy esterni (server FPolicy) per un blocco dei file e una gestione dei file più sofisticati.</li> <li>• Se si desidera utilizzare il motore esterno nativo, non è possibile specificare un valore per questo parametro o è possibile specificare <code>native</code> come valore.</li> <li>• Se si desidera utilizzare i server FPolicy, la configurazione per il motore esterno deve già esistere.</li> </ul>	<p><code>-engine</code> <code>engine_name</code></p>	<p>Sì (a meno che il criterio non utilizzi il motore nativo ONTAP interno)</p>	<p><code>native</code></p>
<p><b>È richiesto lo screening obbligatorio</b></p> <p>Specifica se è richiesto lo screening obbligatorio dell'accesso ai file.</p> <ul style="list-style-type: none"> <li>• L'impostazione di screening obbligatorio determina l'azione intrapresa in caso di evento di accesso al file in caso di inattività di tutti i server primari e secondari o di mancata ricezione di una risposta dai server FPolicy entro un determinato periodo di timeout.</li> <li>• Quando è impostato su <code>true</code>, gli eventi di accesso al file sono negati.</li> <li>• Quando è impostato su <code>false</code>, sono consentiti eventi di accesso al file.</li> </ul>	<p><code>-is-mandatory</code> <code>{true</code></p>	<p><code>false}</code></p>	<p>No</p>

true	<p><b>Consenti accesso privilegiato</b></p> <p>Specifica se si desidera che il server FPolicy disponga di un accesso privilegiato ai file e alle cartelle monitorati utilizzando una connessione dati con privilegi.</p> <p>Se configurati, i server FPolicy possono accedere ai file dalla directory principale della SVM contenente i dati monitorati utilizzando la connessione dati con privilegi.</p> <p>Per un accesso privilegiato ai dati, SMB deve essere concesso in licenza sul cluster e tutti i dati LIF utilizzati per connettersi ai server FPolicy devono essere configurati in modo da avere <code>cifs</code> come uno dei protocolli consentiti.</p> <p>Se si desidera configurare il criterio per consentire l'accesso con privilegi, è necessario specificare anche il nome utente dell'account che il server FPolicy deve utilizzare per l'accesso con privilegi.</p>	<p>-allow -privileged -access {yes</p>	no}
------	---	--	-----

<p>No (a meno che non sia attivata la funzione pass-through-Read)</p>	<p>no</p>	<p><i>Nome utente privilegiato</i></p> <p>Specifica il nome utente dell'account utilizzato dai server FPolicy per l'accesso ai dati con privilegi.</p> <ul style="list-style-type: none"> <li>• Il valore di questo parametro deve utilizzare il formato "<code>`domain` user name</code>".</li> <li>• Se <code>-allow</code> <code>-privileged</code> <code>-access</code> è impostato su <code>no</code>, qualsiasi valore impostato per questo parametro viene ignorato.</li> </ul>	<p><code>-privileged</code> <code>-user-name</code> <code>user_name</code></p>
---	-----------	--	--



<p>No (a meno che non sia abilitato l'accesso privilegiato)</p>	<p>Nessuno</p>	<p><i>Allow pass-through-Read</i></p> <p>Specifica se i server FPolicy possono fornire servizi di lettura pass-through per i file che sono stati archiviati nello storage secondario (file offline) dai server FPolicy:</p> <ul style="list-style-type: none"> <li>• La lettura pass-through è un modo per leggere i dati per i file offline senza ripristinarli nello storage primario.</li> </ul> <p>La funzione Passthrough-Read riduce le latenze delle risposte, poiché non è necessario richiamare i file sullo storage primario prima di rispondere alla richiesta di lettura. Inoltre, la funzione pass-through-Read ottimizza l'efficienza dello storage eliminando la necessità di consumare spazio di storage primario con file richiamati esclusivamente per soddisfare le richieste di lettura.</p> <ul style="list-style-type: none"> <li>• Se attivati, i server FPolicy forniscono i dati per il file su un canale dati privilegiato</li> </ul>	<pre>-is-passthrough -read-enabled {true</pre>
---	----------------	---	--

Requisito per le configurazioni dell'ambito FPolicy se il criterio FPolicy utilizza il motore nativo

Se si configura il criterio FPolicy per utilizzare il motore nativo, esiste un requisito specifico per la definizione dell'ambito FPolicy configurato per il criterio.

L'ambito FPolicy definisce i limiti ai quali si applica il criterio FPolicy, ad esempio se FPolicy si applica a volumi o condivisioni specificati. Esistono diversi parametri che limitano ulteriormente l'ambito a cui si applica la policy FPolicy. Uno di questi parametri, `-is-file-extension-check-on-directories-enabled`, specifica se controllare le estensioni dei file nelle directory. Il valore predefinito è `false`, il che significa che le estensioni dei file nelle directory non sono selezionate.

Quando un criterio FPolicy che utilizza il motore nativo è attivato su una condivisione o volume e su `-is-file-extension-check-on-directories-enabled` il parametro è impostato su `false` per l'ambito del criterio, l'accesso alla directory viene negato. Con questa configurazione, poiché le estensioni dei file non vengono controllate per le directory, qualsiasi operazione di directory viene negata se rientra nell'ambito del criterio.

Per garantire che l'accesso alla directory abbia esito positivo quando si utilizza il motore nativo, è necessario impostare `-is-file-extension-check-on-directories-enabled` parameter a `true` quando si crea l'ambito.

Con questo parametro impostato su `true`, I controlli delle estensioni vengono eseguiti per le operazioni di directory e la decisione di consentire o negare l'accesso viene presa in base alle estensioni incluse o escluse nella configurazione dell'ambito FPolicy.

Completare il foglio di lavoro della policy FPolicy

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione dei criteri FPolicy. Registrare se si desidera includere ciascuna impostazione di parametro nella configurazione del criterio FPolicy e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	
Nome policy	Sì	
Nomi degli eventi	Sì	
Nome del motore esterno		
È richiesto lo screening obbligatorio?		
Consentire l'accesso con privilegi		
Nome utente con privilegi		
Il pass-through-Read è abilitato?		

## Pianificare la configurazione dell'ambito FPolicy

### Pianificare la panoramica della configurazione dell'ambito FPolicy

Prima di configurare l'ambito di FPolicy, è necessario comprendere il significato di creazione di un ambito. È necessario comprendere cosa contiene la configurazione dell'ambito. È inoltre necessario comprendere quali sono le regole di priorità dell'ambito. Queste informazioni consentono di pianificare i valori che si desidera impostare.

### Cosa significa creare un ambito FPolicy

La creazione dell'ambito FPolicy significa definire i limiti ai quali si applica il criterio FPolicy. La macchina virtuale per lo storage (SVM) è il limite di base. Quando si crea un ambito per un criterio FPolicy, è necessario definire il criterio FPolicy a cui si applicherà ed è necessario indicare a quale SVM si desidera applicare l'ambito.

Esistono diversi parametri che limitano ulteriormente l'ambito all'interno della SVM specificata. È possibile limitare l'ambito specificando cosa includere nell'ambito o cosa escludere dall'ambito. Dopo aver applicato un ambito a un criterio abilitato, i controlli degli eventi del criterio vengono applicati all'ambito definito da questo comando.

Le notifiche vengono generate per gli eventi di accesso ai file in cui le corrispondenze si trovano nelle opzioni "include". Le notifiche non vengono generate per gli eventi di accesso al file in cui sono presenti corrispondenze nelle opzioni "exclude".

La configurazione dell'ambito FPolicy definisce le seguenti informazioni di configurazione:

- Nome SVM
- Nome policy
- Le condivisioni da includere o escludere da ciò che viene monitorato
- Le policy di esportazione da includere o escludere da ciò che viene monitorato
- I volumi da includere o escludere da ciò che viene monitorato
- Le estensioni di file da includere o escludere da ciò che viene monitorato
- Se eseguire il controllo dell'estensione del file sugli oggetti di directory



Esistono considerazioni particolari per l'ambito di applicazione di una policy FPolicy del cluster. Il criterio FPolicy del cluster è un criterio creato dall'amministratore del cluster per la SVM amministrativa. Se l'amministratore del cluster crea anche l'ambito per il criterio FPolicy del cluster, l'amministratore SVM non può creare un ambito per lo stesso criterio. Tuttavia, se l'amministratore del cluster non crea un ambito per il criterio FPolicy del cluster, qualsiasi amministratore SVM può creare l'ambito per tale criterio del cluster. Se l'amministratore di SVM crea un ambito per tale criterio FPolicy del cluster, l'amministratore del cluster non potrà successivamente creare un ambito del cluster per lo stesso criterio del cluster. Questo perché l'amministratore del cluster non può eseguire l'override dell'ambito per lo stesso criterio del cluster.

### Quali sono le regole di priorità dell'ambito di applicazione

Le seguenti regole di precedenza si applicano alle configurazioni dell'ambito:

- Quando una condivisione è inclusa in `-shares-to-include` il parametro e il volume padre della condivisione sono inclusi in `-volumes-to-exclude` parametro, `-volumes-to-exclude` ha la precedenza `-shares-to-include`.
  - Quando un criterio di esportazione viene incluso in `-export-policies-to-include` il parametro e il volume principale del criterio di esportazione sono inclusi in `-volumes-to-exclude` parametro, `-volumes-to-exclude` ha la precedenza `-export-policies-to-include`.
  - Un amministratore può specificare entrambi `-file-extensions-to-include` e `-file-extensions-to-exclude` elenchi.
- Il `-file-extensions-to-exclude` il parametro viene controllato prima di `-file-extensions-to-include` parametro selezionato.

## Contenuto della configurazione FPolicy Scope

È possibile utilizzare il seguente elenco di parametri di configurazione FPolicy Scope disponibili per pianificare la configurazione:



Quando si configurano le condivisioni, le policy di esportazione, i volumi e le estensioni dei file da includere o escludere dall'ambito, i parametri include ed exclude possono includere metacaratteri come "?" and "\*". L'utilizzo delle espressioni regolari non è supportato.

Tipo di informazione	Opzione
<p><b>SVM</b></p> <p>Specifica il nome SVM su cui si desidera creare un ambito FPolicy.</p> <p>Ogni configurazione FPolicy viene definita all'interno di una singola SVM. Il motore esterno, l'evento del criterio, l'ambito del criterio e il criterio che si combinano insieme per creare una configurazione del criterio FPolicy devono essere tutti associati alla stessa SVM.</p>	<p><code>-vserver vserver_name</code></p>
<p><b>Nome policy</b></p> <p>Specifica il nome del criterio FPolicy a cui si desidera associare l'ambito. Il criterio FPolicy deve già esistere.</p>	<p><code>-policy-name policy_name</code></p>
<p><b>Condivisioni da includere</b></p> <p>Specifica un elenco delimitato da virgole di condivisioni da monitorare per il criterio FPolicy a cui viene applicato l'ambito.</p>	<p><code>-shares-to-include share_name, ...</code></p>
<p><b>Condivisioni da escludere</b></p> <p>Specifica un elenco delimitato da virgole di condivisioni da escludere dal monitoraggio per il criterio FPolicy a cui viene applicato l'ambito.</p>	<p><code>-shares-to-exclude share_name, ...</code></p>
<p><b>Volumi da includere</b> specifica un elenco di volumi delimitati da virgole da monitorare per il criterio FPolicy a cui viene applicato l'ambito.</p>	<p><code>-volumes-to-include volume_name, ...</code></p>

<p><i>Volumi da escludere</i></p> <p>Specifica un elenco delimitato da virgole di volumi da escludere dal monitoraggio per il criterio FPolicy a cui viene applicato l'ambito.</p>	<pre>-volumes-to-exclude volume_name, ...</pre>
<p><i>Esporta policy da includere</i></p> <p>Specifica un elenco delimitato da virgole di criteri di esportazione da monitorare per il criterio FPolicy a cui viene applicato l'ambito.</p>	<pre>-export-policies-to -include export_policy_name, ...</pre>
<p><i>Esporta policy da escludere</i></p> <p>Specifica un elenco delimitato da virgole di criteri di esportazione da escludere dal monitoraggio per il criterio FPolicy a cui viene applicato l'ambito.</p>	<pre>-export-policies-to -exclude export_policy_name, ...</pre>
<p><i>Estensioni file da includere</i></p> <p>Specifica un elenco delimitato da virgole di estensioni di file da monitorare per il criterio FPolicy a cui viene applicato l'ambito.</p>	<pre>-file-extensions-to -include file_extensions, ...</pre>
<p><i>Estensione del file da escludere</i></p> <p>Specifica un elenco delimitato da virgole di estensioni di file da escludere dal monitoraggio del criterio FPolicy a cui viene applicato l'ambito.</p>	<pre>-file-extensions-to -exclude file_extensions, ...</pre>
<p><i>Il controllo dell'estensione del file sulla directory è abilitato ?</i></p> <p>Specifica se i controlli dell'estensione del nome file si applicano anche agli oggetti di directory. Se questo parametro è impostato su <code>true</code>, gli oggetti di directory sono sottoposti agli stessi controlli di estensione dei file normali. Se questo parametro è impostato su <code>false</code>, i nomi delle directory non corrispondono per gli interni e le notifiche vengono inviate per le directory anche se le relative estensioni non corrispondono.</p> <p>Se il criterio FPolicy a cui è assegnato l'ambito è configurato per utilizzare il motore nativo, questo parametro deve essere impostato su <code>true</code>.</p>	<pre>-is-file-extension -check-on-directories -enabled {true</pre>
<p><code>false</code></p>	<pre>}</pre>

#### Completare il foglio di lavoro FPolicy Scope

È possibile utilizzare questo foglio di lavoro per registrare i valori necessari durante il processo di configurazione dell'ambito FPolicy. Se è richiesto un valore di parametro, è necessario determinare quale valore utilizzare per tali parametri prima di configurare l'ambito FPolicy.

Registrare se si desidera includere ciascuna impostazione di parametro nella configurazione dell'ambito FPolicy e quindi registrare il valore dei parametri che si desidera includere.

Tipo di informazione	Obbligatorio	Includi	I tuoi valori
Nome SVM (Storage Virtual Machine)	Sì	Sì	
Nome policy	Sì	Sì	
Condivisioni da includere	No		
Condivisioni da escludere	No		
Volumi da includere	No		
Volumi da escludere	No		
Policy di esportazione da includere	No		
Esportare i criteri da escludere	No		
Estensioni di file da includere	No		
Estensione del file da escludere	No		
Il controllo dell'estensione del file nella directory è attivato?	No		

## Creare la configurazione FPolicy

### Creare il motore esterno FPolicy

È necessario creare un motore esterno per iniziare a creare una configurazione FPolicy. Il motore esterno definisce il modo in cui FPolicy crea e gestisce le connessioni ai server FPolicy esterni. Se la configurazione utilizza il motore ONTAP interno (il motore esterno nativo) per un semplice blocco dei file, non è necessario configurare un motore esterno FPolicy separato e non è necessario eseguire questa operazione.

#### Di cosa hai bisogno

Il ["motore esterno"](#) il foglio di lavoro deve essere completato.

#### A proposito di questa attività

Se il motore esterno viene utilizzato in una configurazione MetroCluster, è necessario specificare gli indirizzi IP dei server FPolicy nel sito di origine come server primari. Gli indirizzi IP dei server FPolicy nel sito di destinazione devono essere specificati come server secondari.

#### Fasi

1. Creare il motore esterno FPolicy utilizzando `vserver fpolicy policy external-engine create` comando.

Il seguente comando crea un motore esterno su una macchina virtuale di storage (SVM) vs1.example.com. Non è richiesta alcuna autenticazione per le comunicazioni esterne con il server FPolicy.

```
vserver fpolicy policy external-engine create -vserver-name vs1.example.com
-engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
no-auth
```

- 2. Verificare la configurazione del motore esterno FPolicy utilizzando vserver fpolicy policy external-engine show comando.

Il seguente comando visualizza le informazioni su tutti i motori esterni configurati su SVM vs1.example.com:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com
```

		Primary	Secondary		
External					
Vserver	Engine	Servers	Servers	Port	Engine
Type					
-----	-----	-----	-----	-----	
-----					
vs1.example.com	engine1	10.1.1.2,	-	6789	
synchronous		10.1.1.3			

Il seguente comando visualizza informazioni dettagliate sul motore esterno denominato “engine1” su SVM vs1.example.com:

```
vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
-name engine1
```

Vserver:	vs1.example.com
Engine:	engine1
Primary FPolicy Servers:	10.1.1.2, 10.1.1.3
Port Number of FPolicy Service:	6789
Secondary FPolicy Servers:	-
External Engine Type:	synchronous
SSL Option for External Communication:	no-auth
FQDN or Custom Common Name:	-
Serial Number of Certificate:	-
Certificate Authority:	-

**Creare l’evento FPolicy**

Durante la creazione di una configurazione dei criteri FPolicy, è necessario creare un evento FPolicy. L’evento viene associato alla policy FPolicy al momento della sua

creazione. Un evento definisce il protocollo da monitorare e gli eventi di accesso al file da monitorare e filtrare.

**Prima di iniziare**

Devi completare l'evento FPolicy "foglio di lavoro".

**Creare l'evento FPolicy**

- 1. Creare l'evento FPolicy utilizzando `vserver fpolicy policy event create` comando.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name event1 -protocol cifs -file-operations open,close,read,write
```

- 2. Verificare la configurazione dell'evento FPolicy utilizzando `vserver fpolicy policy event show` comando.

```
vserver fpolicy policy event show -vserver vs1.example.com
```

Vserver	Event Name	Protocols	File Operations	Filters	Is Volume Operation
vs1.example.com	event1	cifs	open, close, read, write	-	false

**Creare gli eventi di accesso negato FPolicy**

A partire da ONTAP 9.13.1, gli utenti possono ricevere notifiche per operazioni di file non riuscite a causa della mancanza di autorizzazioni. Queste notifiche sono preziose per la sicurezza, la protezione ransomware e la governance.

- 1. Creare l'evento FPolicy utilizzando `vserver fpolicy policy event create` comando.

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

**Creare archivi persistenti**

A partire da ONTAP 9.14.1, FPolicy consente di impostare un "Archivi persistenti" Per acquisire eventi di accesso ai file per policy asincrone non obbligatorie nella SVM. Gli archivi persistenti possono aiutare a separare l'elaborazione i/o dei client dall'elaborazione delle notifiche FPolicy per ridurre la latenza dei client. Le configurazioni obbligatorie sincrone (obbligatorie o non obbligatorie) e asincrone non sono supportate.

**Best practice**

- Prima di utilizzare la funzionalità di archivio permanente, assicurati che le tue applicazioni partner supportino questa configurazione.
- Il volume dello storage persistente viene configurato in base alle singole SVM. Per ogni SVM abilitata per



FPolicy avrai bisogno di un volume archivio persistente.

- Il nome del volume di archiviazione persistente e il percorso di giunzione specificati al momento della creazione del volume dovrebbero corrispondere.
- Crea il volume di archivio persistente sul nodo con LIF che prevedono il monitoraggio del traffico massimo da parte di Fpolicy.
- Impostare il criterio snapshot su `none` per quel volume invece di `default`. In questo modo si garantisce che non vi sia alcun ripristino accidentale dello snapshot che causa la perdita degli eventi correnti e per impedire un'eventuale elaborazione di eventi duplicati.
- Rendere il volume dell'archivio persistente inaccessibile per l'accesso al protocollo utente esterno (CIFS/NFS) per evitare il danneggiamento accidentale o l'eliminazione dei record di eventi persistenti. Per ottenere questo risultato, dopo aver attivato FPolicy, smontare il volume in ONTAP per rimuovere il percorso di giunzione; ciò lo rende inaccessibile per l'accesso al protocollo utente.

## Fasi

1. Creare un volume vuoto sulla SVM che può essere sottoposto a provisioning per l'archivio persistente:

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -junction  
-path <path> -policy <default> -unix-permissions <777> -size <value>  
-aggregate <aggregate name> -snapshot-policy <none>
```

- Le dimensioni del volume dell'archivio persistente si basano sul periodo di tempo per il quale si desidera mantenere gli eventi non inviati al server esterno (applicazione partner).

Ad esempio, se si desidera che 30 minuti di eventi persistano in un cluster con una capacità di 30K notifiche al secondo:

Dimensioni del volume richiesto = 30000 x 30 x 60 x 0,6KB (dimensioni medie del record di notifica) = 32400000 KB = ~32 GB

Per trovare la percentuale approssimativa di notifica, è possibile contattare l'applicazione partner FPolicy o utilizzare il contatore FPolicy `requests_dispatched_rate`.

- Si prevede che un utente amministratore con privilegi RBAC sufficienti (per creare un volume) creerà un volume (utilizzando il comando cli di volume o l'API REST) della dimensione desiderata e fornirà il nome di quel volume come `-volume`. Nell'archivio persistente creare un comando CLI o API REST.

2. Creare l'archivio persistente:

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store  
<PS_name> -volume <volume>
```

- Persistent-store: Il nome dell'archivio persistente
- Volume: Il volume della memoria persistente

3. Dopo aver creato l'archivio persistente, è possibile creare il criterio FPolicy e aggiungere il nome dell'archivio persistente a tale criterio.

Per ulteriori informazioni, vedere ["Creare il criterio FPolicy"](#).

## Creare il criterio FPolicy

Quando si crea il criterio FPolicy, si associa un motore esterno e uno o più eventi al criterio. Il criterio specifica inoltre se è richiesto lo screening obbligatorio, se i server

FPolicy dispongono di un accesso privilegiato ai dati sulla macchina virtuale di storage (SVM) e se è attivata la funzione pass-through-Read per i file offline.

### Di cosa hai bisogno

- Il foglio di lavoro della policy FPolicy deve essere completato.
- Se si prevede di configurare il criterio per l'utilizzo dei server FPolicy, il motore esterno deve esistere.
- Deve esistere almeno un evento FPolicy che si prevede di associare al criterio FPolicy.
- Se si desidera configurare l'accesso privilegiato ai dati, è necessario che un server SMB esista sulla SVM.
- Per configurare un archivio persistente per un criterio, il tipo di motore deve essere **asincrono** e il criterio deve essere **non obbligatorio**.

Per ulteriori informazioni, vedere ["Creare archivi persistenti"](#).

### Fasi

#### 1. Creare la policy FPolicy:

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name
policy_name -engine engine_name -events event_name, [-persistent-store
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
privileged-user-name domain\user_name] [-is-passthrough-read-enabled
{true|false}]
```

- È possibile aggiungere uno o più eventi alla policy FPolicy.
- Per impostazione predefinita, lo screening obbligatorio è attivato.
- Se si desidera consentire l'accesso con privilegi impostando `-allow-privileged-access` parametro a. `yes`, è inoltre necessario configurare un nome utente con privilegi per l'accesso con privilegi.
- Se si desidera configurare pass-through-Read impostando `-is-passthrough-read-enabled` parametro a. `true`, è inoltre necessario configurare l'accesso privilegiato ai dati.

Il comando seguente crea una policy denominata "policy1" con l'evento "event1" e il motore esterno denominato "engine1" associato. Questo criterio utilizza i valori predefiniti nella configurazione del criterio:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1
-events event1 -engine engine1
```

Il comando seguente crea una policy denominata "policy2" che ha l'evento "event2" e il motore esterno denominato "engine2" associato. Questo criterio è configurato per utilizzare l'accesso privilegiato utilizzando il nome utente specificato. La funzione di lettura pass-through è attivata:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
-events event2 -engine engine2 -allow-privileged-access yes -privileged-
user-name example\archive_acct -is-passthrough-read-enabled true
```

Il comando seguente crea una policy denominata "native1" a cui è associato l'evento "event3". Questo criterio utilizza il motore nativo e i valori predefiniti nella configurazione del criterio:

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. Verificare la configurazione del criterio FPolicy utilizzando `vserver fpolicy policy show` comando.

Il seguente comando visualizza le informazioni relative ai tre criteri FPolicy configurati, incluse le seguenti informazioni:

- SVM associato al criterio
  - Il motore esterno associato alla policy
  - Gli eventi associati al criterio
  - Se è richiesto lo screening obbligatorio
  - Se è richiesto l'accesso con privilegi
- ```
vserver fpolicy policy show
```

| Vserver         | Policy Name | Events | Engine  | Is Mandatory | Privileged Access |
|-----------------|-------------|--------|---------|--------------|-------------------|
| -----           | -----       | -----  | -----   | -----        |                   |
| vs1.example.com | policy1     | event1 | engine1 | true         | no                |
| vs1.example.com | policy2     | event2 | engine2 | true         | yes               |
| vs1.example.com | native1     | event3 | native  | true         | no                |

## Creare l'ambito FPolicy

Dopo aver creato il criterio FPolicy, è necessario creare un ambito FPolicy. Quando si crea l'ambito, si associa l'ambito a un criterio FPolicy. Un ambito definisce i limiti ai quali si applica la policy FPolicy. Gli ambiti possono includere o escludere file in base a condivisioni, policy di esportazione, volumi ed estensioni di file.

### Di cosa hai bisogno

Il foglio di lavoro FPolicy Scope deve essere completato. Il criterio FPolicy deve esistere con un motore esterno associato (se il criterio è configurato per l'utilizzo di server FPolicy esterni) e deve avere almeno un evento FPolicy associato.

### Fasi

1. Creare l'ambito FPolicy utilizzando `vserver fpolicy policy scope create` comando.

```
vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name policy1 -volumes-to-include datavol1,datavol2
```

2. Verificare la configurazione dell'ambito FPolicy utilizzando `vserver fpolicy policy scope show` comando.

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
Vserver: vs1.example.com
Policy: policy1
Shares to Include: -
Shares to Exclude: -
Volumes to Include: datavol1, datavol2
Volumes to Exclude: -
Export Policies to Include: -
Export Policies to Exclude: -
File Extensions to Include: -
File Extensions to Exclude: -
```

### Attivare il criterio FPolicy

Dopo aver configurato una configurazione dei criteri FPolicy, si attiva il criterio FPolicy. L'abilitazione del criterio determina la priorità e avvia il monitoraggio dell'accesso al file per il criterio.

#### Di cosa hai bisogno

Il criterio FPolicy deve esistere con un motore esterno associato (se il criterio è configurato per l'utilizzo di server FPolicy esterni) e deve avere almeno un evento FPolicy associato. L'ambito del criterio FPolicy deve esistere e deve essere assegnato al criterio FPolicy.

#### A proposito di questa attività

La priorità viene utilizzata quando sulla macchina virtuale di storage (SVM) sono attivati più criteri e più criteri sono stati sottoscritti allo stesso evento di accesso al file. I criteri che utilizzano la configurazione nativa del motore hanno una priorità maggiore rispetto ai criteri per qualsiasi altro motore, indipendentemente dal numero di sequenza assegnato al momento dell'attivazione del criterio.



Non è possibile attivare un criterio sulla SVM amministrativa.

#### Fasi

1. Attivare il criterio FPolicy utilizzando `vserver fpolicy enable` comando.

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
-sequence-number 1
```

2. Verificare che il criterio FPolicy sia attivato utilizzando `vserver fpolicy show` comando.

```
vserver fpolicy show -vserver vs1.example.com
```

| Vserver         | Policy Name | Sequence<br>Number | Status | Engine  |
|-----------------|-------------|--------------------|--------|---------|
| -----           | -----       | -----              | -----  | -----   |
| vs1.example.com | policy1     | 1                  | on     | engine1 |

## Gestire le configurazioni FPolicy

### Modificare le configurazioni FPolicy

#### Comandi per la modifica delle configurazioni FPolicy

È possibile modificare le configurazioni FPolicy modificando gli elementi che compongono la configurazione. È possibile modificare motori esterni, eventi FPolicy, ambiti FPolicy e policy FPolicy. È inoltre possibile attivare o disattivare i criteri FPolicy. Quando si disattiva il criterio FPolicy, il monitoraggio dei file viene interrotto per tale criterio.

Si consiglia di disattivare il criterio FPolicy prima di modificare la configurazione.

| Se si desidera modificare... | Utilizzare questo comando...                               |
|------------------------------|------------------------------------------------------------|
| Motori esterni               | <code>vserver fpolicy policy external-engine modify</code> |
| Eventi                       | <code>vserver fpolicy policy event modify</code>           |
| Ambiti                       | <code>vserver fpolicy policy scope modify</code>           |
| Policy                       | <code>vserver fpolicy policy modify</code>                 |

Per ulteriori informazioni, vedere le pagine man per i comandi.

#### Attivare o disattivare i criteri FPolicy

Una volta completata la configurazione, è possibile attivare i criteri FPolicy. L'abilitazione del criterio determina la priorità e avvia il monitoraggio dell'accesso al file per il criterio. È possibile disattivare i criteri FPolicy se si desidera interrompere il monitoraggio dell'accesso ai file per il criterio.

#### Di cosa hai bisogno

Prima di attivare i criteri FPolicy, è necessario completare la configurazione FPolicy.

#### A proposito di questa attività

- La priorità viene utilizzata quando sulla macchina virtuale di storage (SVM) sono attivati più criteri e più criteri sono stati sottoscritti allo stesso evento di accesso al file.
- I criteri che utilizzano la configurazione nativa del motore hanno una priorità maggiore rispetto ai criteri per qualsiasi altro motore, indipendentemente dal numero di sequenza assegnato al momento dell'attivazione del criterio.
- Se si desidera modificare la priorità di un criterio FPolicy, è necessario disattivarlo e riattivarlo utilizzando il nuovo numero di sequenza.

#### Fase

1. Eseguire l'azione appropriata:

| Se si desidera...             | Immettere il seguente comando...                                                                                 |
|-------------------------------|------------------------------------------------------------------------------------------------------------------|
| Attivare un criterio FPolicy  | <code>vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer</code> |
| Disattiva un criterio FPolicy | <code>vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name</code>                         |

## Visualizza informazioni sulle configurazioni FPolicy

### Funzionamento dei comandi di visualizzazione

Durante la visualizzazione delle informazioni sulla configurazione di FPolicy, è utile comprendere come `show` i comandi funzionano.

R `show` il comando senza parametri aggiuntivi visualizza le informazioni in un modulo riepilogativo. Inoltre, ogni `show` il comando ha gli stessi due parametri opzionali che si escludono a vicenda, `-instance` e `-fields`.

Quando si utilizza `-instance` parametro con `a. show` l'output del comando visualizza informazioni dettagliate in un formato di elenco. In alcuni casi, l'output dettagliato può essere lungo e includere più informazioni di quante ne hai bisogno. È possibile utilizzare `-fields fieldname[,fieldname...]` parametro per personalizzare l'output in modo che visualizzi le informazioni solo per i campi specificati. È possibile identificare i campi che è possibile specificare immettendo ? dopo il `-fields` parametro.



L'output di un `show` con il `-fields` il parametro potrebbe visualizzare altri campi pertinenti e necessari relativi ai campi richiesti.

Ogni `show` command dispone di uno o più parametri opzionali che filtrano l'output e consentono di limitare l'ambito delle informazioni visualizzate nell'output del comando. È possibile identificare i parametri opzionali disponibili per un comando immettendo ? dopo il `show` comando.

Il `show` Il comando supporta i modelli e i caratteri jolly in stile UNIX per consentire la corrispondenza di più valori negli argomenti dei parametri di comando. Ad esempio, è possibile utilizzare l'operatore jolly (\*), L'operatore NOT (!), L'operatore OR (|), l'operatore di intervallo (integer...integer), l'operatore meno di (<), l'operatore maggiore di (>), l'operatore minore o uguale a (≤) e maggiore o uguale all'operatore (≥) quando si specificano i valori.

Per ulteriori informazioni sull'utilizzo di modelli e caratteri jolly in stile UNIX, vedere [Utilizzando l'interfaccia della riga di comando di ONTAP](#).

### Comandi per la visualizzazione delle informazioni sulle configurazioni FPolicy

Si utilizza `fpolicy show` Comandi per visualizzare informazioni sulla configurazione di FPolicy, incluse informazioni su motori esterni, eventi, ambiti e policy di FPolicy.

|                                                        |                              |
|--------------------------------------------------------|------------------------------|
| Se si desidera visualizzare informazioni su FPolicy... | Utilizzare questo comando... |
|--------------------------------------------------------|------------------------------|

|                |                                                          |
|----------------|----------------------------------------------------------|
| Motori esterni | <code>vserver fpolicy policy external-engine show</code> |
| Eventi         | <code>vserver fpolicy policy event show</code>           |
| Ambiti         | <code>vserver fpolicy policy scope show</code>           |
| Policy         | <code>vserver fpolicy policy show</code>                 |

Per ulteriori informazioni, vedere le pagine man per i comandi.

#### Visualizza informazioni sullo stato dei criteri FPolicy

È possibile visualizzare informazioni sullo stato dei criteri FPolicy per determinare se un criterio è abilitato, quale motore esterno è configurato per l'utilizzo, quale numero di sequenza corrisponde al criterio e a quale SVM (Storage Virtual Machine) è associato il criterio FPolicy.

#### A proposito di questa attività

Se non si specificano parametri, il comando visualizza le seguenti informazioni:

- Nome SVM
- Nome policy
- Numero di sequenza del criterio
- Stato della policy

Oltre a visualizzare le informazioni sullo stato dei criteri per i criteri FPolicy configurati sul cluster o su una SVM specifica, è possibile utilizzare i parametri dei comandi per filtrare l'output del comando in base ad altri criteri.

È possibile specificare `-instance` parametro per visualizzare informazioni dettagliate sui criteri elencati. In alternativa, è possibile utilizzare `-fields` per visualizzare solo i campi indicati nell'output del comando, o. `-fields ?` per determinare quali campi è possibile utilizzare.

#### Fase

1. Visualizzare le informazioni filtrate sullo stato dei criteri FPolicy utilizzando il comando appropriato:

|                                                                             |                                                |
|-----------------------------------------------------------------------------|------------------------------------------------|
| Se si desidera visualizzare le informazioni di stato relative ai criteri... | Immettere il comando...                        |
| Sul cluster                                                                 | <code>vserver fpolicy show</code>              |
| Che hanno lo stato specificato                                              | <code>`vserver fpolicy show -status {on</code> |
| <code>off}`</code>                                                          | Su una SVM specificata                         |

|                                                                            |                                              |
|----------------------------------------------------------------------------|----------------------------------------------|
| <code>vserver fpolicy show</code><br><code>-vserver vserver_name</code>    | Con il nome del criterio specificato         |
| <code>vserver fpolicy show</code><br><code>-policy-name policy_name</code> | Che utilizzano il motore esterno specificato |

## Esempio

Nell'esempio seguente vengono visualizzate le informazioni relative ai criteri FPolicy nel cluster:

```
cluster1::> vserver fpolicy show
```

| Vserver         | Policy Name    | Sequence<br>Number | Status | Engine |
|-----------------|----------------|--------------------|--------|--------|
| -----           | -----          | -----              | -----  | -----  |
| FPolicy         | cserver_policy | -                  | off    | eng1   |
| vs1.example.com | v1p1           | -                  | off    | eng2   |
| vs1.example.com | v1p2           | -                  | off    | native |
| vs1.example.com | v1p3           | -                  | off    | native |
| vs1.example.com | cserver_policy | -                  | off    | eng1   |
| vs2.example.com | v1p1           | 3                  | on     | native |
| vs2.example.com | v1p2           | 1                  | on     | eng3   |
| vs2.example.com | cserver_policy | 2                  | on     | eng1   |

## Visualizza informazioni sui criteri FPolicy abilitati

È possibile visualizzare informazioni sui criteri FPolicy abilitati per determinare il motore esterno FPolicy configurato per l'utilizzo, la priorità del criterio e la macchina virtuale dello storage (SVM) a cui è associato il criterio FPolicy.

### A proposito di questa attività

Se non si specificano parametri, il comando visualizza le seguenti informazioni:

- Nome SVM
- Nome policy
- Priorità della policy

È possibile utilizzare i parametri dei comandi per filtrare l'output del comando in base a criteri specifici.

### Fase

1. Visualizzare le informazioni sui criteri FPolicy abilitati utilizzando il comando appropriato:

|                                                                   |                                           |
|-------------------------------------------------------------------|-------------------------------------------|
| Se si desidera visualizzare informazioni sui criteri abilitati... | Immettere il comando...                   |
| Sul cluster                                                       | <code>vserver fpolicy show-enabled</code> |



|                                       |                                                                    |
|---------------------------------------|--------------------------------------------------------------------|
| Su una SVM specificata                | <code>vserver fpolicy show-enabled -vserver vserver_name</code>    |
| Con il nome del criterio specificato  | <code>vserver fpolicy show-enabled -policy-name policy_name</code> |
| Con il numero di sequenza specificato | <code>vserver fpolicy show-enabled -priority integer</code>        |

## Esempio

Nell'esempio seguente vengono visualizzate le informazioni relative ai criteri FPolicy abilitati sul cluster:

```
cluster1::> vserver fpolicy show-enabled
Vserver                Policy Name                Priority
-----
vs1.example.com        pol_native                 native
vs1.example.com        pol_native2                native
vs1.example.com        pol1                       2
vs1.example.com        pol2                       4
```

## Gestire le connessioni del server FPolicy

### Connettersi a server FPolicy esterni

Per attivare l'elaborazione dei file, potrebbe essere necessario connettersi manualmente a un server FPolicy esterno se la connessione è stata interrotta in precedenza. Una connessione viene interrotta dopo il timeout del server o a causa di un errore. In alternativa, l'amministratore potrebbe interrompere manualmente una connessione.

### A proposito di questa attività

Se si verifica un errore irreversibile, la connessione al server FPolicy può essere interrotta. Dopo aver risolto il problema che ha causato l'errore irreversibile, è necessario riconnettersi manualmente al server FPolicy.

### Fasi

1. Connettersi al server FPolicy esterno utilizzando `vserver fpolicy engine-connect` comando.

Per ulteriori informazioni sul comando, vedere le pagine man.

2. Verificare che il server FPolicy esterno sia connesso utilizzando `vserver fpolicy show-engine` comando.

Per ulteriori informazioni sul comando, vedere le pagine man.

### Disconnettersi dai server FPolicy esterni

Potrebbe essere necessario disconnettersi manualmente da un server FPolicy esterno.

Ciò potrebbe essere utile se il server FPolicy ha problemi con l'elaborazione della richiesta di notifica o se è necessario eseguire la manutenzione sul server FPolicy.

**Fasi**

1. Disconnettersi dal server FPolicy esterno utilizzando `vserver fpolicy engine-disconnect` comando.  
  
Per ulteriori informazioni sul comando, vedere le pagine man.
2. Verificare che il server FPolicy esterno sia disconnesso utilizzando `vserver fpolicy show-engine` comando.  
  
Per ulteriori informazioni sul comando, vedere le pagine man.

**Visualizza informazioni sulle connessioni a server FPolicy esterni**

È possibile visualizzare informazioni sullo stato delle connessioni a server FPolicy esterni (server FPolicy) per il cluster o per una specifica macchina virtuale di storage (SVM). Queste informazioni consentono di determinare quali server FPolicy sono connessi.

**A proposito di questa attività**

Se non si specificano parametri, il comando visualizza le seguenti informazioni:

- Nome SVM
- Nome del nodo
- Nome del criterio FPolicy
- Indirizzo IP del server FPolicy
- Stato del server FPolicy
- Tipo di server FPolicy

Oltre a visualizzare informazioni sulle connessioni FPolicy sul cluster o su una specifica SVM, è possibile utilizzare i parametri dei comandi per filtrare l'output del comando in base ad altri criteri.

È possibile specificare `-instance` parametro per visualizzare informazioni dettagliate sui criteri elencati. In alternativa, è possibile utilizzare `-fields` parametro per visualizzare solo i campi indicati nell'output del comando. È possibile immettere ? dopo il `-fields` parametro per scoprire quali campi è possibile utilizzare.

**Fase**

1. Visualizzare le informazioni filtrate sullo stato della connessione tra il nodo e il server FPolicy utilizzando il comando appropriato:

|                                                                                                         |                                                             |
|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Se si desidera visualizzare le informazioni sullo stato della connessione relative ai server FPolicy... | Inserisci...                                                |
| Specificato dall'utente                                                                                 | <code>vserver fpolicy show-engine -server IP_address</code> |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Per una SVM specificata                     | <code>vserver fpolicy show-engine -vserver vserver_name</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Che sono associati a una policy specificata | <code>vserver fpolicy show-engine -policy-name policy_name</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Con lo stato del server specificato         | <code>vserver fpolicy show-engine -server-status status</code><br><br>Lo stato del server può essere uno dei seguenti: <ul style="list-style-type: none"> <li>• <code>connected</code></li> <li>• <code>disconnected</code></li> <li>• <code>connecting</code></li> <li>• <code>disconnecting</code></li> </ul>                                                                                                                                                                                                                                                                                                                                                                  |
| Con il tipo specificato                     | <code>vserver fpolicy show-engine -server-type type</code><br><br>Il tipo di server FPolicy può essere uno dei seguenti: <ul style="list-style-type: none"> <li>• <code>primary</code></li> <li>• <code>secondary</code></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Disconnessi con il motivo specificato       | <code>vserver fpolicy show-engine -disconnect-reason text</code><br><br>La disconnessione può essere dovuta a diversi motivi. Di seguito sono riportati i motivi più comuni per la disconnessione: <ul style="list-style-type: none"> <li>• <code>Disconnect command received from CLI.</code></li> <li>• <code>Error encountered while parsing notification response from FPolicy server.</code></li> <li>• <code>FPolicy Handshake failed.</code></li> <li>• <code>SSL handshake failed.</code></li> <li>• <code>TCP Connection to FPolicy server failed.</code></li> <li>• <code>The screen response message received from the FPolicy server is not valid.</code></li> </ul> |

### Esempio

Questo esempio mostra informazioni sulle connessioni esterne del motore ai server FPolicy su SVM `vs1.example.com`:

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
```

| FPolicy         |         |       |          | Server-      | Server- |
|-----------------|---------|-------|----------|--------------|---------|
| Vserver         | Policy  | Node  | Server   | status       | type    |
| -----           | -----   | ----- | -----    | -----        |         |
| vs1.example.com | policy1 | node1 | 10.1.1.2 | connected    | primary |
| vs1.example.com | policy1 | node1 | 10.1.1.3 | disconnected | primary |
| vs1.example.com | policy1 | node2 | 10.1.1.2 | connected    | primary |
| vs1.example.com | policy1 | node2 | 10.1.1.3 | disconnected | primary |

Nell'esempio riportato di seguito vengono visualizzate solo informazioni relative ai server FPolicy connessi:

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
```

| node  | vserver         | policy-name | server   |
|-------|-----------------|-------------|----------|
| ----- | -----           | -----       | -----    |
| node1 | vs1.example.com | policy1     | 10.1.1.2 |
| node2 | vs1.example.com | policy1     | 10.1.1.2 |

#### Visualizza le informazioni sullo stato della connessione pass-through-Read di FPolicy

È possibile visualizzare informazioni sullo stato della connessione pass-through-Read di FPolicy ai server FPolicy esterni (server FPolicy) per il cluster o per una specifica macchina virtuale di storage (SVM). Queste informazioni consentono di determinare quali server FPolicy dispongono di connessioni dati pass-through-Read e per quali server FPolicy la connessione pass-through-Read è disconnessa.

#### A proposito di questa attività

Se non si specifica alcun parametro, il comando visualizza le seguenti informazioni:

- Nome SVM
- Nome del criterio FPolicy
- Nome del nodo
- Indirizzo IP del server FPolicy
- Stato della connessione pass-through-Read di FPolicy

Oltre a visualizzare informazioni sulle connessioni FPolicy sul cluster o su una specifica SVM, è possibile utilizzare i parametri dei comandi per filtrare l'output del comando in base ad altri criteri.

È possibile specificare `-instance` parametro per visualizzare informazioni dettagliate sui criteri elencati. In alternativa, è possibile utilizzare `-fields` parametro per visualizzare solo i campi indicati nell'output del comando. È possibile immettere ? dopo il `-fields` parametro per scoprire quali campi è possibile utilizzare.

#### Fase

1. Visualizzare le informazioni filtrate sullo stato della connessione tra il nodo e il server FPolicy utilizzando il

comando appropriato:

|                                                                                           |                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se si desidera visualizzare le informazioni sullo stato della connessione relative a...   | Immettere il comando...                                                                                                                                                                                                                          |
| Stato della connessione pass-through-Read FPolicy per il cluster                          | <code>vserver fpolicy show-passthrough-read-connection</code>                                                                                                                                                                                    |
| Stato della connessione pass-through-Read FPolicy per una SVM specificata                 | <code>vserver fpolicy show-passthrough-read-connection -vserver vserver_name</code>                                                                                                                                                              |
| Stato della connessione pass-through-Read FPolicy per una policy specifica                | <code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name</code>                                                                                                                                                           |
| Stato dettagliato della connessione pass-through-Read di FPolicy per una policy specifica | <code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance</code>                                                                                                                                                 |
| Stato della connessione passthrough-Read FPolicy per lo stato specificato                 | <code>vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status</code> Lo stato del server può essere uno dei seguenti: <ul style="list-style-type: none"><li>• connected</li><li>• disconnected</li></ul> |

Esempio

Il seguente comando visualizza informazioni sulle connessioni pass-through-Read da tutti i server FPolicy del cluster:

```
cluster1::> vserver fpolicy show-passthrough-read-connection
```

| Vserver         | Policy Name | Node       | FPolicy Server | Server Status |
|-----------------|-------------|------------|----------------|---------------|
| vs2.example.com | pol_cifs_2  | FPolicy-01 | 2.2.2.2        | disconnected  |
| vs1.example.com | pol_cifs_1  | FPolicy-01 | 1.1.1.1        | connected     |

Il seguente comando visualizza informazioni dettagliate sulle connessioni pass-through-Read dai server FPolicy configurati nel criterio “pol\_cifs\_1”:

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name  
pol_cifs_1 -instance
```

Node: FPolicy-01

Vserver: vs1.example.com

Policy: pol\_cifs\_1

Server: 1.1.1.1

Session ID of the Control Channel: 8cef052e-2502-11e3-  
88d4-123478563412

Server Status: connected

Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45

Time Passthrough Read Channel was Disconnected: -

Reason for Passthrough Read Channel Disconnection: none

## Verificare l'accesso utilizzando il tracciamento di sicurezza

### Come funzionano le tracce di sicurezza

È possibile aggiungere filtri di tracciamento delle autorizzazioni per indicare a ONTAP di registrare le informazioni sul motivo per cui i server SMB e NFS su una macchina virtuale di storage (SVM) consentono o negano la richiesta di un client o di un utente di eseguire un'operazione. Ciò può essere utile quando si desidera verificare che lo schema di protezione per l'accesso ai file sia appropriato o quando si desidera risolvere i problemi di accesso ai file.

Le tracce di sicurezza consentono di configurare un filtro che rileva le operazioni client su SMB e NFS su SVM e di tracciare tutti i controlli di accesso corrispondenti a tale filtro. È quindi possibile visualizzare i risultati della traccia, che fornisce un pratico riepilogo del motivo per cui l'accesso è stato consentito o negato.

Se si desidera verificare le impostazioni di sicurezza per l'accesso SMB o NFS su file e cartelle su SVM o se si verifica un problema di accesso, è possibile aggiungere rapidamente un filtro per attivare il tracciamento delle autorizzazioni.

Il seguente elenco illustra importanti informazioni sul funzionamento delle tracce di protezione:

- ONTAP applica le tracce di sicurezza a livello di SVM.
- Ogni richiesta in entrata viene sottoposta a screening per verificare se corrisponde ai criteri di filtraggio di eventuali tracce di sicurezza attivate.
- Le tracce vengono eseguite per le richieste di accesso a file e cartelle.
- Le tracce possono filtrare in base ai seguenti criteri:
  - IP client
  - Percorso SMB o NFS
  - Nome di Windows
  - Nome UNIX

- Le richieste vengono sottoposte a screening per i risultati delle risposte di accesso *consentito* e *negato*.
- Ogni richiesta di criteri di filtraggio corrispondenti delle tracce attivate viene registrata nel log dei risultati della traccia.
- L'amministratore dello storage può configurare un timeout su un filtro per disattivarlo automaticamente.
- Se una richiesta corrisponde a più filtri, vengono registrati i risultati del filtro con il numero di indice più alto.
- L'amministratore dello storage può stampare i risultati dal log dei risultati della traccia per determinare il motivo per cui una richiesta di accesso è stata consentita o negata.

## **Tipi di controllo degli accessi monitorano le tracce di sicurezza**

I controlli di accesso per un file o una cartella vengono eseguiti in base a criteri multipli. Le tracce di sicurezza monitorano le operazioni su tutti questi criteri.

I tipi di controlli degli accessi monitorati dalle tracce di protezione includono quanto segue:

- Stile di sicurezza del volume e del qtree
- Sicurezza effettiva del file system contenente i file e le cartelle su cui sono richieste le operazioni
- Mappatura dell'utente
- Permessi a livello di condivisione
- Permessi a livello di esportazione
- Permessi a livello di file
- Sicurezza di Access Guard a livello di storage

## **Considerazioni per la creazione di tracce di protezione**

Quando si creano tracce di sicurezza sulle macchine virtuali di storage (SVM), è necessario tenere a mente diverse considerazioni. Ad esempio, è necessario conoscere i protocolli che è possibile creare una traccia, gli stili di protezione supportati e il numero massimo di tracce attive.

- È possibile creare tracce di sicurezza solo sulle SVM.
- Ogni voce di filtro di traccia di protezione è specifica per SVM.

Specificare la SVM su cui si desidera eseguire la traccia.

- È possibile aggiungere filtri di tracciamento delle autorizzazioni per le richieste SMB e NFS.
- È necessario configurare il server SMB o NFS sulla SVM su cui si desidera creare i filtri di traccia.
- È possibile creare tracce di sicurezza per file e cartelle che risiedono su NTFS, UNIX e volumi e qtree misti di sicurezza.
- È possibile aggiungere un massimo di 10 filtri di tracciamento delle autorizzazioni per SVM.
- Quando si crea o si modifica un filtro, è necessario specificare un numero di indice del filtro.

I filtri vengono considerati in ordine del numero di indice. I criteri di un filtro con un numero di indice superiore vengono considerati prima dei criteri con un numero di indice inferiore. Se la richiesta tracciata corrisponde ai criteri in più filtri abilitati, viene attivato solo il filtro con il numero di indice più alto.

- Dopo aver creato e attivato un filtro di traccia di protezione, è necessario eseguire alcune richieste di file o cartelle su un sistema client per generare attività che il filtro di traccia può acquisire e accedere al registro dei risultati di traccia.
- È necessario aggiungere filtri di tracciamento delle autorizzazioni solo per la verifica dell'accesso al file o per la risoluzione dei problemi.

L'aggiunta di filtri di tracciamento delle autorizzazioni ha un effetto minore sulle prestazioni del controller.

Una volta completata l'attività di verifica o risoluzione dei problemi, è necessario disattivare o rimuovere tutti i filtri di tracciamento delle autorizzazioni. Inoltre, i criteri di filtraggio selezionati devono essere il più specifici possibile, in modo che ONTAP non invii un numero elevato di risultati di traccia al registro.

## Eseguire le tracce di sicurezza

### Eseguire una panoramica delle tracce di sicurezza

L'esecuzione di una traccia di protezione implica la creazione di un filtro di traccia di protezione, la verifica dei criteri di filtro, la generazione di richieste di accesso su un client SMB o NFS che corrispondono ai criteri di filtro e la visualizzazione dei risultati.

Dopo aver utilizzato un filtro di sicurezza per acquisire le informazioni di traccia, è possibile modificare il filtro e riutilizzarlo oppure disattivarlo se non è più necessario. Dopo aver visualizzato e analizzato i risultati della traccia del filtro, è possibile eliminarli se non sono più necessari.

### Creare filtri di traccia per la sicurezza

È possibile creare filtri di traccia per la sicurezza che rilevano le operazioni dei client SMB e NFS sulle macchine virtuali di storage (SVM) e tracciano tutti i controlli di accesso corrispondenti al filtro. È possibile utilizzare i risultati delle tracce di protezione per convalidare la configurazione o risolvere i problemi di accesso.


#### A proposito di questa attività

Sono necessari due parametri per il comando `vserver Security trace filter create`:

| Parametri richiesti                | Descrizione                                                                                                                                                                                                                                  |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-vserver vserver_name</code> | <p><i>Nome SVM</i></p> <p>Il nome della SVM che contiene i file o le cartelle su cui si desidera applicare il filtro di traccia di protezione.</p>                                                                                           |
| <code>-index index_number</code>   | <p><i>Numero indice del filtro</i></p> <p>Il numero di indice che si desidera applicare al filtro. È possibile utilizzare un massimo di 10 filtri di traccia per SVM. I valori consentiti per questo parametro sono compresi tra 1 e 10.</p> |

Una serie di parametri di filtro opzionali consente di personalizzare il filtro di traccia di protezione in modo da restringere i risultati prodotti dalla traccia di protezione:



| Parametro del filtro                                                                                                                                                                                                                                           | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-client-ip IP_Address</code>                                                                                                                                                                                                                             | Questo filtro specifica l'indirizzo IP da cui l'utente accede a SVM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <code>-path path</code>                                                                                                                                                                                                                                        | <p>Questo filtro specifica il percorso su cui applicare il filtro di traccia delle autorizzazioni. Il valore per <code>-path</code> può utilizzare uno dei seguenti formati:</p> <ul style="list-style-type: none"> <li>• Il percorso completo, a partire dalla directory principale della condivisione o dell'esportazione</li> <li>• Un percorso parziale, relativo alla radice della condivisione</li> </ul> <p>È necessario utilizzare i separatori di directory in stile UNIX di NFS nel valore del percorso.</p>                                                                                                                            |
| <code>-windows-name win_user_name</code><br>oppure <code>-unix</code><br><code>-name ``unix_user_name</code>                                                                                                                                                   | <p>È possibile specificare il nome utente Windows o UNIX di cui si desidera tenere traccia delle richieste di accesso. La variabile del nome utente non fa distinzione tra maiuscole e minuscole. Non è possibile specificare un nome utente Windows e un nome utente UNIX nello stesso filtro.</p> <div>  <p>Anche se è possibile tracciare gli eventi di accesso SMB e NFS, l'utente UNIX mappato e i gruppi di utenti UNIX mappati potrebbero essere utilizzati quando si eseguono controlli di accesso su dati misti o UNIX di tipo di sicurezza.</p> </div> |
| <code>-trace-allow {yes</code>                                                                                                                                                                                                                                 | <code>no}</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p>La funzione di traccia per gli eventi di negazione è sempre abilitata per un filtro di traccia di protezione. Facoltativamente, è possibile tracciare gli eventi Allow. Per tracciare gli eventi Allow, impostare questo parametro su <code>yes</code>.</p> | <code>-enabled {enabled</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <code>disabled}</code>                                                                                                                                                                                                                                         | È possibile attivare o disattivare il filtro di traccia di protezione. Per impostazione predefinita, il filtro di traccia di protezione è attivato.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <code>-time-enabled integer</code>                                                                                                                                                                                                                             | È possibile specificare un timeout per il filtro, dopo il quale viene disattivato.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Fasi

### 1. Creazione di un filtro di traccia per la protezione:

```
vserver security trace filter create -vserver vserver_name -index
index_numberfilter_parameters
```

`filter_parameters` è un elenco di parametri di filtro opzionali.

Per ulteriori informazioni, vedere le pagine man del comando.

## 2. Verificare la voce Security trace filter:

```
vserver security trace filter show -vserver vserver_name -index index_number
```

### Esempi

Il comando seguente crea un filtro di traccia di protezione per qualsiasi utente che accede a un file con un percorso di condivisione `\\server\share1\dir1\dir2\file.txt` Dall'indirizzo IP 10.10.10.7. Il filtro utilizza un percorso completo per `-path` opzione. L'indirizzo IP del client utilizzato per accedere ai dati è 10.10.10.7. Il filtro si esaurisce dopo 30 minuti:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
```

| Vserver      | Index | Client-IP  | Path                | Trace-Allow |
|--------------|-------|------------|---------------------|-------------|
| Windows-Name |       |            |                     |             |
| -----        | ----- | -----      | -----               | -----       |
| vs1          | 1     | 10.10.10.7 | /dir1/dir2/file.txt | no          |

Il comando seguente crea un filtro di traccia di protezione utilizzando un percorso relativo per `-path` opzione. Il filtro traccia l'accesso di un utente Windows chiamato "joe". Joe sta accedendo a un file con un percorso di condivisione `\\server\share1\dir1\dir2\file.txt`. Le tracce del filtro consentono e negano gli eventi:

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
```

```

Vserver: vs1
Filter Index: 2
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: mydomain\joe
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

### Visualizza informazioni sui filtri di traccia per la sicurezza

È possibile visualizzare informazioni sui filtri di traccia di protezione configurati sulla macchina virtuale di storage (SVM). In questo modo è possibile visualizzare i tipi di eventi di accesso che ciascun filtro traccia.

## Fase

1. Visualizzare le informazioni relative alle voci del filtro di traccia di protezione utilizzando `vserver security trace filter show` comando.

Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine `man`.

## Esempi

Il seguente comando visualizza informazioni su tutti i filtri di traccia di sicurezza su SVM vs1:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index  Client-IP          Path                Trace-Allow
Windows-Name
-----
vs1      1      -                  /dir1/dir2/file.txt  yes                -
vs1      2      -                  /dir3/dir4/          no
mydomain\joe
```

## Visualizzare i risultati della traccia di sicurezza

È possibile visualizzare i risultati della traccia di protezione generati per le operazioni dei file che corrispondono ai filtri di traccia di protezione. È possibile utilizzare i risultati per convalidare la configurazione di sicurezza per l'accesso ai file o per risolvere i problemi di accesso ai file SMB e NFS.

### Di cosa hai bisogno

Per generare i risultati della traccia di protezione, è necessario che esista un filtro di traccia di protezione abilitato e che siano state eseguite operazioni da un client SMB o NFS che corrisponda al filtro di traccia di protezione.

### A proposito di questa attività

È possibile visualizzare un riepilogo di tutti i risultati della traccia di protezione oppure personalizzare le informazioni visualizzate nell'output specificando parametri opzionali. Ciò può essere utile quando i risultati della traccia di protezione contengono un gran numero di record.

Se non si specifica alcun parametro opzionale, viene visualizzato quanto segue:

- Nome SVM (Storage Virtual Machine)
- Nome del nodo
- Numero di indice della traccia di sicurezza
- Stile di sicurezza
- Percorso
- Motivo
- Nome utente

Il nome utente viene visualizzato in base alla configurazione del filtro di traccia:

|                               |                                                                                |
|-------------------------------|--------------------------------------------------------------------------------|
| Se il filtro è configurato... | Quindi...                                                                      |
| Con un nome utente UNIX       | Il risultato della traccia di protezione visualizza il nome utente UNIX.       |
| Con un nome utente Windows    | Il risultato della traccia di protezione visualizza il nome utente di Windows. |
| Senza nome utente             | Il risultato della traccia di protezione visualizza il nome utente di Windows. |

È possibile personalizzare l'output utilizzando parametri opzionali. Alcuni dei parametri facoltativi che è possibile utilizzare per limitare i risultati restituiti nell'output del comando includono:

| Parametro facoltativo                       | Descrizione                                                                                                                                                                                                          |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-fields field_name, ...</code>        | Visualizza l'output nei campi scelti. È possibile utilizzare questo parametro da solo o in combinazione con altri parametri opzionali.                                                                               |
| <code>-instance</code>                      | Visualizza informazioni dettagliate sugli eventi di analisi della sicurezza. Utilizzare questo parametro con altri parametri opzionali per visualizzare informazioni dettagliate sui risultati specifici del filtro. |
| <code>-node node_name</code>                | Visualizza solo informazioni sugli eventi nel nodo specificato.                                                                                                                                                      |
| <code>-vserver vserver_name</code>          | Visualizza solo le informazioni sugli eventi sulla SVM specificata.                                                                                                                                                  |
| <code>-index integer</code>                 | Visualizza le informazioni sugli eventi che si sono verificati come risultato del filtro corrispondente al numero di indice specificato.                                                                             |
| <code>-client-ip IP_address</code>          | Visualizza informazioni sugli eventi che si sono verificati in seguito all'accesso al file dall'indirizzo IP del client specificato.                                                                                 |
| <code>-path path</code>                     | Visualizza le informazioni sugli eventi che si sono verificati in seguito all'accesso al file al percorso specificato.                                                                                               |
| <code>-user-name user_name</code>           | Visualizza informazioni sugli eventi che si sono verificati in seguito all'accesso al file da parte dell'utente Windows o UNIX specificato.                                                                          |
| <code>-security-style security_style</code> | Visualizza informazioni sugli eventi che si sono verificati nei file system con lo stile di sicurezza specificato.                                                                                                   |

Consultare la pagina man per informazioni sugli altri parametri opzionali che è possibile utilizzare con il comando.

## Fase

1. Visualizzare i risultati del filtro di traccia di protezione utilizzando `vserver security trace trace-`

result show comando.

```
vserver security trace trace-result show -user-name domain\user
```

Vserver: vs1

| Node  | Index | Filter Details                                               | Reason                        |
|-------|-------|--------------------------------------------------------------|-------------------------------|
| ----- | ----- | -----                                                        | -----                         |
| node1 | 3     | User:domain\user<br>Security Style:mixed<br>Path:/dir1/dir2/ | Access denied by explicit ACE |
| node1 | 5     | User:domain\user<br>Security Style:unix<br>Path:/dir1/       | Access denied by explicit ACE |

## Modificare i filtri di traccia di protezione

Se si desidera modificare i parametri di filtro opzionali utilizzati per determinare gli eventi di accesso da tracciare, è possibile modificare i filtri di traccia di protezione esistenti.

### A proposito di questa attività

È necessario identificare il filtro di traccia di protezione che si desidera modificare specificando il nome della macchina virtuale di storage (SVM) a cui è applicato il filtro e il numero di indice del filtro. È possibile modificare tutti i parametri del filtro opzionali.

### Fasi

1. Modificare un filtro di traccia di protezione:

```
vserver security trace filter modify -vserver vserver_name -index  
index_numberfilter_parameters
```

- ° `vserver_name` È il nome della SVM su cui si desidera applicare un filtro di traccia di protezione.
- ° `index_number` è il numero di indice che si desidera applicare al filtro. I valori consentiti per questo parametro sono compresi tra 1 e 10.
- ° `filter_parameters` è un elenco di parametri di filtro opzionali.

2. Verificare la voce Security trace filter:

```
vserver security trace filter show -vserver vserver_name -index index_number
```

### Esempio

Il comando seguente modifica il filtro di traccia di protezione con il numero di indice 1. Il filtro traccia gli eventi di qualsiasi utente che accede a un file con un percorso di condivisione

\\server\share1\dir1\dir2\file.txt Da qualsiasi indirizzo IP. Il filtro utilizza un percorso completo per `-path` opzione. Le tracce del filtro consentono e negano gli eventi:

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
Vserver: vs1
Filter Index: 1
Client IP Address to Match: -
Path: /dir1/dir2/file.txt
Windows User Name: -
UNIX User Name: -
Trace Allow Events: yes
Filter Enabled: enabled
Minutes Filter is Enabled: 60
```

### Eliminare i filtri di traccia di sicurezza

Quando non è più necessario un filtro di traccia di protezione, è possibile eliminarlo. Poiché è possibile disporre di un massimo di 10 filtri di traccia di sicurezza per macchina virtuale di storage (SVM), l'eliminazione dei filtri non necessari consente di creare nuovi filtri se si è raggiunto il massimo.

#### A proposito di questa attività

Per identificare in modo univoco il filtro di traccia di protezione che si desidera eliminare, è necessario specificare quanto segue:

- Il nome della SVM a cui viene applicato il filtro di traccia
- Il numero dell'indice del filtro di traccia

#### Fasi

1. Identificare il numero di indice del filtro della voce di Security trace filter che si desidera eliminare:

```
vserver security trace filter show -vserver vserver_name

vserver security trace filter show -vserver vs1
```

| Vserver      | Index | Client-IP | Path                | Trace-Allow | Windows-Name |
|--------------|-------|-----------|---------------------|-------------|--------------|
| -----        | ----- | -----     | -----               | -----       | -----        |
| vs1          | 1     | -         | /dir1/dir2/file.txt | yes         | -            |
| vs1          | 2     | -         | /dir3/dir4/         | no          |              |
| mydomain\joe |       |           |                     |             |              |

2. Utilizzando le informazioni sul numero di indice del filtro del passaggio precedente, eliminare la voce del filtro:

```
vserver security trace filter delete -vserver vserver_name -index index_number

vserver security trace filter delete -vserver vs1 -index 1
```

### 3. Verificare che la voce Security trace filter sia stata eliminata:

```
vserver security trace filter show -vserver vserver_name

vserver security trace filter show -vserver vs1
```

| Vserver      | Index | Client-IP | Path        | Trace-Allow |
|--------------|-------|-----------|-------------|-------------|
| Windows-Name |       |           |             |             |
| vs1          | 2     | -         | /dir3/dir4/ | no          |
| mydomain\joe |       |           |             |             |

## Eliminare i record di traccia di sicurezza

Dopo aver utilizzato un record di traccia del filtro per verificare la sicurezza dell'accesso ai file o per risolvere i problemi di accesso al client SMB o NFS, è possibile eliminare il record di traccia della protezione dal registro di traccia della protezione.

### A proposito di questa attività

Prima di eliminare un record di traccia di protezione, è necessario conoscere il numero di sequenza del record.



Ogni macchina virtuale di storage (SVM) può memorizzare un massimo di 128 record di traccia. Se si raggiunge il valore massimo sulla SVM, i record di traccia meno recenti vengono eliminati automaticamente quando vengono aggiunti nuovi record. Se non si desidera eliminare manualmente i record di traccia su questa SVM, è possibile consentire a ONTAP di eliminare automaticamente i risultati di traccia meno recenti una volta raggiunto il numero massimo di risultati per creare spazio per i nuovi risultati.

## Fasi

### 1. Identificare il numero di sequenza del record che si desidera eliminare:

```
vserver security trace trace-result show -vserver vserver_name -instance
```

### 2. Eliminare il record di traccia di protezione:

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name -seqnum integer

vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
999
```

° -node node\_name è il nome del nodo del cluster in cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.

Questo è un parametro obbligatorio.

- `-vserver vserver_name` È il nome della SVM in cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.

Questo è un parametro obbligatorio.

- `-seqnum integer` è il numero di sequenza dell'evento di log che si desidera eliminare.

Questo è un parametro obbligatorio.

## Eliminare tutti i record di traccia di sicurezza

Se non si desidera conservare alcun record di traccia di protezione esistente, è possibile eliminare tutti i record di un nodo con un singolo comando.

### Fase

1. Eliminare tutti i record di traccia di sicurezza:

```
vserver security trace trace-result delete -node node_name -vserver  
vserver_name *
```

- `-node node_name` è il nome del nodo del cluster in cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.
- `-vserver vserver_name` È il nome della macchina virtuale di storage (SVM) su cui si è verificato l'evento di tracciamento delle autorizzazioni che si desidera eliminare.

## Interpretare i risultati della traccia di sicurezza

I risultati della traccia di protezione forniscono il motivo per cui una richiesta è stata consentita o negata. L'output visualizza il risultato come combinazione del motivo per cui l'accesso è consentito o negato e della posizione all'interno del percorso di controllo degli accessi in cui l'accesso è consentito o negato. È possibile utilizzare i risultati per isolare e identificare i motivi per cui le azioni sono o non sono consentite.

### Ricerca di informazioni sugli elenchi dei tipi di risultati e sui dettagli dei filtri

È possibile trovare gli elenchi dei tipi di risultati e i dettagli dei filtri che possono essere inclusi nei risultati della traccia di protezione nelle pagine man di `vserver security trace trace-result show` comando.

### Esempio di output da Reason in un campo Allow tipo di risultato

Di seguito viene riportato un esempio dell'output di Reason che viene visualizzato nel log dei risultati della traccia in un Allow tipo di risultato:

```
Access is allowed because SMB implicit permission grants requested  
access while opening existing file or directory.
```



```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

### **Esempio di output da Reason in un campo Allow tipo di risultato**

Di seguito viene riportato un esempio dell'output di Reason che viene visualizzato nel log dei risultati della traccia in un Deny tipo di risultato:

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

### **Esempio di output da Filter details campo**

Di seguito viene riportato un esempio dell'output di Filter details nel log dei risultati della traccia, che elenca lo stile di sicurezza effettivo del file system contenente file e cartelle che corrispondono ai criteri di filtro:

```
Security Style: MIXED and ACL
```

## **Dove trovare ulteriori informazioni**

Una volta verificato l'accesso al client SMB, è possibile eseguire una configurazione SMB avanzata o aggiungere l'accesso SAN. Una volta verificato l'accesso al client NFS, è possibile eseguire una configurazione NFS avanzata o aggiungere l'accesso SAN. Una volta completato l'accesso al protocollo, è necessario proteggere il volume root di SVM.

### **Configurazione SMB**

È possibile configurare ulteriormente l'accesso SMB utilizzando quanto segue:

- ["Gestione delle PMI"](#)

Descrive come configurare e gestire l'accesso ai file utilizzando il protocollo SMB.

- ["Report tecnico di NetApp 4191: Guida alle Best practice per i file service Windows di Clustered Data ONTAP 8.2"](#)

Fornisce una breve panoramica dell'implementazione SMB e di altre funzionalità di servizi file Windows con consigli e informazioni di base per la risoluzione dei problemi di ONTAP.

- ["Report tecnico di NetApp 3740: Protocollo CIFS di prossima generazione per PMI 2 in Data ONTAP"](#)

Descrive le funzionalità di SMB 2, i dettagli di configurazione e la relativa implementazione in ONTAP.

### **Configurazione NFS**

È possibile configurare ulteriormente l'accesso NFS utilizzando quanto segue:

- ["Gestione NFS"](#)

Descrive come configurare e gestire l'accesso ai file utilizzando il protocollo NFS.

- ["Report tecnico di NetApp 4067: Guida all'implementazione e alle Best practice di NFS"](#)

Funge da guida operativa NFSv3 e NFSv4 e fornisce una panoramica del sistema operativo ONTAP con particolare attenzione a NFSv4.

- ["Report tecnico di NetApp 4668: Guida alle Best practice per i servizi di nome"](#)

Fornisce un elenco completo di Best practice, limiti, raccomandazioni e considerazioni per la configurazione di LDAP, NIS, DNS e file di utenti e gruppi locali a scopo di autenticazione.

- ["Report tecnico NetApp 4616: NFS Kerberos in ONTAP con Microsoft Active Directory"](#)
- ["Report tecnico di NetApp 4835: Come configurare LDAP in ONTAP"](#)
- ["Report tecnico di NetApp 3580: Guida ai miglioramenti e alle Best practice di NFSv4 per l'implementazione di Data ONTAP"](#)

Descrive le Best practice da seguire durante l'implementazione dei componenti NFSv4 su client AIX, Linux o Solaris collegati a sistemi che eseguono ONTAP.

## Protezione del volume root

Dopo aver configurato i protocolli su SVM, assicurarsi che il volume root sia protetto:

- ["Protezione dei dati"](#)

Descrive come creare un mirror di condivisione del carico per proteggere il volume root SVM, una Best practice NetApp per le SVM abilitate per NAS. Viene inoltre descritto come eseguire rapidamente il ripristino da guasti o perdite di volume promuovendo il volume root SVM da un mirror di condivisione del carico.

# Gestione della crittografia con System Manager


## Crittografare i dati memorizzati utilizzando la crittografia basata su software


Utilizzare la crittografia del volume per garantire che i dati del volume non possano essere letti se il dispositivo sottostante viene riassegnato, restituito, smarrito o rubato. La crittografia dei volumi non richiede dischi speciali, ma funziona con tutti gli HDD e gli SSD.

La crittografia del volume richiede un gestore delle chiavi. È possibile configurare Onboard Key Manager utilizzando System Manager. È anche possibile utilizzare un gestore di chiavi esterno, ma è necessario prima impostarlo utilizzando l'interfaccia utente di ONTAP.

Una volta configurato il gestore delle chiavi, i nuovi volumi vengono crittografati per impostazione predefinita.

### Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. In **Encryption**, fare clic su  Per configurare Onboard Key Manager per la prima volta.
3. Per crittografare i volumi esistenti, fare clic su **Storage > Volumes** (archiviazione > volumi).

4. Sul volume desiderato, fare clic su  Quindi fare clic su **Edit** (Modifica).
5. Selezionare **Enable Encryption** (attiva crittografia).



## Crittografare i dati memorizzati utilizzando unità con crittografia automatica

Utilizzare la crittografia del disco per garantire che tutti i dati di un Tier locale non possano essere letti se il dispositivo sottostante viene riassegnato, restituito, smarrito o rubato. La crittografia dei dischi richiede speciali HDD o SSD con crittografia automatica.

La crittografia del disco richiede un gestore delle chiavi. È possibile configurare il gestore delle chiavi integrato utilizzando System Manager. È anche possibile utilizzare un gestore di chiavi esterno, ma è necessario prima impostarlo utilizzando l'interfaccia utente di ONTAP.

Se ONTAP rileva dischi con crittografia automatica, richiede di configurare il gestore delle chiavi integrato quando si crea il Tier locale.

### Fasi

1. In **Encryption**, fare clic su  per configurare il gestore delle chiavi integrato.
2. Se viene visualizzato un messaggio che indica la necessità di riscrivere i dischi, fare clic su , Quindi fare clic su **Rekey Disks**.

## Gestire la crittografia con la CLI

### Panoramica sulla crittografia NetApp

NetApp offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

- La crittografia basata su software con NetApp Volume Encryption (NVE) supporta la crittografia dei dati di un volume alla volta
- La crittografia basata su hardware con NetApp Storage Encryption (NSE) supporta la crittografia completa dei dati su disco (FDE) durante la scrittura.

### Configurare NetApp Volume Encryption

#### Panoramica sulla configurazione di NetApp Volume Encryption

NetApp Volume Encryption (NVE) è una tecnologia software per la crittografia dei dati inattivi di un volume alla volta. Una chiave di crittografia accessibile solo al sistema di storage impedisce la lettura dei dati del volume in caso di riallocazione, restituzione, smarrimento o furto del dispositivo sottostante.

#### Comprensione di NVE

Con NVE, sia i metadati che i dati (incluse le copie Snapshot) vengono crittografati. L'accesso ai dati viene fornito da una chiave XTS-AES-256 univoca, una per volume. Un server di gestione delle chiavi esterno o Onboard Key Manager (OKM) serve le chiavi ai nodi:

- Il server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol). Si consiglia di configurare i server di gestione delle chiavi esterni su un sistema storage diverso dai dati.
- Onboard Key Manager è uno strumento integrato che serve le chiavi ai nodi dello stesso sistema storage dei dati.

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita se si dispone di una licenza di crittografia del volume (VE) e si utilizza un gestore di chiavi integrato o esterno. La licenza VE è inclusa con "ONTAP uno". Ogni volta che viene configurato un gestore di chiavi esterno o integrato, viene modificato il modo in cui viene configurata la crittografia dei dati inattivi per aggregati nuovi di zecca e volumi nuovi di zecca. I nuovi aggregati avranno NetApp aggregate Encryption (NAE) abilitato per impostazione predefinita. I volumi nuovi di zecca che non fanno parte di un aggregato NAE avranno NetApp Volume Encryption (NVE) abilitato per impostazione predefinita. Se una macchina virtuale per lo storage dei dati (SVM) viene configurata con un proprio gestore delle chiavi utilizzando la gestione delle chiavi multi-tenant, il volume creato per tale SVM viene configurato automaticamente con NVE.

È possibile attivare la crittografia su un volume nuovo o esistente. NVE supporta la gamma completa di funzionalità per l'efficienza dello storage, tra cui deduplica e compressione. A partire da ONTAP 9.14.1, è possibile [Abilitazione di NVE su volumi root SVM esistenti](#).



Se si utilizza SnapLock, è possibile attivare la crittografia solo su volumi SnapLock nuovi e vuoti. Non è possibile attivare la crittografia su un volume SnapLock esistente.

È possibile utilizzare NVE su qualsiasi tipo di aggregato (HDD, SSD, ibrido, LUN array), con qualsiasi tipo di RAID e in qualsiasi implementazione ONTAP supportata, incluso ONTAP Select. È inoltre possibile utilizzare NVE con crittografia basata su hardware per "crittografare `ddoppio`" i dati su dischi con crittografia automatica.

Quando NVE è abilitato, anche il core dump è crittografato.

### Crittografia a livello di aggregato

Normalmente, a ogni volume crittografato viene assegnata una chiave univoca. Quando il volume viene cancellato, la chiave viene eliminata con esso.

A partire da ONTAP 9.6, è possibile utilizzare la crittografia aggregata NetApp per assegnare le chiavi all'aggregato contenente per i volumi da crittografare. Quando si elimina un volume crittografato, le chiavi dell'aggregato vengono conservate. Le chiavi vengono eliminate se l'intero aggregato viene cancellato.

Se si intende eseguire la deduplica a livello di aggregato inline o in background, è necessario utilizzare la crittografia a livello di aggregato. La deduplica a livello di aggregato non è altrimenti supportata da NVE.

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita se si dispone di una licenza di crittografia del volume (VE) e si utilizza un gestore di chiavi integrato o esterno.

I volumi NVE e NAE possono coesistere sullo stesso aggregato. Per impostazione predefinita, i volumi crittografati con crittografia a livello di aggregato sono volumi NAE. È possibile ignorare l'impostazione predefinita quando si crittografa il volume.

È possibile utilizzare `volume move` Per convertire un volume NVE in un volume NAE e viceversa. È possibile replicare un volume NAE in un volume NVE.

Non è possibile utilizzare `secure purge` Comandi su un volume NAE.

## Quando utilizzare server di gestione delle chiavi esterni

Sebbene sia meno costoso e generalmente più conveniente utilizzare il gestore delle chiavi integrato, è necessario configurare i server KMIP se si verifica una delle seguenti condizioni:

- La soluzione di gestione delle chiavi di crittografia deve essere conforme agli standard FIPS (Federal Information Processing Standards) 140-2 o ALLO standard OASIS KMIP.
- Hai bisogno di una soluzione multi-cluster, con gestione centralizzata delle chiavi di crittografia.
- La tua azienda richiede una maggiore sicurezza nell'archiviazione delle chiavi di autenticazione su un sistema o in una posizione diversa dai dati.

## Scopo della gestione esterna delle chiavi

L'ambito della gestione esterna delle chiavi determina se i server di gestione delle chiavi proteggono tutte le SVM nel cluster o solo le SVM selezionate:

- È possibile utilizzare un *ambito del cluster* per configurare la gestione delle chiavi esterne per tutte le SVM nel cluster. L'amministratore del cluster ha accesso a tutte le chiavi memorizzate sui server.
- A partire da ONTAP 9.6, è possibile utilizzare un *ambito SVM* per configurare la gestione delle chiavi esterne per una SVM denominata nel cluster. Questo è il meglio per gli ambienti multi-tenant in cui ciascun tenant utilizza una SVM (o un insieme di SVM) diversa per la distribuzione dei dati. Solo l'amministratore SVM di un determinato tenant ha accesso alle chiavi del tenant.
- A partire da ONTAP 9.10.1, è possibile utilizzare [Azure Key Vault e Google Cloud KMS](#) Proteggere le chiavi NVE solo per dati SVM. Questa funzione è disponibile per i sistemi KMS di AWS a partire dal 9.12.0.

È possibile utilizzare entrambi gli ambiti nello stesso cluster. Se i server di gestione delle chiavi sono stati configurati per una SVM, ONTAP utilizza solo questi server per proteggere le chiavi. In caso contrario, ONTAP protegge le chiavi con i server di gestione delle chiavi configurati per il cluster.

Un elenco di Key Manager esterni validati è disponibile in "[Tool di matrice di interoperabilità NetApp \(IMT\)](#)". Per trovare questo elenco, inserire il termine "Key Manager" nella funzione di ricerca di IMT.

## Dettagli del supporto

La seguente tabella mostra i dettagli del supporto NVE:

| Risorsa o funzione | Dettagli del supporto                                                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Piattaforme        | Funzionalità di offload AES-NI richiesta. Consultare il Hardware Universe (HWU) per verificare che NVE e NAE siano supportati per la piattaforma in uso. |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Crittografia                        | <p>A partire da ONTAP 9.7, gli aggregati e i volumi appena creati vengono crittografati per impostazione predefinita quando si aggiunge una licenza VE (Volume Encryption) e si dispone di un gestore di chiavi integrato o esterno configurato. Se è necessario creare un aggregato non crittografato, utilizzare il seguente comando:</p> <pre>storage aggregate create -encrypt-with-aggr-key false</pre> <p>Se è necessario creare un volume di testo normale, utilizzare il seguente comando:</p> <pre>volume create -encrypt false</pre> <p>La crittografia non è attivata per impostazione predefinita quando:</p> <ul style="list-style-type: none"> <li>• La licenza VE non è installata.</li> <li>• Gestore chiavi non configurato.</li> <li>• La piattaforma o il software non supportano la crittografia.</li> <li>• La crittografia hardware è attivata.</li> </ul> |
| ONTAP                               | Tutte le implementazioni ONTAP. Il supporto per il cloud ONTAP è disponibile in ONTAP 9.5 e versioni successive.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Dispositivi                         | HDD, SSD, ibrido, LUN array.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| RAID                                | RAID0, RAID4, RAID-DP, RAID-TEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Volumi                              | Volumi di dati e volumi root della SVM esistenti. Non puoi crittografare i dati sui volumi di metadati MetroCluster. Nelle versioni di ONTAP precedenti alla 9.14.1, non è possibile crittografare i dati sul volume root della SVM con NVE. A partire da ONTAP 9.14.1, ONTAP supporta <a href="#">NVE su volumi root SVM</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Crittografia a livello di aggregato | <p>A partire da ONTAP 9.6, NVE supporta la crittografia a livello aggregato (NAE):</p> <ul style="list-style-type: none"> <li>• Se si intende eseguire la deduplica a livello di aggregato inline o in background, è necessario utilizzare la crittografia a livello di aggregato.</li> <li>• Non è possibile reimmettere la chiave di un volume di crittografia a livello di aggregato.</li> <li>• L'eliminazione sicura non è supportata sui volumi di crittografia a livello di aggregato.</li> <li>• Oltre ai volumi di dati, NAE supporta la crittografia dei volumi root SVM e del volume di metadati MetroCluster. NAE non supporta la crittografia del volume root.</li> </ul>                                                                                                                                                                                           |
| Ambito SVM                          | A partire da ONTAP 9.6, NVE supporta l'ambito SVM solo per la gestione delle chiavi esterne, non per Onboard Key Manager. MetroCluster è supportato a partire da ONTAP 9.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

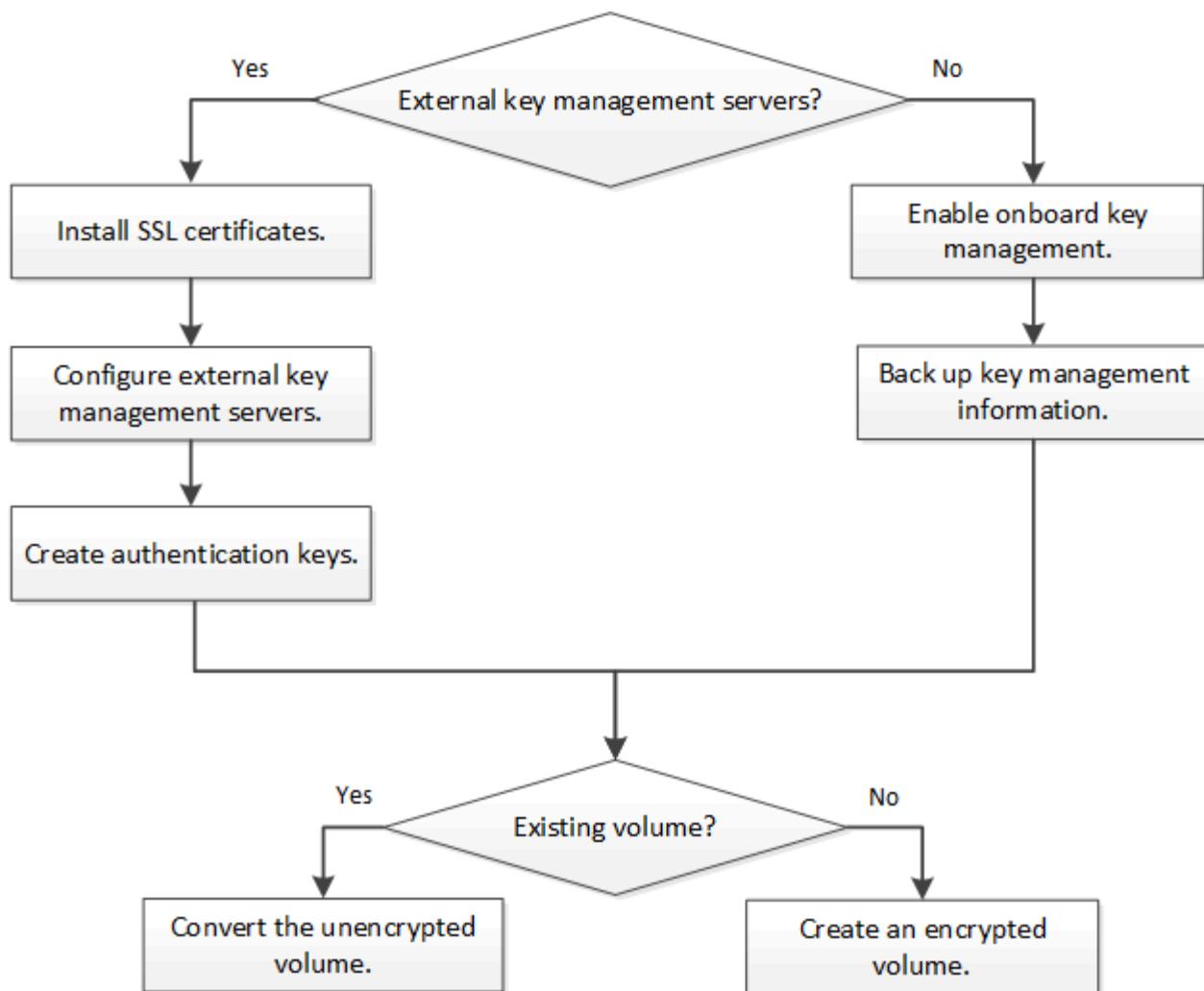
|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Efficienza dello storage | <p>Deduplica, compressione, compattazione, FlexClone.</p> <p>I cloni utilizzano la stessa chiave del padre, anche dopo aver sdoppiato il clone dal padre. Eseguire una <code>volume move</code> su un clone split, dopodiché il clone split avrà una chiave diversa.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Replica                  | <ul style="list-style-type: none"> <li>• Per la replica dei volumi, i volumi di origine e di destinazione possono avere impostazioni di crittografia diverse. La crittografia può essere configurata per l'origine e non configurata per la destinazione e viceversa.</li> <li>• Per la replica SVM, il volume di destinazione viene crittografato automaticamente, a meno che la destinazione non contenga un nodo che supporti la crittografia del volume, nel qual caso la replica riesce, ma il volume di destinazione non viene crittografato.</li> <li>• Per le configurazioni MetroCluster, ogni cluster estrae le chiavi di gestione delle chiavi esterne dai relativi server delle chiavi configurati. Le chiavi OKM vengono replicate nel sito del partner dal servizio di replica della configurazione.</li> </ul> |
| Conformità               | A partire da ONTAP 9.2, SnapLock è supportato sia in modalità Compliance che Enterprise, solo per nuovi volumi. Non è possibile attivare la crittografia su un volume SnapLock esistente.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| FlexGroups               | A partire da ONTAP 9.2, sono supportati FlexGroups. Gli aggregati di destinazione devono essere dello stesso tipo degli aggregati di origine, a livello di volume o aggregato. A partire da ONTAP 9.5, è supportata la rekey in-place dei volumi FlexGroup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Transizione 7-Mode       | A partire da 7-Mode Transition Tool 3.3, è possibile utilizzare 7-Mode Transition Tool CLI per eseguire una transizione basata su copia a volumi di destinazione abilitati per NVE sul sistema in cluster.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

#### Informazioni correlate

["FAQ - NetApp Volume Encryption e NetApp aggregate Encryption"](#)

#### Workflow di NetApp Volume Encryption

È necessario configurare i servizi di gestione delle chiavi prima di poter attivare la crittografia dei volumi. È possibile attivare la crittografia su un nuovo volume o su un volume esistente.



"È necessario installare la [licenza VE](#)" E configurare i servizi di gestione delle chiavi prima di poter criptare i dati con NVE. Prima di installare la licenza, è necessario ["Determinare se la versione di ONTAP in uso supporta NVE"](#).

## Configurare NVE

### Determinare se la versione del cluster supporta NVE

Prima di installare la licenza, è necessario determinare se la versione del cluster supporta NVE. È possibile utilizzare `version` per determinare la versione del cluster.

### A proposito di questa attività

La versione del cluster è la versione più bassa di ONTAP in esecuzione su qualsiasi nodo del cluster.

### Fase

1. Determinare se la versione del cluster supporta NVE:

```
version -v
```

NVE non è supportato se l'output del comando visualizza il testo "1Ono-DARE" (per "no Data at Rest Encryption") o se si utilizza una piattaforma non elencata nella ["Dettagli del supporto"](#).

Il seguente comando determina se NVE è supportato su `cluster1`.



```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
```

L'output di 1Ono-DARE Indica che NVE non è supportato sulla versione del cluster.

## Installare la licenza

Una licenza VE consente di utilizzare la funzione su tutti i nodi del cluster. Questa licenza è necessaria prima di poter crittografare i dati con NVE. È incluso con ["ONTAP uno"](#).

Prima di ONTAP One, la licenza VE era inclusa nel pacchetto crittografia. Il pacchetto di crittografia non è più disponibile, ma è ancora valido. Sebbene non sia attualmente richiesto, i clienti esistenti possono scegliere di farlo ["Eseguire l'aggiornamento a ONTAP One"](#).

## Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario aver ricevuto la chiave di licenza VE dal rappresentante di vendita o avere installato ONTAP ONE.

## Fasi

1. ["Verificare che la licenza VE sia installata"](#).

Il nome del pacchetto di licenza VE è `VE`.

2. Se la licenza non è installata, ["Utilizzare Gestione sistema o l'interfaccia CLI di ONTAP per installarlo"](#).

## Configurare la gestione esterna delle chiavi

### Configurare una panoramica sulla gestione esterna delle chiavi

È possibile utilizzare uno o più server di gestione delle chiavi esterni per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. Un server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).



Per ONTAP 9.1 e versioni precedenti, è necessario assegnare le LIF di gestione dei nodi alle porte configurate con il ruolo di gestione dei nodi prima di poter utilizzare il gestore delle chiavi esterno.

NetApp Volume Encryption (NVE) supporta Onboard Key Manager in ONTAP 9.1 e versioni successive. A partire da ONTAP 9.3, NVE supporta la gestione delle chiavi esterne (KMIP) e Onboard Key Manager. A partire da ONTAP 9.10.1, è possibile utilizzare [Azure Key Vault](#) o [Google Cloud Key Manager Service](#) Per proteggere le chiavi NVE. A partire da ONTAP 9.11.1, è possibile configurare più Key Manager esterni in un cluster. Vedere [Configurare i server delle chiavi in cluster](#).

## Gestisci i manager delle chiavi esterne con System Manager

A partire da ONTAP 9.7, è possibile memorizzare e gestire le chiavi di autenticazione e crittografia con Onboard Key Manager. A partire da ONTAP 9.13.1, è possibile utilizzare

anche i gestori delle chiavi esterni per memorizzare e gestire queste chiavi.

Onboard Key Manager memorizza e gestisce le chiavi in un database sicuro interno al cluster. Il suo scopo è il cluster. Un gestore delle chiavi esterno memorizza e gestisce le chiavi all'esterno del cluster. Il suo ambito può essere il cluster o la VM di storage. È possibile utilizzare uno o più gestori di chiavi esterne. Si applicano le seguenti condizioni:

- Se Onboard Key Manager è attivato, non è possibile attivare un gestore di chiavi esterno a livello di cluster, ma può essere attivato a livello di storage VM.
- Se un gestore delle chiavi esterno è abilitato a livello di cluster, il gestore delle chiavi integrato non può essere abilitato.

Quando si utilizzano key manager esterni, è possibile registrare fino a quattro key server primari per storage VM e cluster. Ogni server principale delle chiavi può essere cluster con un massimo di tre server secondari delle chiavi.



### Configurare un gestore di chiavi esterno


Per aggiungere un gestore di chiavi esterno per una VM di storage, è necessario aggiungere un gateway opzionale quando si configura l'interfaccia di rete per la VM di storage. Se la VM di storage è stata creata senza il percorso di rete, sarà necessario creare il percorso in modo esplicito per il gestore delle chiavi esterno. Vedere "[Creazione di una LIF \(interfaccia di rete\)](#)".



#### Fasi

È possibile configurare un gestore di chiavi esterno partendo da posizioni diverse in System Manager.

1. Per configurare un gestore di chiavi esterno, eseguire una delle seguenti operazioni iniziali.

| Workflow                                                                                               | Navigazione                      | Fase di avvio                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configurare Key Manager                                                                                | <b>Cluster &gt; Impostazioni</b> | Scorrere fino alla sezione <b>sicurezza</b> . In <b>Encryption</b> , selezionare  . Selezionare <b>External Key Manager</b> .                    |
| Aggiungi Tier locale                                                                                   | <b>Storage &gt; Tier</b>         | Selezionare <b>+ Aggiungi livello locale</b> . Selezionare la casella di controllo "Configure Key Manager" (Configura gestore chiavi). Selezionare <b>External Key Manager</b> .                                                      |
| Preparare lo storage                                                                                   | <b>Dashboard</b>                 | Nella sezione <b>capacità</b> , selezionare <b>Prepare Storage</b> (prepara storage). Quindi, selezionare "Configure Key Manager" (Configura gestore chiavi). Selezionare <b>External Key Manager</b> .                               |
| Configurare la crittografia (solo gestore delle chiavi nell'ambito delle macchine virtuali di storage) | <b>Storage &gt; Storage VM</b>   | Selezionare la VM di storage. Selezionare la scheda <b>Impostazioni</b> . Nella sezione <b>Encryption</b> sotto <b>Security</b> , selezionare  . |

2. Per aggiungere un server delle chiavi principale, selezionare  **Add** E compilare i campi **IP Address (Indirizzo IP)** o **host Name (Nome host)** e **Port** (porta).



- I certificati esistenti installati sono elencati nei campi **certificati CA del server KMIP** e **certificato client KMIP**. È possibile eseguire una delle seguenti operazioni:
  - Selezionare  per selezionare i certificati installati che si desidera mappare al gestore delle chiavi. (È possibile selezionare più certificati CA di servizio, ma è possibile selezionare un solo certificato client).
  - Selezionare **Aggiungi nuovo certificato** per aggiungere un certificato non ancora installato e associarlo al gestore delle chiavi esterno.
  - Selezionare  accanto al nome del certificato per eliminare i certificati installati che non si desidera mappare al gestore delle chiavi esterno.
- Per aggiungere un server chiavi secondario, selezionare **Aggiungi** nella colonna **Server chiavi secondari** e fornire i relativi dettagli.
- Selezionare **Salva** per completare la configurazione.



## Modificare un gestore di chiavi esterno esistente

Se è già stato configurato un gestore di chiavi esterno, è possibile modificarne le impostazioni.

### Fasi

- Per modificare la configurazione di un gestore di chiavi esterno, eseguire una delle seguenti operazioni iniziali.

| Scopo                                                | Navigazione                      | Fase di avvio                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestore delle chiavi esterne dell'ambito del cluster | <b>Cluster &gt; Impostazioni</b> | Scorrere fino alla sezione <b>sicurezza</b> . In <b>Encryption</b> , selezionare  , Quindi selezionare <b>Edit External Key Manager</b> (Modifica gestore chiavi esterno).                                                                |
| Storage VM Scope External Key Manager                | <b>Storage &gt; Storage VM</b>   | Selezionare la VM di storage. Selezionare la scheda <b>Impostazioni</b> . Nella sezione <b>Encryption</b> sotto <b>Security</b> , selezionare  , Quindi selezionare <b>Edit External Key Manager</b> (Modifica gestore chiavi esterno). |

- I server delle chiavi esistenti sono elencati nella tabella **Server delle chiavi**. È possibile eseguire le seguenti operazioni:
  - Aggiungere un nuovo server chiavi selezionando  **Add**.
  - Eliminare un server delle chiavi selezionando  alla fine della cella della tabella che contiene il nome del server delle chiavi. Anche i server di chiavi secondari associati a quel server di chiavi primario vengono rimossi dalla configurazione.



## Eliminare un gestore di chiavi esterno

Se i volumi non sono crittografati, è possibile eliminare un gestore di chiavi esterno.

### Fasi

- Per eliminare un gestore di chiavi esterno, eseguire una delle seguenti operazioni.

| Scopo | Navigazione | Fase di avvio |
|-------|-------------|---------------|
|-------|-------------|---------------|

|                                                      |                                  |                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestore delle chiavi esterne dell'ambito del cluster | <b>Cluster &gt; Impostazioni</b> | Scorrere fino alla sezione <b>sicurezza</b> . In <b>Encryption</b> , selezionare  , Quindi selezionare <b>Delete External Key Manager</b> (Elimina gestore chiavi esterne).                                                              |
| Storage VM Scope External Key Manager                | <b>Storage &gt; Storage VM</b>   | Selezionare la VM di storage. Selezionare la scheda <b>Impostazioni</b> . Nella sezione <b>Encryption</b> sotto <b>Security</b> , selezionare  , Quindi selezionare <b>Delete External Key Manager</b> (Elimina gestore chiavi esterne). |

## Migrare le chiavi tra i principali manager

Quando su un cluster sono attivati più gestori di chiavi, è necessario migrare le chiavi da un gestore di chiavi a un altro. Questo processo viene completato automaticamente con System Manager.

- Se Onboard Key Manager o un gestore di chiavi esterno è abilitato a livello di cluster e alcuni volumi sono crittografati, Quindi, quando si configura un gestore di chiavi esterno a livello di storage VM, le chiavi devono essere migrate da Onboard Key Manager o da un gestore di chiavi esterno a livello di cluster a un gestore di chiavi esterno a livello di storage VM. Questo processo viene completato automaticamente da System Manager.
- Se i volumi sono stati creati senza crittografia su una VM di storage, non è necessario migrare le chiavi.

## Installare i certificati SSL sul cluster

Il cluster e il server KMIP utilizzano i certificati SSL KMIP per verificare l'identità reciproca e stabilire una connessione SSL. Prima di configurare la connessione SSL con il server KMIP, è necessario installare i certificati SSL del client KMIP per il cluster e il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.

### A proposito di questa attività

In una coppia ha, entrambi i nodi devono utilizzare gli stessi certificati SSL KMIP pubblici e privati. Se si collegano più coppie ha allo stesso server KMIP, tutti i nodi delle coppie ha devono utilizzare gli stessi certificati SSL KMIP pubblici e privati.

### Prima di iniziare

- L'ora deve essere sincronizzata sul server che crea i certificati, sul server KMIP e sul cluster.
- È necessario avere ottenuto il certificato del client KMIP SSL pubblico per il cluster.
- È necessario aver ottenuto la chiave privata associata al certificato del client SSL KMIP per il cluster.
- Il certificato del client SSL KMIP non deve essere protetto da password.
- È necessario aver ottenuto il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.
- In un ambiente MetroCluster, è necessario installare gli stessi certificati SSL KMIP su entrambi i cluster.



È possibile installare i certificati client e server sul server KMIP prima o dopo l'installazione dei certificati sul cluster.

## Fasi

1. Installare i certificati del client KMIP SSL per il cluster:

```
security certificate install -vserver admin_svm_name -type client
```

Viene richiesto di immettere i certificati SSL KMIP pubblici e privati.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Installare il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

### **Abilitare la gestione esterna delle chiavi in ONTAP 9.6 e versioni successive (NVE)**

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. A partire da ONTAP 9.6, è possibile configurare un gestore di chiavi esterno separato per proteggere le chiavi utilizzate da un SVM di dati per accedere ai dati crittografati.

A partire da ONTAP 9.11.1, è possibile aggiungere fino a 3 server chiavi secondari per server chiavi primario per creare un server chiavi in cluster. Per ulteriori informazioni, vedere [Configurare i server di chiavi esterne in cluster](#).

#### **A proposito di questa attività**

È possibile collegare fino a quattro server KMIP a un cluster o a una SVM. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

L'ambito della gestione esterna delle chiavi determina se i server di gestione delle chiavi proteggono tutte le SVM nel cluster o solo le SVM selezionate:

- È possibile utilizzare un *ambito del cluster* per configurare la gestione delle chiavi esterne per tutte le SVM nel cluster. L'amministratore del cluster ha accesso a tutte le chiavi memorizzate sui server.
- A partire da ONTAP 9.6, è possibile utilizzare un *ambito SVM* per configurare la gestione delle chiavi esterne per una SVM di dati nel cluster. Questo è il meglio per gli ambienti multi-tenant in cui ciascun tenant utilizza una SVM (o un insieme di SVM) diversa per la distribuzione dei dati. Solo l'amministratore SVM di un determinato tenant ha accesso alle chiavi del tenant.
- Per gli ambienti multi-tenant, installare una licenza per *MT\_EK\_MGMT* utilizzando il seguente comando:

```
system license add -license-code <MT_EK_MGMT license code>
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

È possibile utilizzare entrambi gli ambiti nello stesso cluster. Se i server di gestione delle chiavi sono stati configurati per una SVM, ONTAP utilizza solo questi server per proteggere le chiavi. In caso contrario, ONTAP protegge le chiavi con i server di gestione delle chiavi configurati per il cluster.

È possibile configurare la gestione delle chiavi integrata nell'ambito del cluster e la gestione delle chiavi esterne nell'ambito SVM. È possibile utilizzare `security key-manager key migrate` Comando per la migrazione delle chiavi dalla gestione delle chiavi integrata nell'ambito del cluster ai key manager esterni

nell'ambito SVM.

### Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- Se si desidera attivare la gestione esterna delle chiavi per un ambiente MetroCluster, MetroCluster deve essere completamente configurato prima di attivare la gestione esterna delle chiavi.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

### Fasi

#### 1. Configurare la connettività del gestore delle chiavi per il cluster:

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- Il `security key-manager external enable` il comando sostituisce `security key-manager setup` comando. Se si esegue il comando al prompt di login del cluster, *admin\_SVM* Per impostazione predefinita, viene impostata la SVM amministrativa del cluster corrente. Per configurare l'ambito del cluster, è necessario essere l'amministratore del cluster. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne.
- In un ambiente MetroCluster, se si sta configurando la gestione esterna delle chiavi per la SVM amministrativa, è necessario ripetere `security key-manager external enable` sul cluster partner.

Il seguente comando abilita la gestione esterna delle chiavi per `cluster1` con tre key server esterni. Il primo server chiavi viene specificato utilizzando il nome host e la porta, il secondo viene specificato utilizzando un indirizzo IP e la porta predefinita, mentre il terzo viene specificato utilizzando un indirizzo IPv6 e una porta:

```
cluster1::> security key-manager external enable -vserver cluster1 -key  
-servers  
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234  
-client-cert AdminVserverClientCert -server-ca-certs  
AdminVserverServerCaCert
```

#### 2. Configurare un gestore delle chiavi e una SVM:

```
security key-manager external enable -vserver SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- Se si esegue il comando al prompt di accesso SVM, SVM Per impostazione predefinita, viene impostata la SVM corrente. Per configurare l'ambito di SVM, è necessario essere un amministratore del cluster o di SVM. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne.
- In un ambiente MetroCluster, se si configura la gestione esterna delle chiavi per una SVM di dati, non è necessario ripetere `security key-manager external enable` sul cluster partner.

Il seguente comando abilita la gestione esterna delle chiavi per `svm1` con un server a chiave singola in ascolto sulla porta predefinita 5696:

```
svm11::> security key-manager external enable -vserver svm1 -key-servers  
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs  
SVM1ServerCaCert
```

3. Ripetere l'ultimo passaggio per eventuali SVM aggiuntive.



È inoltre possibile utilizzare `security key-manager external add-servers` Comando per configurare SVM aggiuntive. Il `security key-manager external add-servers` il comando sostituisce `security key-manager add` comando. Per la sintassi completa dei comandi, vedere la pagina `man`.

4. Verificare che tutti i server KMIP configurati siano connessi:

```
security key-manager external show-status -node node_name
```



Il `security key-manager external show-status` il comando sostituisce `security key-manager show -status` comando. Per la sintassi completa dei comandi, vedere la pagina `man`.

```
cluster1::> security key-manager external show-status
```

| Node  | Vserver  | Key Server                                   | Status    |
|-------|----------|----------------------------------------------|-----------|
| ----- |          |                                              |           |
| ----- |          |                                              |           |
| node1 |          |                                              |           |
|       | svm1     | keyserver.svm1.com:5696                      | available |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |
| node2 |          |                                              |           |
|       | svm1     | keyserver.svm1.com:5696                      | available |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |

```
8 entries were displayed.
```

5. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

```
volume encryption conversion start
```

Prima di convertire i volumi, è necessario configurare completamente un gestore di chiavi esterno. In un ambiente MetroCluster, è necessario configurare un gestore di chiavi esterno su entrambi i siti.

### Abilitare la gestione esterna delle chiavi in ONTAP 9.5 e versioni precedenti

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

#### A proposito di questa attività

ONTAP configura la connettività del server KMIP per tutti i nodi del cluster.

#### Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

#### Fasi

1. Configurare la connettività del gestore delle chiavi per i nodi del cluster:



```
security key-manager setup
```

Viene avviata la configurazione di Key Manager.



In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

2. Immettere la risposta appropriata a ogni richiesta.

3. Aggiunta di un server KMIP:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

4. Aggiungere un server KMIP aggiuntivo per la ridondanza:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

5. Verificare che tutti i server KMIP configurati siano connessi:

```
security key-manager show -status
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager show -status
```

| Node        | Port | Registered Key Manager | Status    |
|-------------|------|------------------------|-----------|
| -----       | ---- | -----                  | -----     |
| cluster1-01 | 5696 | 20.1.1.1               | available |
| cluster1-01 | 5696 | 20.1.1.2               | available |
| cluster1-02 | 5696 | 20.1.1.1               | available |
| cluster1-02 | 5696 | 20.1.1.2               | available |

6. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

```
volume encryption conversion start
```

Prima di convertire i volumi, è necessario configurare completamente un gestore di chiavi esterno. In un ambiente MetroCluster, è necessario configurare un gestore di chiavi esterno su entrambi i siti.

## Gestire le chiavi con un cloud provider

A partire da ONTAP 9.10.1, è possibile utilizzare ["Azure Key Vault \(AKV\)"](#) e ["Servizio di gestione delle chiavi di Google Cloud Platform \(Cloud KMS\)"](#) Per proteggere le chiavi di crittografia ONTAP in un'applicazione ospitata nel cloud. A partire da ONTAP 9.12.0, è anche possibile proteggere le chiavi NVE con ["KMS DI AWS"](#).

AWS KMS, AKV e Cloud KMS possono essere utilizzati per proteggere ["Chiavi NetApp Volume Encryption \(NVE\)"](#) Solo per SVM di dati.

### A proposito di questa attività

La gestione delle chiavi con un provider cloud può essere abilitata con l'interfaccia CLI o l'API REST ONTAP.

Quando si utilizza un cloud provider per proteggere le chiavi, tenere presente che per impostazione predefinita viene utilizzata una LIF SVM dati per comunicare con l'endpoint di gestione delle chiavi cloud. Una rete di gestione dei nodi viene utilizzata per comunicare con i servizi di autenticazione del provider cloud (login.microsoftonline.com per Azure; oauth2.googleapis.com per Cloud KMS). Se la rete del cluster non è configurata correttamente, il cluster non utilizzerà correttamente il servizio di gestione delle chiavi.

Quando si utilizza un servizio di gestione delle chiavi di un provider cloud, è necessario tenere presenti le seguenti limitazioni:

- La gestione delle chiavi con cloud provider non è disponibile per crittografia dello storage NetApp (NSE) e crittografia aggregata di NetApp (NAE). ["KMIP esterni"](#) può essere utilizzato in alternativa.
- La gestione delle chiavi del provider cloud non è disponibile per le configurazioni MetroCluster.
- La gestione delle chiavi del cloud provider può essere configurata solo su una SVM dati.

### Prima di iniziare

- È necessario aver configurato il KMS sul cloud provider appropriato.
- I nodi del cluster ONTAP devono supportare NVE.
- ["È necessario aver installato le licenze Volume Encryption \(VE\) e Encryption Key Management \(MTEKM\) multi-tenant"](#). Queste licenze sono incluse con ["ONTAP uno"](#).
- Devi essere un amministratore del cluster o di SVM.
- I dati SVM non devono includere volumi crittografati né utilizzare un gestore delle chiavi. Se i dati SVM includono volumi crittografati, è necessario eseguirne la migrazione prima di configurare il KMS.

### Abilitare la gestione esterna delle chiavi

L'attivazione della gestione esterna delle chiavi dipende dal gestore specifico delle chiavi utilizzato. Scegliere la scheda del gestore delle chiavi e dell'ambiente appropriati.

## AWS

### Prima di iniziare

- È necessario creare una concessione per la chiave AWS KMS che verrà utilizzata dal ruolo IAM che gestisce la crittografia. Il ruolo IAM deve includere una policy che consenta le seguenti operazioni:
  - DescribeKey
  - Encrypt
  - Decrypt

Per ulteriori informazioni, consultare la documentazione AWS per "[sovvenzioni](#)".

### Abilitare AWS KMS su una SVM ONTAP

1. Prima di iniziare, procurarsi l'ID della chiave di accesso e la chiave segreta da AWS KMS.
2. Impostare il livello di privilegio su Advanced (avanzato):  
`set -priv advanced`
3. Abilitare AWS KMS:  
`security key-manager external aws enable -vserver svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. Quando richiesto, inserire la chiave segreta.
5. Verificare che AWS KMS sia stato configurato correttamente:  
`security key-manager external aws show -vserver svm_name`

## Azure

### Abilitare il vault delle chiavi Azure su una SVM ONTAP

1. Prima di iniziare, è necessario ottenere le credenziali di autenticazione appropriate dall'account Azure, un certificato o un segreto client. È inoltre necessario garantire che tutti i nodi del cluster siano integri. Puoi controllare questo con il comando `cluster show`.
2. Impostare il livello di privilegi su avanzato  
`set -priv advanced`
3. Abilitare AKV su SVM  
``security key-manager external azure enable -client-id client_id -tenant-id tenant_id -name -key-id key_id -authentication-method {certificate|client-secret}`` Quando richiesto, immettere il certificato del client o il segreto del client dall'account Azure.
4. Verificare che AKV sia attivato correttamente:  
`security key-manager external azure show vserver svm_name`  
Se la raggiungibilità del servizio non è corretta, stabilire la connettività con il servizio di gestione delle chiavi AKV tramite data SVM LIF.

## Google Cloud

### Abilitare KMS cloud su una SVM ONTAP

1. Prima di iniziare, ottenere la chiave privata per il file delle chiavi dell'account Google Cloud KMS in formato JSON. Questo è disponibile nel tuo account GCP.  
È inoltre necessario garantire che tutti i nodi del cluster siano integri. Puoi controllare questo con il comando `cluster show`.
2. Impostare il livello di privilegi su avanzato:

```
set -priv advanced
```

### 3. Abilitare Cloud KMS su SVM

```
security key-manager external gcp enable -vserver svm_name -project-id  
project_id-key-ring-name key_ring_name -key-ring-location key_ring_location  
-key-name key_name
```

Quando richiesto, inserire il contenuto del file JSON con la chiave privata dell'account di servizio

### 4. Verificare che Cloud KMS sia configurato con i parametri corretti:

```
security key-manager external gcp show vserver svm_name
```

Lo stato di `kms_wrapped_key_status` lo sarà "UNKNOWN" se non sono stati creati volumi crittografati.

Se la raggiungibilità del servizio non è corretta, stabilire la connettività al servizio di gestione delle chiavi GCP tramite data SVM LIF.

Se uno o più volumi crittografati sono già configurati per un SVM di dati e le chiavi NVE corrispondenti sono gestite dal gestore delle chiavi integrato SVM di amministrazione, tali chiavi devono essere migrate al servizio di gestione delle chiavi esterno. Per eseguire questa operazione con la CLI, eseguire il comando:

```
`security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM`
```

Non è possibile creare nuovi volumi crittografati per i dati SVM del tenant fino a quando tutte le chiavi NVE dei dati SVM non vengono migrate correttamente.

## Informazioni correlate

- ["Crittografia dei volumi con le soluzioni di crittografia NetApp per Cloud Volumes ONTAP"](#)

## Abilitare la gestione delle chiavi integrata in ONTAP 9.6 e versioni successive (NVE)

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

### A proposito di questa attività

È necessario eseguire `security key-manager onboard sync` ogni volta che si aggiunge un nodo al cluster.

Se si dispone di una configurazione MetroCluster, è necessario eseguire `security key-manager onboard enable` eseguire prima il comando sul cluster locale, quindi eseguire `security key-manager onboard sync` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi. Quando si esegue `security key-manager onboard enable` dal cluster locale, quindi eseguire la sincronizzazione sul cluster remoto, non è necessario eseguire `enable` comando di nuovo dal cluster remoto.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. È possibile utilizzare `cc-mode-enabled=yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `cc-mode-enabled=yes`, volumi creati con `volume create` e `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.

Quando si configura la crittografia dei dati ONTAP a riposo, per soddisfare i requisiti per le soluzioni commerciali per classificati (CSFC), è necessario utilizzare NSE con NVE e assicurarsi che il gestore delle chiavi integrato sia attivato in modalità Criteri comuni. Fare riferimento a. ["CSFC Solution Brief"](#) Per ulteriori

Quando Onboard Key Manager è attivato in modalità Common Criteria (Criteri comuni) (`cc-mode-enabled=yes`), il comportamento del sistema viene modificato nei seguenti modi:

- Il sistema monitora i tentativi consecutivi di passphrase del cluster non riusciti quando si opera in modalità Common Criteria.

Se non si riesce a inserire la passphrase del cluster corretta all'avvio, i volumi crittografati non vengono montati. Per risolvere questo problema, riavviare il nodo e inserire la passphrase del cluster corretta. Una volta avviato, il sistema consente fino a 5 tentativi consecutivi di inserire correttamente la passphrase del cluster in un periodo di 24 ore per qualsiasi comando che richieda la passphrase del cluster come parametro. Se il limite viene raggiunto (ad esempio, non è stato possibile inserire correttamente la passphrase del cluster 5 volte di seguito), è necessario attendere che il periodo di timeout di 24 ore sia trascorso oppure riavviare il nodo per ripristinare il limite.

- Gli aggiornamenti delle immagini di sistema utilizzano il certificato di firma del codice NetApp RSA-3072 insieme ai digest con firma del codice SHA-384 per controllare l'integrità dell'immagine invece del certificato di firma del codice NetApp RSA-2048 e dei digest con firma del codice SHA-256.

Il comando `upgrade` verifica che il contenuto dell'immagine non sia stato alterato o corrotto controllando varie firme digitali. Se la convalida ha esito positivo, il processo di aggiornamento dell'immagine passa alla fase successiva; in caso contrario, l'aggiornamento dell'immagine non riesce. Vedere `cluster image` pagina man per informazioni relative agli aggiornamenti del sistema.

Onboard Key Manager memorizza le chiavi nella memoria volatile. I contenuti della memoria volatile vengono cancellati quando il sistema viene riavviato o arrestato. In condizioni operative normali, il contenuto della memoria volatile viene cancellato entro 30 secondi quando il sistema viene arrestato.

## Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

## Fasi

1. Avviare la configurazione di Key Manager:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

Impostare `cc-mode-enabled=yes` per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Per NVE, se si imposta `cc-mode-enabled=yes`, volumi creati con `volume create` e `volume move start` i comandi vengono crittografati automaticamente. Il `- cc-mode-enabled` L'opzione non è supportata nelle configurazioni MetroCluster. Il `security key-manager onboard enable` il comando sostituisce `security key-manager setup` comando.

Nell'esempio seguente viene avviato il comando di configurazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver  
"cluster1"::    <32..256 ASCII characters long text>  
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long  
text>
```

2. Al prompt della passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per “cc-mode”, una passphrase compresa tra 64 e 256 caratteri.



Se la passphrase “cc-mode” specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l'operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della passphrase.

3. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
4. Verificare che le chiavi di autenticazione siano state create:

```
security key-manager key query -key-type NSE-AK
```



Il `security key-manager key query` il comando **sostituisce** `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager key query -key-type NSE-AK
Node: node1
Vserver: cluster1
Key Manager: onboard
Key Manager Type: OKM
Key Manager Policy: -
```

| Key Tag                                                                                         | Key Type | Encryption | Restored |
|-------------------------------------------------------------------------------------------------|----------|------------|----------|
| node1                                                                                           | NSE-AK   | AES-256    | true     |
| Key ID:<br>00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000<br>00000000 |          |            |          |
| node1                                                                                           | NSE-AK   | AES-256    | true     |
| Key ID:<br>00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000<br>00000000 |          |            |          |

2 entries were displayed.

##### 5. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

```
volume encryption conversion start
```

Onboard Key Manager deve essere completamente configurato prima di convertire i volumi. In un ambiente MetroCluster, il gestore delle chiavi integrato deve essere configurato su entrambi i siti.

#### Al termine

Copiare la passphrase in una posizione sicura all'esterno del sistema di storage per utilizzarla in futuro.

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario eseguire il backup manuale delle informazioni in una posizione sicura all'esterno del sistema di storage per l'utilizzo in caso di disastro. Vedere ["Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate"](#).

#### Abilitare la gestione delle chiavi integrata in ONTAP 9.5 e versioni precedenti (NVE)

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

#### A proposito di questa attività

È necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.

Se si dispone di una configurazione MetroCluster, consultare le seguenti linee guida:

- In ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale e `security key-manager setup -sync-metrocluster-config yes` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- Prima di ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale, attendere circa 20 secondi, quindi eseguire `security key-manager setup` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.



Dopo un tentativo di passphrase non riuscito, riavviare nuovamente il nodo.

### Prima di iniziare

- Se si utilizza NSE o NVE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno.

["Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"](#)

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

### Fasi

1. Avviare la configurazione di Key Manager:

```
security key-manager setup -enable-cc-mode yes|no
```



A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e `volume move start` i comandi vengono crittografati automaticamente.

Nell'esempio seguente viene avviata l'impostazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:



• • •

- 



- 



6. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

```
volume encryption conversion start
```

Onboard Key Manager deve essere completamente configurato prima di convertire i volumi. In un ambiente MetroCluster, il gestore delle chiavi integrato deve essere configurato su entrambi i siti.

### Al termine

Copiare la passphrase in una posizione sicura all'esterno del sistema di storage per utilizzarla in futuro.

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario eseguire il backup manuale delle informazioni in una posizione sicura all'esterno del sistema di storage per l'utilizzo in caso di disastro. Vedere ["Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate"](#).

### Abilitare la gestione delle chiavi integrata nei nodi appena aggiunti

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.



Per ONTAP 9.5 e versioni precedenti, è necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.

Per ONTAP 9.6 e versioni successive, è necessario eseguire `security key-manager sync` ogni volta che si aggiunge un nodo al cluster.

Se si aggiunge un nodo a un cluster che ha configurato la gestione delle chiavi integrate, eseguire questo comando per aggiornare le chiavi mancanti.

Se si dispone di una configurazione MetroCluster, consultare le seguenti linee guida:

- A partire da ONTAP 9.6, è necessario eseguire `security key-manager onboard enable` sul cluster locale, quindi eseguire `security key-manager onboard sync` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- In ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale e `security key-manager setup -sync-metrocluster-config yes` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- Prima di ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale, attendere circa 20 secondi, quindi eseguire `security key-manager setup` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.



Dopo un tentativo di passphrase non riuscito, riavviare nuovamente il nodo.

## Crittografare i dati del volume con NVE

### Crittografare i dati del volume con la panoramica di NVE

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita quando si dispone della licenza VE e della gestione delle chiavi integrata o esterna. Per ONTAP 9.6 e versioni precedenti, è possibile attivare la crittografia su un nuovo volume o su un volume esistente. Prima di attivare la crittografia dei volumi, è necessario aver installato la licenza VE e attivato la gestione delle chiavi. NVE è conforme a FIPS-140-2 livello 1.

### Abilitare la crittografia a livello aggregato con la licenza VE

A partire da ONTAP 9,7, gli aggregati e i volumi appena creati sono crittografati per impostazione predefinita, quando si dispone di "[Licenza VE](#)" e gestione della chiave integrata o esterna. A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da crittografare.

#### A proposito di questa attività

Se si intende eseguire la deduplica a livello di aggregato inline o in background, è necessario utilizzare la crittografia a livello di aggregato. La deduplica a livello di aggregato non è altrimenti supportata da NVE.

Un aggregato abilitato per la crittografia a livello di aggregato è denominato *aggregato NAE* (per NetApp aggregate Encryption). Tutti i volumi in un aggregato NAE devono essere crittografati con crittografia NAE o NVE. Con la crittografia a livello di aggregato, i volumi creati nell'aggregato vengono crittografati con la crittografia NAE per impostazione predefinita. È possibile eseguire l'override del valore predefinito per utilizzare la crittografia NVE.

I volumi di testo normale non sono supportati negli aggregati NAE.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

#### Fasi

1. Attivare o disattivare la crittografia a livello di aggregato:

| Per...                                                      | Utilizzare questo comando...                                                                                 |
|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Creare un aggregato NAE con ONTAP 9.7 o versione successiva | <code>storage aggregate create -aggregate aggregate_name -node node_name</code>                              |
| Crea un aggregato NAE con ONTAP 9.6                         | <code>storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code> |
| Convertire un aggregato non NAE in un aggregato NAE         | <code>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code> |

Convertire un aggregato NAE in un aggregato non NAE

```
storage aggregate modify -aggregate  
aggregate_name -node node_name -encrypt-with  
-aggr-key false
```

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando attiva la crittografia a livello di aggregato `aggr1`:

- ONTAP 9.7 o versione successiva:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 o versioni precedenti:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with  
-aggr-key true
```

## 2. Verificare che l'aggregato sia abilitato per la crittografia:

```
storage aggregate show -fields encrypt-with-aggr-key
```

Per la sintassi completa dei comandi, vedere la pagina man.

Il seguente comando verifica `aggr1` è abilitato per la crittografia:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key  
aggregate          encrypt-aggr-key  
-----  
aggr0_vsim4        false  
aggr1               true  
2 entries were displayed.
```

### Al termine

Eseguire `volume create` per creare i volumi crittografati.

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP “invia automaticamente” una chiave di crittografia al server quando si crittografa un volume.

### Attivare la crittografia su un nuovo volume

È possibile utilizzare `volume create` per attivare la crittografia su un nuovo volume.

### A proposito di questa attività

È possibile crittografare i volumi utilizzando NetApp Volume Encryption (NVE) e, a partire da ONTAP 9.6, NetApp aggregate Encryption (NAE). Per ulteriori informazioni su NAE e NVE, fare riferimento a [panoramica](#)

La procedura per attivare la crittografia su un nuovo volume in ONTAP varia in base alla versione di ONTAP in uso e alla configurazione specifica:


- A partire da ONTAP 9.4, se si attiva `cc-mode` Quando si configura Onboard Key Manager, i volumi creati con `volume create` i comandi vengono crittografati automaticamente, indipendentemente dal fatto che l'utente lo specifichi o meno `-encrypt true`.
- In ONTAP 9.6 e versioni precedenti, è necessario utilizzare `-encrypt true` con `volume create` comandi per attivare la crittografia (a condizione che non sia stata attivata) `cc-mode`).
- Se si desidera creare un volume NAE in ONTAP 9.6, è necessario attivare NAE a livello di aggregato. Fare riferimento a [Abilitare la crittografia a livello di aggregato con la licenza VE](#) per ulteriori dettagli su questa attività.
- A partire da ONTAP 9.7, i volumi appena creati vengono crittografati per impostazione predefinita quando si dispone di "Licenza VE" e gestione della chiave integrata o esterna. Per impostazione predefinita, i nuovi volumi creati in un aggregato NAE saranno di tipo NAE anziché NVE.
  - In ONTAP 9.7 e versioni successive, se si aggiunge `-encrypt true` al `volume create` Comando per creare un volume in un aggregato NAE, il volume avrà la crittografia NVE invece di NAE. Tutti i volumi in un aggregato NAE devono essere crittografati con NVE o NAE.



I volumi non in testo normale non sono supportati negli aggregati NAE.

Fasi

1. Creare un nuovo volume e specificare se la crittografia è attivata sul volume. Se il nuovo volume si trova in un aggregato NAE, per impostazione predefinita il volume sarà un volume NAE:

| Per creare...              | Utilizzare questo comando...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Un volume NAE              | <code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Un volume NVE              | <div><div><code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true +</code></div><div><p>In ONTAP 9.6 e versioni precedenti, dove non è supportato il servizio NAE, <code>-encrypt true</code> Specifica che il volume deve essere crittografato con NVE. In ONTAP 9.7 e versioni successive, dove i volumi vengono creati in aggregati NAE, <code>-encrypt true</code> Esegue l'override del tipo di crittografia predefinito di NAE per creare un volume NVE.</p></div></div> |
| Un volume di testo normale | <code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false</code>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Per la sintassi completa dei comandi, fare riferimento alla pagina di riferimento dei comandi per `volume create`.

2. Verificare che i volumi siano abilitati per la crittografia:

```
volume show -is-encrypted true
```

Per la sintassi completa dei comandi, vedere ["riferimento al comando"](#).

## Risultato

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP "invia" automaticamente una chiave di crittografia al server quando si crittografa un volume.

```
=  
:allow-uri-read:
```

## Attivare la crittografia su un volume esistente

È possibile utilizzare il `volume move start` o il `volume encryption conversion start` per abilitare la crittografia su un volume esistente.

### A proposito di questa attività

- A partire da ONTAP 9.3, è possibile utilizzare `volume encryption conversion start` comando per abilitare la crittografia di un volume esistente "sul posto", senza dover spostare il volume in una posizione diversa. In alternativa, è possibile utilizzare `volume move start` comando.
- Per ONTAP 9,2 e versioni precedenti, è possibile utilizzare solo `volume move start` per attivare la crittografia spostando un volume esistente.

## Attivare la crittografia su un volume esistente con il comando di avvio della conversione della crittografia del volume

A partire da ONTAP 9.3, è possibile utilizzare `volume encryption conversion start` comando per abilitare la crittografia di un volume esistente "sul posto", senza dover spostare il volume in una posizione diversa.

Dopo aver avviato un'operazione di conversione, è necessario completarla. Se si verificano problemi di prestazioni durante l'operazione, è possibile eseguire `volume encryption conversion pause` per sospendere l'operazione e il `volume encryption conversion resume` per riprendere l'operazione.



Non è possibile utilizzare `volume encryption conversion start` Per convertire un volume SnapLock.

## Fasi

1. Abilitare la crittografia su un volume esistente:

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

Il seguente comando consente la crittografia sul volume esistente `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

Il sistema crea una chiave di crittografia per il volume. I dati del volume vengono crittografati.

## 2. Verificare lo stato dell'operazione di conversione:

```
volume encryption conversion show
```

Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

Il seguente comando visualizza lo stato dell'operazione di conversione:

```
cluster1::> volume encryption conversion show
```

| Vserver | Volume | Start Time         | Status                       |
|---------|--------|--------------------|------------------------------|
| -----   | -----  | -----              | -----                        |
| vs1     | vol1   | 9/18/2017 17:51:41 | Phase 2 of 2 is in progress. |

## 3. Una volta completata l'operazione di conversione, verificare che il volume sia abilitato per la crittografia:

```
volume show -is-encrypted true
```

Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

Il seguente comando visualizza i volumi crittografati su cluster1:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

### Risultato

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP "invia automaticamente" una chiave di crittografia al server quando si crittografa un volume.

### Attivare la crittografia su un volume esistente con il comando di avvio spostamento volume

È possibile utilizzare `volume move start` per attivare la crittografia spostando un volume esistente. È necessario utilizzare `volume move start` in ONTAP 9.2 e versioni precedenti. È possibile utilizzare lo stesso aggregato o un aggregato diverso.

### A proposito di questa attività

- A partire da ONTAP 9.8, è possibile utilizzare `volume move start` Per attivare la crittografia su un volume SnapLock o FlexGroup.
- A partire da ONTAP 9.4, se si attiva "cc-mode" quando si imposta il Gestore chiavi integrato, i volumi creati con `volume move start` i comandi vengono crittografati automaticamente. Non è necessario specificare `-encrypt-destination true`.
- A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da spostare. Un volume crittografato con una chiave univoca è chiamato *volume NVE* (ovvero utilizza la crittografia del volume NetApp). Un volume crittografato con una

chiave a livello di aggregato viene chiamato *volume NAE* (per NetApp aggregate Encryption). I volumi non in testo normale non sono supportati negli aggregati NAE.

- A partire da ONTAP 9.14.1, puoi crittografare un volume root di una SVM con NVE. Per ulteriori informazioni, vedere [Configurare la crittografia dei volumi NetApp su un volume root della SVM](#).

## Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o un amministratore SVM al quale l'amministratore del cluster ha delegato l'autorità.

"Delega dell'autorizzazione all'esecuzione del comando di spostamento del volume"

## Fasi

1. Spostare un volume esistente e specificare se la crittografia è attivata sul volume:

| Per convertire...                                                                                                                  | Utilizzare questo comando...                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Un volume non crittografato su un volume NVE                                                                                       | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true</code>                               |
| Un volume NVE o plaintext su un volume NAE (supponendo che la crittografia a livello di aggregato sia attivata sulla destinazione) | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true</code>                             |
| Un volume NAE su un volume NVE                                                                                                     | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false</code>                            |
| Un volume NAE su un volume non crittografato                                                                                       | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false</code> |
| Un volume NVE su un volume non crittografato                                                                                       | <code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false</code>                              |

Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

Il seguente comando converte un volume non crittografato denominato `vol1` Su un volume NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Supponendo che la crittografia a livello di aggregato sia attivata sulla destinazione, il seguente comando converte un volume NVE o non crittografato denominato `vol1` Su un volume NAE:



```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggregate aggr2 -encrypt-with-aggr-key true
```

Il seguente comando converte un volume NAE denominato `vol2` Su un volume NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination  
-aggregate aggr2 -encrypt-with-aggr-key false
```

Il seguente comando converte un volume NAE denominato `vol2` su un volume non crittografato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination  
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

Il seguente comando converte un volume NVE denominato `vol2` su un volume non crittografato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination  
-aggregate aggr2 -encrypt-destination false
```

## 2. Visualizzare il tipo di crittografia dei volumi del cluster:

```
volume show -fields encryption-type none|volume|aggregate
```

Il `encryption-type` Field è disponibile in ONTAP 9.6 e versioni successive.

Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

Il seguente comando visualizza il tipo di crittografia dei volumi in `cluster2`:

```
cluster2::> volume show -fields encryption-type
```

| vserver | volume | encryption-type |
|---------|--------|-----------------|
| -----   | -----  | -----           |
| vs1     | vol1   | none            |
| vs2     | vol2   | volume          |
| vs3     | vol3   | aggregate       |

## 3. Verificare che i volumi siano abilitati per la crittografia:

```
volume show -is-encrypted true
```

Per l'intera sintassi dei comandi, vedere la pagina man relativa al comando.

Il seguente comando visualizza i volumi crittografati su `cluster2`:

```
cluster2::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

## Risultato

Se si utilizza un server KMIP per memorizzare le chiavi di crittografia di un nodo, ONTAP invia automaticamente una chiave di crittografia al server quando si crittografa un volume.

## Configurare la crittografia dei volumi NetApp su un volume root della SVM

A partire da ONTAP 9.14.1, puoi abilitare NetApp Volume Encryption (NVE) su un volume root di una Storage VM (SVM). Con NVE, il volume root è crittografato con una chiave univoca, abilitando una maggiore sicurezza sulla SVM.

### A proposito di questa attività

NVE su un volume root di SVM può essere abilitato solo dopo che è stata creata la SVM.

### Prima di iniziare

- Il volume root della SVM non deve trovarsi in un aggregato crittografato con crittografia degli aggregati NetApp (NAE).
- È necessario aver abilitato la crittografia con Onboard Key Manager o con un gestore di chiavi esterno.
- È necessario eseguire ONTAP 9.14.1 o versione successiva.
- Per migrare una SVM contenente un volume root crittografato con NVE, al termine della migrazione è necessario convertire il volume root della SVM in un volume di testo normale, quindi crittografare di nuovo il volume root della SVM.
  - Se l'aggregato di destinazione della migrazione SVM utilizza NAE, il volume root eredita NAE per impostazione predefinita.
- Se la SVM si trova in una relazione di disaster recovery della SVM:
  - Le impostazioni di crittografia su una SVM con mirroring non vengono copiate nella destinazione. Se abiliti NVE sull'origine o sulla destinazione, devi abilitare NVE separatamente sul volume root della SVM con mirroring.
  - Se tutti gli aggregati nel cluster di destinazione utilizzano NAE, il volume root della SVM utilizzerà NAE.

## Fasi

Puoi abilitare NVE su un volume root di SVM con l'interfaccia a riga di comando di ONTAP o System Manager.

## CLI

È possibile abilitare NVE sul volume root della SVM in-place o spostando il volume tra aggregati.

### Crittografare il volume root in uso

1. Convertire il volume root in un volume crittografato:

```
volume encryption conversion start -vserver svm_name -volume volume
```

2. Conferma crittografia riuscita. Il `volume show -encryption-type volume` Visualizza un elenco di tutti i volumi che utilizzano NVE.

### Crittografa il volume root della SVM spostandolo


1. Avvio dello spostamento di un volume:

```
volume move start -vserver svm_name -volume volume -destination-aggregate  
aggregato -encrypt-with-aggr-key false -encrypt-destination true
```

Per ulteriori informazioni su `volume move`, vedere [Spostare un volume](#).

2. Confermare `volume move` operazione riuscita con il `volume move show` comando. Il `volume show -encryption-type volume` Visualizza un elenco di tutti i volumi che utilizzano NVE.

## System Manager

1. Passare a **archiviazione > volumi**.
2. Selezionare, accanto al nome del volume root della SVM che si desidera crittografare  Poi **Modifica**.
3. Sotto l'intestazione **archiviazione e ottimizzazione**, selezionare **Abilita crittografia**.
4. Selezionare **Salva**.

### Abilitare la crittografia del volume root del nodo

A partire da ONTAP 9.8, è possibile utilizzare la crittografia dei volumi NetApp per proteggere il volume root del nodo.



#### A proposito di questa attività

Questa procedura si applica al volume root del nodo. Non si applica ai volumi root SVM. I volumi root delle SVM possono essere protetti tramite crittografia a livello di aggregato e [A partire da ONTAP 9.14.1, NVE](#).

Una volta avviata, la crittografia del volume root deve essere completata. Non è possibile sospendere l'operazione. Una volta completata la crittografia, non è possibile assegnare una nuova chiave al volume root e non è possibile eseguire un'operazione di eliminazione sicura.

### Prima di iniziare

- Il sistema deve utilizzare una configurazione ha.
- Il volume root del nodo deve essere già creato.
- Il sistema deve disporre di un gestore delle chiavi integrato o di un server di gestione delle chiavi esterno che utilizzi il protocollo KMIP (Key Management Interoperability Protocol).

## Fasi

1. Crittografare il volume root:

```
volume encryption conversion start -vserver SVM_name -volume root_vol_name
```

2. Verificare lo stato dell'operazione di conversione:

```
volume encryption conversion show
```

3. Una volta completata l'operazione di conversione, verificare che il volume sia crittografato:

```
volume show -fields
```

Di seguito viene riportato un esempio di output per un volume crittografato.

```
::> volume show -vserver xyz -volume vol0 -fields is-encrypted
vserver      volume is-encrypted
-----
xyz          vol0      true
```

## Configurare la crittografia basata su hardware NetApp

### Configurazione della panoramica della crittografia basata su hardware NetApp

La crittografia basata su hardware di NetApp supporta la crittografia completa dei dischi (FDE) dei dati così come vengono scritti. I dati non possono essere letti senza una chiave di crittografia memorizzata nel firmware. La chiave di crittografia, a sua volta, è accessibile solo a un nodo autenticato.

### Comprendere la crittografia basata su hardware NetApp

Un nodo esegue l'autenticazione su un'unità con crittografia automatica utilizzando una chiave di autenticazione recuperata da un server di gestione delle chiavi esterno o da Onboard Key Manager:

- Il server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol). Si consiglia di configurare i server di gestione delle chiavi esterni su un sistema storage diverso dai dati.
- Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati.

È possibile utilizzare NetApp Volume Encryption con crittografia basata su hardware per "eseguire la doppia crittografia `d`" dei dati su dischi con crittografia automatica.

Quando i dischi con crittografia automatica sono abilitati, anche il core dump è crittografato.



Se una coppia ha utilizzato dischi SAS o NVMe con crittografia (SED, NSE, FIPS), seguire le istruzioni riportate nell'argomento [Ripristino di un'unità FIPS o SED in modalità non protetta](#). Per tutti i dischi all'interno della coppia ha prima dell'inizializzazione del sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

### Tipi di dischi con crittografia automatica supportati

Sono supportati due tipi di dischi con crittografia automatica:

- I dischi SAS o NVMe con crittografia automatica certificati FIPS sono supportati su tutti i sistemi FAS e AFF. Questi dischi, denominati *dischi FIPS*, sono conformi ai requisiti della pubblicazione Federal Information Processing Standard 140-2, livello 2. Le funzionalità certificate consentono di proteggere oltre alla crittografia, ad esempio prevenendo attacchi di tipo Denial-of-service sul disco. I dischi FIPS non possono essere combinati con altri tipi di dischi sullo stesso nodo o coppia ha.
- A partire da ONTAP 9.6, i dischi NVMe con crittografia automatica che non hanno superato i test FIPS sono supportati sui sistemi AFF A800, A320 e successivi. Questi dischi, denominati *SED*, offrono le stesse funzionalità di crittografia dei dischi FIPS, ma possono essere combinati con dischi non crittografanti sullo stesso nodo o coppia ha.
- Tutti i dischi convalidati FIPS utilizzano un modulo di crittografia del firmware che è stato eseguito attraverso la convalida FIPS. Il modulo crittografico del disco FIPS non utilizza chiavi generate al di fuori del disco (la passphrase di autenticazione immessa nel disco viene utilizzata dal modulo crittografico del firmware del disco per ottenere una chiave di crittografia).



Le unità non crittografate sono unità che non sono unità SED o FIPS.



Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSE non crittografa i dati che risiedono nel modulo Flash cache.

### Quando utilizzare la gestione esterna delle chiavi

Sebbene sia meno costoso e generalmente più conveniente utilizzare il gestore delle chiavi integrato, è consigliabile utilizzare la gestione esterna delle chiavi se si verifica una delle seguenti condizioni:

- La policy aziendale richiede una soluzione di gestione delle chiavi che utilizzi un modulo crittografico FIPS 140-2 livello 2 (o superiore).
- Hai bisogno di una soluzione multi-cluster, con gestione centralizzata delle chiavi di crittografia.
- La tua azienda richiede una maggiore sicurezza nell'archiviazione delle chiavi di autenticazione su un sistema o in una posizione diversa dai dati.

### Dettagli del supporto

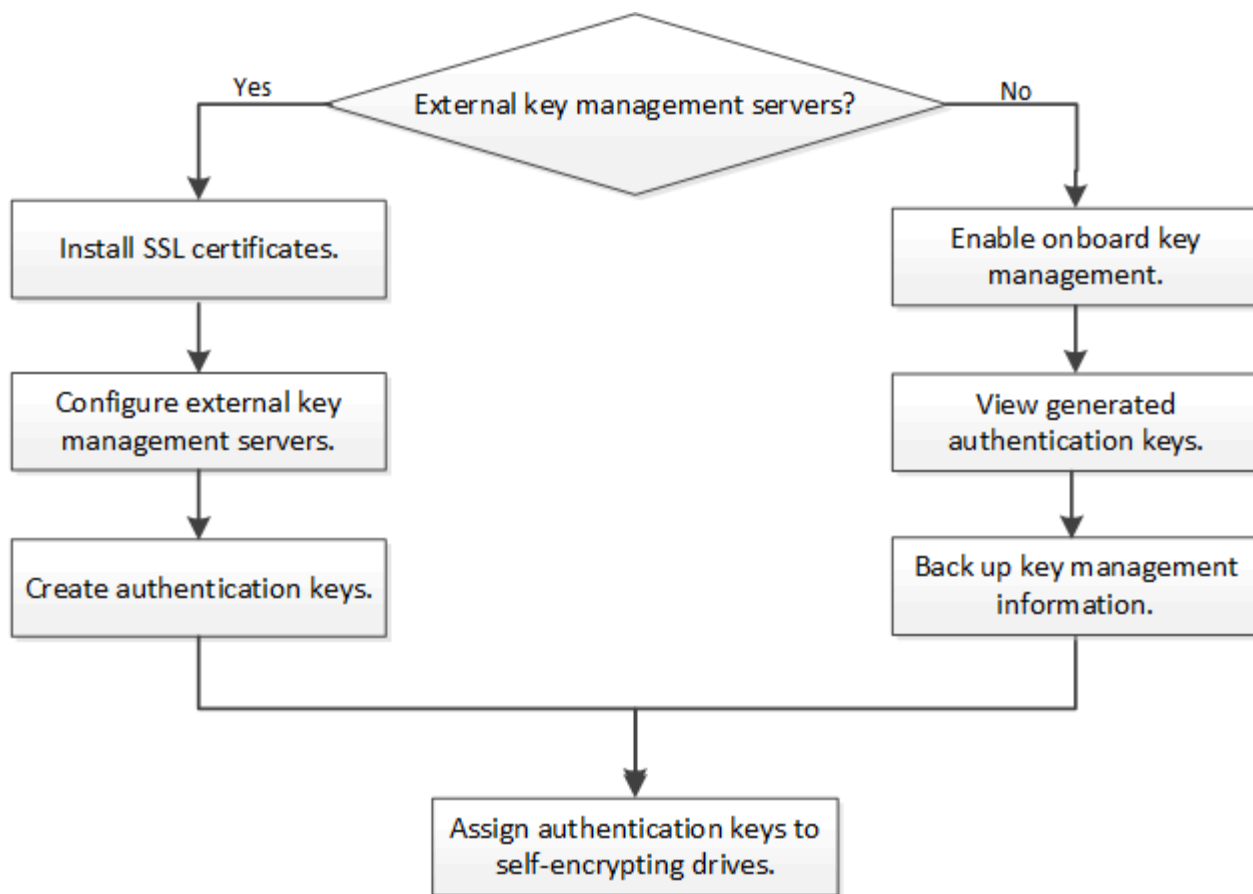
La seguente tabella mostra importanti dettagli sul supporto della crittografia hardware. Consulta la matrice di interoperabilità per le informazioni più recenti su server KMIP, sistemi storage e shelf di dischi supportati.

| Risorsa o funzione | Dettagli del supporto |
|--------------------|-----------------------|
|--------------------|-----------------------|

|                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Set di dischi non omogenei                                        | <ul style="list-style-type: none"> <li>• I dischi FIPS non possono essere combinati con altri tipi di dischi sullo stesso nodo o coppia ha. Le coppie ha conformi possono coesistere con coppie ha non conformi nello stesso cluster.</li> <li>• È possibile combinare i dischi con dischi non crittografanti sullo stesso nodo o coppia ha.</li> </ul>                                                                                                           |
| Tipo di disco                                                     | <ul style="list-style-type: none"> <li>• I dischi FIPS possono essere SAS o NVMe.</li> <li>• I dischi Sed devono essere NVMe.</li> </ul>                                                                                                                                                                                                                                                                                                                          |
| Interfacce di rete da 10 GB                                       | A partire da ONTAP 9.3, le configurazioni di gestione delle chiavi KMIP supportano interfacce di rete da 10 GB per le comunicazioni con server di gestione delle chiavi esterni.                                                                                                                                                                                                                                                                                  |
| Porte per la comunicazione con il server di gestione delle chiavi | A partire da ONTAP 9.3, è possibile utilizzare qualsiasi porta del controller di storage per la comunicazione con il server di gestione delle chiavi. In caso contrario, utilizzare la porta e0M per la comunicazione con i server di gestione delle chiavi. A seconda del modello di controller di storage, alcune interfacce di rete potrebbero non essere disponibili durante il processo di avvio per la comunicazione con i server di gestione delle chiavi. |
| MetroCluster (MCC)                                                | <ul style="list-style-type: none"> <li>• I dischi NVMe supportano MCC.</li> <li>• I dischi SAS non supportano MCC.</li> </ul>                                                                                                                                                                                                                                                                                                                                     |

#### **Workflow di crittografia basato su hardware**

È necessario configurare i servizi di gestione delle chiavi prima che il cluster possa autenticarsi sull'unità con crittografia automatica. È possibile utilizzare un server di gestione delle chiavi esterno o un gestore delle chiavi integrato.



#### Informazioni correlate

- ["NetApp Hardware Universe"](#)
- ["NetApp Volume Encryption e NetApp aggregate Encryption"](#)

### Configurare la gestione esterna delle chiavi

#### Configurare una panoramica sulla gestione esterna delle chiavi

È possibile utilizzare uno o più server di gestione delle chiavi esterni per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. Un server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

Per ONTAP 9.1 e versioni precedenti, è necessario assegnare le LIF di gestione dei nodi alle porte configurate con il ruolo di gestione dei nodi prima di poter utilizzare il gestore delle chiavi esterno.

La crittografia dei volumi NetApp (NVE) può essere implementata con Onboard Key Manager in ONTAP 9.1 e versioni successive. In ONTAP 9.3 e versioni successive, NVE può essere implementato con gestione delle chiavi esterna (KMIP) e Gestione delle chiavi integrata. A partire da ONTAP 9.11.1, è possibile configurare più Key Manager esterni in un cluster. Vedere [Configurare i server delle chiavi in cluster](#).

#### Raccogliere le informazioni di rete in ONTAP 9.2 e versioni precedenti

Se si utilizza ONTAP 9.2 o versioni precedenti, compilare il foglio di lavoro per la configurazione di rete prima di attivare la gestione esterna delle chiavi.



A partire da ONTAP 9.3, il sistema rileva automaticamente tutte le informazioni di rete necessarie.

| Elemento                                                                  | Note                                                                                                                                                                                                                                                                                     | Valore |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Nome dell'interfaccia di rete per la gestione delle chiavi                |                                                                                                                                                                                                                                                                                          |        |
| Indirizzo IP dell'interfaccia di rete per la gestione delle chiavi        | Indirizzo IP della LIF di gestione dei nodi, in formato IPv4 o IPv6                                                                                                                                                                                                                      |        |
| Gestione delle chiavi interfaccia di rete IPv6 lunghezza prefisso di rete | Se si utilizza IPv6, la lunghezza del prefisso di rete IPv6                                                                                                                                                                                                                              |        |
| Subnet mask dell'interfaccia di rete per la gestione delle chiavi         |                                                                                                                                                                                                                                                                                          |        |
| Gestione delle chiavi Indirizzo IP del gateway dell'interfaccia di rete   |                                                                                                                                                                                                                                                                                          |        |
| Indirizzo IPv6 per l'interfaccia di rete del cluster                      | Obbligatorio solo se si utilizza IPv6 per l'interfaccia di rete per la gestione delle chiavi                                                                                                                                                                                             |        |
| Numero di porta per ciascun server KMIP                                   | Opzionale. Il numero di porta deve essere lo stesso per tutti i server KMIP. Se non si specifica un numero di porta, per impostazione predefinita viene impostata la porta 5696, che corrisponde alla porta assegnata dall'autorità IANA (Internet Assigned Numbers Authority) per KMIP. |        |
| Nome tag chiave                                                           | Opzionale. Il nome del tag della chiave viene utilizzato per identificare tutte le chiavi appartenenti a un nodo. Il nome predefinito del tag della chiave è il nome del nodo.                                                                                                           |        |

#### Informazioni correlate

["Report tecnico di NetApp 3954: Requisiti e procedure di preinstallazione di NetApp Storage Encryption per IBM Tivoli Lifetime Key Manager"](#)

["Report tecnico di NetApp 4074: Requisiti e procedure di preinstallazione di NetApp Storage Encryption per SafeNet KeySecure"](#)

#### Installare i certificati SSL sul cluster

Il cluster e il server KMIP utilizzano i certificati SSL KMIP per verificare l'identità reciproca e stabilire una connessione SSL. Prima di configurare la connessione SSL con il server



KMIP, è necessario installare i certificati SSL del client KMIP per il cluster e il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.

### A proposito di questa attività

In una coppia ha, entrambi i nodi devono utilizzare gli stessi certificati SSL KMIP pubblici e privati. Se si collegano più coppie ha allo stesso server KMIP, tutti i nodi delle coppie ha devono utilizzare gli stessi certificati SSL KMIP pubblici e privati.

### Prima di iniziare

- L'ora deve essere sincronizzata sul server che crea i certificati, sul server KMIP e sul cluster.
- È necessario avere ottenuto il certificato del client KMIP SSL pubblico per il cluster.
- È necessario aver ottenuto la chiave privata associata al certificato del client SSL KMIP per il cluster.
- Il certificato del client SSL KMIP non deve essere protetto da password.
- È necessario aver ottenuto il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP.
- In un ambiente MetroCluster, è necessario installare gli stessi certificati SSL KMIP su entrambi i cluster.



È possibile installare i certificati client e server sul server KMIP prima o dopo l'installazione dei certificati sul cluster.

### Fasi

1. Installare i certificati del client KMIP SSL per il cluster:

```
security certificate install -vserver admin_svm_name -type client
```

Viene richiesto di immettere i certificati SSL KMIP pubblici e privati.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Installare il certificato pubblico SSL per l'autorità di certificazione principale (CA) del server KMIP:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

### Gestione esterna delle chiavi in ONTAP 9.6 e versioni successive (basato su hardware)

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

A partire da ONTAP 9.11.1, è possibile aggiungere fino a 3 server di chiavi secondari per ogni server di chiavi primario per creare un server di chiavi in cluster. Per ulteriori informazioni, vedere [Configurare i server di chiavi esterne in cluster](#).

### Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

## Fasi

### 1. Configurare la connettività del gestore delle chiavi per il cluster:

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



- Il `security key-manager external enable` il comando sostituisce `security key-manager setup` comando. È possibile eseguire `security key-manager external modify` comando per modificare la configurazione di gestione delle chiavi esterne. Per la sintassi completa dei comandi, vedere le pagine man.
- In un ambiente MetroCluster, se si sta configurando la gestione esterna delle chiavi per la SVM amministrativa, è necessario ripetere `security key-manager external enable` sul cluster partner.

Il seguente comando abilita la gestione esterna delle chiavi per `cluster1` con tre key server esterni. Il primo server chiavi viene specificato utilizzando il nome host e la porta, il secondo viene specificato utilizzando un indirizzo IP e la porta predefinita, mentre il terzo viene specificato utilizzando un indirizzo IPv6 e una porta:

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

### 2. Verificare che tutti i server KMIP configurati siano connessi:

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```



- Il `security key-manager external show-status` il comando sostituisce `security key-manager show -status` comando. Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager external show-status
```

| Node  | Vserver  | Key Server                                   | Status    |
|-------|----------|----------------------------------------------|-----------|
| ----- |          |                                              |           |
| node1 |          |                                              |           |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |
| node2 |          |                                              |           |
|       | cluster1 | 10.0.0.10:5696                               | available |
|       |          | fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 | available |
|       |          | ks1.local:15696                              | available |

6 entries were displayed.

#### Abilitare la gestione esterna delle chiavi in ONTAP 9.5 e versioni precedenti

È possibile utilizzare uno o più server KMIP per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È possibile collegare fino a quattro server KMIP a un nodo. Si consiglia di utilizzare almeno due server per la ridondanza e il disaster recovery.

#### A proposito di questa attività

ONTAP configura la connettività del server KMIP per tutti i nodi del cluster.

#### Prima di iniziare

- I certificati del server e del client SSL KMIP devono essere stati installati.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare un gestore di chiavi esterno.
- In un ambiente MetroCluster, è necessario installare il certificato SSL KMIP su entrambi i cluster.

#### Fasi

1. Configurare la connettività del gestore delle chiavi per i nodi del cluster:

```
security key-manager setup
```

Viene avviata la configurazione di Key Manager.



In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

2. Immettere la risposta appropriata a ogni richiesta.
3. Aggiunta di un server KMIP:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

4. Aggiungere un server KMIP aggiuntivo per la ridondanza:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



In un ambiente MetroCluster, è necessario eseguire questo comando su entrambi i cluster.

5. Verificare che tutti i server KMIP configurati siano connessi:

```
security key-manager show -status
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security key-manager show -status
```

| Node        | Port | Registered Key Manager | Status    |
|-------------|------|------------------------|-----------|
| -----       | ---- | -----                  | -----     |
| cluster1-01 | 5696 | 20.1.1.1               | available |
| cluster1-01 | 5696 | 20.1.1.2               | available |
| cluster1-02 | 5696 | 20.1.1.1               | available |
| cluster1-02 | 5696 | 20.1.1.2               | available |

6. Facoltativamente, convertire volumi di testo normale in volumi crittografati.

```
volume encryption conversion start
```

Prima di convertire i volumi, è necessario configurare completamente un gestore di chiavi esterno. In un ambiente MetroCluster, è necessario configurare un gestore di chiavi esterno su entrambi i siti.

### Configurare i server di chiavi esterne in cluster

A partire da ONTAP 9.11.1, è possibile configurare la connettività ai server di gestione delle chiavi esterni in cluster su una SVM. Con i key server in cluster, è possibile designare i key server primari e secondari su una SVM. Durante la registrazione delle chiavi, ONTAP tenta innanzitutto di accedere a un server principale prima di tentare di accedere in sequenza ai server secondari fino al completamento dell'operazione, evitando la duplicazione delle chiavi.

I Key server esterni possono essere utilizzati per le chiavi NSE, NVE, NAE e SED. Una SVM può supportare fino a quattro server KMIP esterni primari. Ciascun server primario può supportare fino a tre server secondari

per le chiavi.

## Prima di iniziare

- ["La gestione delle chiavi di KMIP deve essere abilitata per la SVM"](#).
- Questo processo supporta solo i server chiave che utilizzano KMIP. Per un elenco dei server delle chiavi supportati, consultare ["Tool di matrice di interoperabilità NetApp"](#).
- Tutti i nodi del cluster devono eseguire ONTAP 9.11.1 o versione successiva.
- L'ordine dei server elenca gli argomenti in `-secondary-key-servers`. Il parametro riflette l'ordine di accesso dei server KMIP (gestione delle chiavi esterne).

## Creare un server di chiavi in cluster

La procedura di configurazione dipende dal fatto che sia stato configurato o meno un server di chiavi primario.

### Aggiunta di server di chiavi primari e secondari a una SVM

1. Verificare che non sia stata attivata alcuna gestione delle chiavi per il cluster:  
`security key-manager external show -vserver svm_name`  
Se SVM ha già attivato un massimo di quattro server principali, è necessario rimuovere uno dei server principali esistenti prima di aggiungerne uno nuovo.
2. Attivare il gestore delle chiavi primario:  
`security key-manager external enable -vserver svm_name -key-servers  
server_ip -client-cert client_cert_name -server-ca-certs  
server_ca_cert_names`
3. Modificare il server delle chiavi primario per aggiungere i server delle chiavi secondari. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole di un massimo di tre server chiave.  
`security key-manager external modify-server -vserver svm_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers`

### Aggiungere i server di chiavi secondari a un server di chiavi primario esistente

1. Modificare il server delle chiavi primario per aggiungere i server delle chiavi secondari. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole di un massimo di tre server chiave.  
`security key-manager external modify-server -vserver svm_name -key-servers  
primary_key_server -secondary-key-servers list_of_key_servers`  
Per ulteriori informazioni sui server di chiavi secondari, vedere [\[mod-secondary\]](#).

## Modificare i server delle chiavi in cluster

È possibile modificare i cluster di Key Server esterni modificando lo stato (primario o secondario) di determinati Key Server, aggiungendo e rimuovendo i Key Server secondari o modificando l'ordine di accesso dei Key Server secondari.

## Convertire i server chiavi primari e secondari

Per convertire un server di chiavi primario in un server di chiavi secondario, è necessario prima rimuoverlo dalla SVM con `security key-manager external remove-servers` comando.

Per convertire un server chiavi secondario in un server chiavi primario, è necessario prima rimuovere il server chiavi secondario dal server chiavi primario esistente. Vedere [\[mod-secondary\]](#). Se si converte un server chiavi secondario in un server primario durante la rimozione di una chiave esistente, il tentativo di aggiungere un nuovo server prima di completare la rimozione e la conversione può comportare la duplicazione delle chiavi.

## Modificare i server chiavi secondari

I server di chiavi secondari vengono gestiti con `-secondary-key-servers` del parametro `security key-manager external modify-server` comando. Il `-secondary-key-servers` parameter accetta un elenco separato da virgole. L'ordine specificato dei server di chiavi secondari nell'elenco determina la sequenza di accesso per i server di chiavi secondari. L'ordine di accesso può essere modificato eseguendo il comando `security key-manager external modify-server` con i server di chiavi secondari inseriti in una sequenza diversa.

Per rimuovere un server di chiavi secondario, la `-secondary-key-servers` gli argomenti devono includere i server chiave che si desidera conservare mentre si omette quello da rimuovere. Per rimuovere tutti i server di chiavi secondari, utilizzare l'argomento `-`, non significa nessuno.

Per ulteriori informazioni, fare riferimento a `security key-manager external` nella ["Riferimento al comando ONTAP"](#).

## Creare chiavi di autenticazione in ONTAP 9.6 e versioni successive

È possibile utilizzare `security key-manager key create` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

### A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando Onboard Key Manager è attivato. Tuttavia, quando Onboard Key Manager è attivato, vengono create automaticamente due chiavi di autenticazione. I tasti possono essere visualizzati con il seguente comando:

```
security key-manager key query -key-type NSE-AK
```

- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.
- È possibile utilizzare `security key-manager key delete` per eliminare le chiavi inutilizzate. Il `security key-manager key delete` Il comando non riesce se la chiave è attualmente in uso da ONTAP. Per utilizzare questo comando, è necessario disporre di privilegi superiori a "admin".



In un ambiente MetroCluster, prima di eliminare una chiave, è necessario assicurarsi che la chiave non sia in uso nel cluster partner. È possibile utilizzare i seguenti comandi sul cluster partner per verificare che la chiave non sia in uso:

- ° `storage encryption disk show -data-key-id key-id`
- ° `storage encryption disk show -fips-key-id key-id`



```
cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: external
      Node: node1
```

| Key Tag                                                                                            | Key Type | Restored |
|----------------------------------------------------------------------------------------------------|----------|----------|
| node1                                                                                              | NSE-AK   | yes      |
| Key ID:<br>000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000<br>00000000 |          |          |
| node1                                                                                              | NSE-AK   | yes      |
| Key ID:<br>000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000<br>00000000 |          |          |

```
      Vserver: cluster1
      Key Manager: external
      Node: node2
```

| Key Tag                                                                                            | Key Type | Restored |
|----------------------------------------------------------------------------------------------------|----------|----------|
| node2                                                                                              | NSE-AK   | yes      |
| Key ID:<br>000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000<br>00000000 |          |          |
| node2                                                                                              | NSE-AK   | yes      |
| Key ID:<br>000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000<br>00000000 |          |          |

### Creare chiavi di autenticazione in ONTAP 9.5 e versioni precedenti

È possibile utilizzare `security key-manager create-key` Per creare le chiavi di autenticazione per un nodo e memorizzarle nei server KMIP configurati.

#### A proposito di questa attività

Se la configurazione della protezione richiede l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2, è necessario creare una chiave separata per ciascuna di esse. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

ONTAP crea chiavi di autenticazione per tutti i nodi del cluster.

- Questo comando non è supportato quando è attivata la gestione delle chiavi integrate.
- Viene visualizzato un avviso se i server di gestione delle chiavi configurati memorizzano già più di 128 chiavi di autenticazione.



È possibile utilizzare il software del server di gestione delle chiavi per eliminare le chiavi inutilizzate, quindi eseguire nuovamente il comando.

## Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

## Fasi

1. Creare le chiavi di autenticazione per i nodi del cluster:

```
security key-manager create-key
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.



L'ID della chiave visualizzato nell'output è un identificatore utilizzato per fare riferimento alla chiave di autenticazione. Non si tratta della chiave di autenticazione effettiva o della chiave di crittografia dei dati.

Nell'esempio seguente vengono create le chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager create-key
(security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. Verificare che le chiavi di autenticazione siano state create:

```
security key-manager query
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per `cluster1`:

```
cluster1::> security key-manager query

(security key-manager query)

Node: cluster1-01
Key Manager: 20.1.1.1
Server Status: available

Key Tag          Key Type  Restored
-----
cluster1-01      NSE-AK    yes
Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-02
Key Manager: 20.1.1.1
Server Status: available

Key Tag          Key Type  Restored
-----
cluster1-02      NSE-AK    yes
Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

#### Assegnazione di una chiave di autenticazione dei dati a un disco FIPS o SED (gestione esterna delle chiavi)

È possibile utilizzare `storage encryption disk modify` Comando per assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED. I nodi del cluster utilizzano questa chiave per bloccare o sbloccare i dati crittografati sul disco.

#### A proposito di questa attività

Un'unità con crittografia automatica è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione è impostato su un valore non predefinito. L'ID sicuro del produttore (MSID), con ID chiave 0x0, è il valore predefinito standard per i dischi SAS. Per i dischi NVMe, il valore predefinito standard è una chiave nulla, rappresentata come ID chiave vuoto. Quando si assegna l'ID della chiave a un'unità con crittografia automatica, il sistema modifica l'ID della chiave di autenticazione in un valore non predefinito.

Questa procedura non comporta interruzioni.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

#### Fasi

1. Assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.



È possibile utilizzare `security key-manager query -key-type NSE-AK` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

```
Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

## 2. Verificare che le chiavi di autenticazione siano state assegnate:

```
storage encryption disk show
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
[...]
```

## Configurare la gestione delle chiavi integrata

**Attiva la gestione delle chiavi integrata in ONTAP 9.6 e versioni successive**

È possibile utilizzare Onboard Key Manager per autenticare i nodi del cluster su un disco FIPS o SED. Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati. Onboard Key Manager è conforme a FIPS-140-2 livello 1.

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

### A proposito di questa attività

È necessario eseguire `security key-manager onboard enable` ogni volta che si aggiunge un nodo al cluster. Nelle configurazioni MetroCluster, è necessario eseguire `security key-manager onboard enable` sul cluster locale, quindi eseguire `security key-manager onboard sync` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. Ad eccezione di MetroCluster, è possibile utilizzare `cc-mode-enabled=yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Quando Onboard Key Manager è attivato in modalità Common Criteria (Criteri comuni) (`cc-mode-enabled=yes`), il comportamento del sistema viene modificato nei seguenti modi:

- Il sistema monitora i tentativi consecutivi di passphrase del cluster non riusciti quando si opera in modalità Common Criteria.

Se NetApp Storage Encryption (NSE) è attivato e non si riesce a inserire la passphrase del cluster corretta all'avvio, il sistema non può autenticare i propri dischi e si riavvia automaticamente. Per risolvere il problema, al prompt di boot occorre inserire la passphrase del cluster corretta. Una volta avviato, il sistema consente fino a 5 tentativi consecutivi di inserire correttamente la passphrase del cluster in un periodo di 24 ore per qualsiasi comando che richieda la passphrase del cluster come parametro. Se il limite viene raggiunto (ad esempio, non è stato possibile inserire correttamente la passphrase del cluster 5 volte di seguito), è necessario attendere che il periodo di timeout di 24 ore sia trascorso oppure riavviare il nodo per ripristinare il limite.

- Gli aggiornamenti delle immagini di sistema utilizzano il certificato di firma del codice NetApp RSA-3072 insieme ai digest con firma del codice SHA-384 per controllare l'integrità dell'immagine invece del certificato di firma del codice NetApp RSA-2048 e dei digest con firma del codice SHA-256.

Il comando `upgrade` verifica che il contenuto dell'immagine non sia stato alterato o corrotto controllando varie firme digitali. Se la convalida ha esito positivo, il processo di aggiornamento dell'immagine passa alla fase successiva; in caso contrario, l'aggiornamento dell'immagine non riesce. Per informazioni sugli aggiornamenti di sistema, consultare la pagina man "cluster image".

Onboard Key Manager memorizza le chiavi nella memoria volatile. I contenuti della memoria volatile vengono cancellati quando il sistema viene riavviato o arrestato. In condizioni operative normali, il contenuto della memoria volatile viene cancellato entro 30 secondi quando il sistema viene arrestato.

## Prima di iniziare

- Se si utilizza NSE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno.

### "Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

## Fasi

1. Avviare il comando di configurazione del gestore delle chiavi:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```



Impostare `cc-mode-enabled=yes` per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Il - `cc-mode-enabled` L'opzione non è supportata nelle configurazioni MetroCluster. Il `security key-manager onboard enable` il comando sostituisce `security key-manager setup` comando.

Nell'esempio seguente viene avviato il comando di configurazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

```
cluster1::> security key-manager onboard enable
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":<32..256 ASCII characters long text>
Reenter the cluster-wide passphrase: <32..256 ASCII characters long
text>
```

2. Al prompt della passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per “cc-mode”, una passphrase compresa tra 64 e 256 caratteri.



Se la passphrase “cc-mode” specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l'operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della passphrase.

3. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
4. Verificare che le chiavi di autenticazione siano state create:

```
security key-manager key query -node node
```



Il `security key-manager key query` il comando sostituisce `security key-manager query key` comando. Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene verificata la creazione di chiavi di autenticazione per cluster1:

```
cluster1::> security key-manager key query
```

```
Vserver: cluster1
```

```
Key Manager: onboard
```

```
Node: node1
```

| Key Tag                                                                             | Key Type | Restored |
|-------------------------------------------------------------------------------------|----------|----------|
| -----                                                                               | -----    | -----    |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000 |          |          |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000 |          |          |

```
Vserver: cluster1
```

```
Key Manager: onboard
```

```
Node: node2
```

| Key Tag                                                                             | Key Type | Restored |
|-------------------------------------------------------------------------------------|----------|----------|
| -----                                                                               | -----    | -----    |
| node1                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e0000000000000000 |          |          |
| node2                                                                               | NSE-AK   | yes      |
| Key ID:                                                                             |          |          |
| 000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf7970000000000000000 |          |          |

## Al termine

Copiare la passphrase in una posizione sicura all'esterno del sistema di storage per utilizzarla in futuro.

Viene eseguito automaticamente il backup di tutte le informazioni di gestione delle chiavi nel database replicato (RDB) del cluster. È inoltre necessario eseguire il backup manuale delle informazioni per utilizzarle in caso di disastro.

## Abilitare la gestione delle chiavi integrata in ONTAP 9.5 e versioni precedenti

È possibile utilizzare Onboard Key Manager per autenticare i nodi del cluster su un disco FIPS o SED. Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati. Onboard Key Manager è conforme a FIPS-140-2 livello 1.

È possibile utilizzare Onboard Key Manager per proteggere le chiavi utilizzate dal cluster per accedere ai dati

crittografati. È necessario attivare Onboard Key Manager su ogni cluster che accede a un volume crittografato o a un disco con crittografia automatica.

### A proposito di questa attività

È necessario eseguire `security key-manager setup` ogni volta che si aggiunge un nodo al cluster.

Se si dispone di una configurazione MetroCluster, consultare le seguenti linee guida:

- In ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale e `security key-manager setup -sync-metrocluster-config yes` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.
- Prima di ONTAP 9.5, è necessario eseguire `security key-manager setup` sul cluster locale, attendere circa 20 secondi, quindi eseguire `security key-manager setup` sul cluster remoto, utilizzando la stessa passphrase su ciascuno di essi.

Per impostazione predefinita, non è necessario immettere la passphrase del gestore delle chiavi quando si riavvia un nodo. A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase dopo un riavvio.

Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e `volume move start` i comandi vengono crittografati automaticamente. Per `volume create`, non è necessario specificare `-encrypt true`. Per `volume move start`, non è necessario specificare `-encrypt-destination true`.



Dopo un tentativo di passphrase non riuscito, riavviare nuovamente il nodo.

### Prima di iniziare

- Se si utilizza NSE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno.

["Passaggio alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"](#)

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario configurare l'ambiente MetroCluster prima di configurare il Gestore chiavi integrato.

### Fasi

1. Avviare la configurazione di Key Manager:

```
security key-manager setup -enable-cc-mode yes|no
```



A partire da ONTAP 9.4, è possibile utilizzare `-enable-cc-mode yes` opzione per richiedere agli utenti di inserire la passphrase del gestore delle chiavi dopo un riavvio. Per NVE, se si imposta `-enable-cc-mode yes`, volumi creati con `volume create` e `volume move start` i comandi vengono crittografati automaticamente.

Nell'esempio seguente viene avviata l'impostazione del gestore delle chiavi sul cluster1 senza che sia necessario inserire la passphrase dopo ogni riavvio:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:  <32..256 ASCII characters long
text>
```

2. Invio `yes` quando viene richiesto di configurare la gestione delle chiavi integrata.
3. Al prompt della passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per “cc-mode”, una passphrase compresa tra 64 e 256 caratteri.



Se la passphrase “cc-mode” specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l’operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della passphrase.

4. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.
5. Verificare che le chiavi siano configurate per tutti i nodi:

```
security key-manager key show
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

```
cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                     Used By
-----
-----
0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                     Used By
-----
-----
0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```



## Al termine

Viene eseguito automaticamente il backup di tutte le informazioni di gestione delle chiavi nel database replicato (RDB) del cluster.

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario eseguire il backup manuale delle informazioni in una posizione sicura all'esterno del sistema di storage per l'utilizzo in caso di disastro.

Vedere ["Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate"](#).

## Assegnazione di una chiave di autenticazione dei dati a un'unità FIPS o SED (onboard key management)

È possibile utilizzare `storage encryption disk modify` Comando per assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED. I nodi del cluster utilizzano questa chiave per accedere ai dati sul disco.

### A proposito di questa attività

Un'unità con crittografia automatica è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione è impostato su un valore non predefinito. L'ID sicuro del produttore (MSID), con ID chiave 0x0, è il valore predefinito standard per i dischi SAS. Per i dischi NVMe, il valore predefinito standard è una chiave nulla, rappresentata come ID chiave vuoto. Quando si assegna l'ID della chiave a un'unità con crittografia automatica, il sistema modifica l'ID della chiave di autenticazione in un valore non predefinito.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

### Fasi

1. Assegnare una chiave di autenticazione dei dati a un'unità FIPS o SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.



È possibile utilizzare `security key-manager key query -key-type NSE-AK` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
```

```
Info: Starting modify on 14 disks.
```

```
View the status of the operation by using the  
storage encryption disk show-status command.
```

2. Verificare che le chiavi di autenticazione siano state assegnate:

```
storage encryption disk show
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
00000000000000000000200000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1     data
00000000000000000000200000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

## Assegnare una chiave di autenticazione FIPS 140-2 a un disco FIPS

È possibile utilizzare `storage encryption disk modify` con il `-fips-key-id` Opzione per assegnare una chiave di autenticazione FIPS 140-2 a un disco FIPS. I nodi del cluster utilizzano questa chiave per operazioni di guida diverse dall'accesso ai dati, come la prevenzione di attacchi di tipo Denial-of-service sul disco.

### A proposito di questa attività

La configurazione della sicurezza potrebbe richiedere l'utilizzo di chiavi diverse per l'autenticazione dei dati e l'autenticazione FIPS 140-2. In caso contrario, è possibile utilizzare la stessa chiave di autenticazione per la conformità FIPS utilizzata per l'accesso ai dati.

Questa procedura non comporta interruzioni.

### Prima di iniziare

Il firmware del disco deve supportare la conformità FIPS 140-2. Il ["Tool di matrice di interoperabilità NetApp"](#) contiene informazioni sulle versioni del firmware del disco supportate.

### Fasi

1. Assicurarsi di aver assegnato una chiave di autenticazione dei dati. Questa operazione può essere eseguita utilizzando un [gestore delle chiavi esterno](#) o un [gestore delle chiavi integrato](#). Verificare che il tasto sia assegnato con il comando `storage encryption disk show`.
2. Assegnare una chiave di autenticazione FIPS 140-2 ai SED:

```
storage encryption disk modify -disk disk_id -fips-key-id
fips_authentication_key_id
```

È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
```

```
Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

### 3. Verificare che la chiave di autenticazione sia stata assegnata:

```
storage encryption disk show -fips
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage encryption disk show -fips
Disk      Mode FIPS-Compliance Key ID
-----
-----
2.10.0    full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1    full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

### Abilitare la modalità compatibile con FIPS a livello di cluster per le connessioni al server KMIP

È possibile utilizzare `security config modify` con il `-is-fips-enabled` Opzione per abilitare la modalità compatibile con FIPS a livello di cluster per i dati in volo. In questo modo, il cluster utilizza OpenSSL in modalità FIPS durante la connessione ai server KMIP.

#### A proposito di questa attività

Quando si attiva la modalità compatibile con FIPS a livello di cluster, il cluster utilizza automaticamente solo le suite di crittografia convalidate da TLS1.2 e FIPS. La modalità compatibile con FIPS a livello di cluster è disattivata per impostazione predefinita.

È necessario riavviare manualmente i nodi del cluster dopo aver modificato la configurazione di sicurezza a livello di cluster.

#### Prima di iniziare

- Lo storage controller deve essere configurato in modalità conforme a FIPS.
- Tutti i server KMIP devono supportare TLSv1.2. Il sistema richiede TLSv1.2 per completare la connessione al server KMIP quando è attivata la modalità compatibile con FIPS a livello di cluster.

#### Fasi

##### 1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

##### 2. Verificare che TLSv1.2 sia supportato:

```
security config show -supported-protocols
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> security config show
```

|           | Cluster   |                         | Cluster                             |
|-----------|-----------|-------------------------|-------------------------------------|
| Security  |           |                         |                                     |
| Interface | FIPS Mode | Supported Protocols     | Supported Ciphers Config            |
| Ready     |           |                         |                                     |
| -----     | -----     | -----                   | -----                               |
| -----     | -----     |                         |                                     |
| SSL       | false     | TLSv1.2, TLSv1.1, TLSv1 | ALL:!LOW:<br>!aNULL:!EXP:<br>!eNULL |
|           |           |                         | yes                                 |

### 3. Abilitare la modalità compatibile con FIPS a livello di cluster:

```
security config modify -is-fips-enabled true -interface SSL
```

Per la sintassi completa dei comandi, vedere la pagina man.

### 4. Riavviare manualmente i nodi del cluster.

### 5. Verificare che la modalità compatibile con FIPS a livello di cluster sia attivata:

```
security config show
```

```
cluster1::> security config show
```

|           | Cluster   |                     | Cluster                                  |
|-----------|-----------|---------------------|------------------------------------------|
| Security  |           |                     |                                          |
| Interface | FIPS Mode | Supported Protocols | Supported Ciphers Config                 |
| Ready     |           |                     |                                          |
| -----     | -----     | -----               | -----                                    |
| -----     | -----     |                     |                                          |
| SSL       | true      | TLSv1.2, TLSv1.1    | ALL:!LOW:<br>!aNULL:!EXP:<br>!eNULL:!RC4 |
|           |           |                     | yes                                      |

## Gestire la crittografia NetApp

### Decrittografare i dati del volume

È possibile utilizzare `volume move start` comando per spostare e rimuovere la crittografia dei dati del volume.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere ["Delegare l'autorità per eseguire il comando di spostamento del volume"](#).

#### Fasi

1. Spostare un volume crittografato esistente e annullare la crittografia dei dati sul volume:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate  
aggregate_name -encrypt-destination false
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando sposta un volume esistente denominato `vol1` all'aggregato di destinazione `aggr3` e annulla la crittografia dei dati sul volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggregate aggr3 -encrypt-destination false
```

Il sistema elimina la chiave di crittografia per il volume. I dati del volume non sono crittografati.

2. Verificare che il volume sia disattivato per la crittografia:

```
volume show -encryption
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando indica se i volumi sono accessi `cluster1` sono crittografati:

```
cluster1::> volume show -encryption
```

| Vserver | Volume | Aggregate | State  | Encryption State |
|---------|--------|-----------|--------|------------------|
| vs1     | vol1   | aggr1     | online | none             |

## Spostare un volume crittografato

È possibile utilizzare `volume move start` comando per spostare un volume crittografato. Il volume spostato può risiedere sullo stesso aggregato o su un aggregato diverso.

### A proposito di questa attività

Lo spostamento non riesce se il nodo di destinazione o il volume di destinazione non supporta la crittografia del volume.

Il `-encrypt-destination` opzione per `volume move start` l'impostazione predefinita è `true` per i volumi crittografati. Il requisito di specificare che non si desidera che il volume di destinazione venga crittografato garantisce che i dati sul volume non vengano inavvertitamente decrittografati.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere ["delegare l'autorità per eseguire il comando di spostamento del volume"](#).

## Fasi

1. Spostare un volume crittografato esistente e lasciare crittografati i dati sul volume:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando sposta un volume esistente denominato `vol1` all'aggregato di destinazione `aggr3` e lascia crittografati i dati sul volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination -aggregate aggr3
```

2. Verificare che il volume sia abilitato per la crittografia:

```
volume show -is-encrypted true
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando visualizza i volumi crittografati su `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type | Size  | Available | Used  |
|---------|--------|-----------|--------|------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ---- | ----- | -----     | ----- |
| vs1     | vol1   | aggr3     | online | RW   | 200GB | 160.0GB   | 20%   |

## Delegare l'autorità per eseguire il comando di spostamento del volume

È possibile utilizzare `volume move` comando per crittografare un volume esistente, spostare un volume crittografato o annullare la crittografia di un volume. Gli amministratori del cluster possono eseguire `volume move` Oppure possono delegare l'autorità per eseguire il comando agli amministratori SVM.

### A proposito di questa attività

Per impostazione predefinita, agli amministratori SVM viene assegnato il `vsadmin` ruolo, che non include l'autorità per spostare i volumi. È necessario assegnare `vsadmin-volume` Agli amministratori di SVM per consentire loro di eseguire `volume move` comando.

## Fase

1. Delegare l'autorità per eseguire `volume move` comando:

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role vsadmin-volume
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando concede all'amministratore SVM l'autorizzazione per eseguire `volume move` comando.

```
cluster1::>security login modify -vserver engData -user-or-group-name  
SVM-admin -application ssh -authmethod domain -role vsadmin-volume
```

### Modificare la chiave di crittografia per un volume con il comando di avvio della chiave di crittografia del volume

È consigliabile modificare periodicamente la chiave di crittografia di un volume. A partire da ONTAP 9.3, è possibile utilizzare `volume encryption rekey start` per modificare la chiave di crittografia.

#### A proposito di questa attività

Una volta avviata un'operazione di rekey, questa deve essere completata. Non è possibile tornare alla vecchia chiave. Se si verificano problemi di prestazioni durante l'operazione, è possibile eseguire `volume encryption rekey pause` per sospendere l'operazione e il `volume encryption rekey resume` per riprendere l'operazione.

Fino al termine dell'operazione di rekey, il volume avrà due tasti. Le nuove scritture e le corrispondenti letture utilizzeranno la nuova chiave. In caso contrario, Read utilizzerà la vecchia chiave.



Non è possibile utilizzare `volume encryption rekey start` Per modificare la chiave di un volume SnapLock.

#### Fasi

1. Modifica di una chiave di crittografia:

```
volume encryption rekey start -vserver SVM_name -volume volume_name
```

Il seguente comando modifica la chiave di crittografia per `vol1` Su `SVMvs1`:

```
cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
```

2. Verificare lo stato dell'operazione di rekey:

```
volume encryption rekey show
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando visualizza lo stato dell'operazione di rekey:

```
cluster1::> volume encryption rekey show
```

| Vserver | Volume | Start Time         | Status                       |
|---------|--------|--------------------|------------------------------|
| -----   | -----  | -----              | -----                        |
| vs1     | vol1   | 9/18/2017 17:51:41 | Phase 2 of 2 is in progress. |

3. Una volta completata l'operazione di rekey, verificare che il volume sia abilitato per la crittografia:

```
volume show -is-encrypted true
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando visualizza i volumi crittografati su `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | vol1   | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

### Modificare la chiave di crittografia per un volume con il comando di avvio spostamento volume

È consigliabile modificare periodicamente la chiave di crittografia di un volume. È possibile utilizzare `volume move start` per modificare la chiave di crittografia. È necessario utilizzare `volume move start` in ONTAP 9.2 e versioni precedenti. Il volume spostato può risiedere sullo stesso aggregato o su un aggregato diverso.

#### A proposito di questa attività

Non è possibile utilizzare `volume move start` Per modificare la chiave di un volume SnapLock o FlexGroup.

#### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere ["delegare l'autorità per eseguire il comando di spostamento del volume"](#).

#### Fasi

1. Spostare un volume esistente e modificare la chiave di crittografia:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate  
aggregate_name -generate-destination-key true
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando sposta un volume esistente denominato **vol1** all'aggregato di destinazione **aggr2** e modifica la chiave di crittografia:



```
cluster1::> volume move start -vserver vs1 -volume voll1 -destination  
-aggregate aggr2 -generate-destination-key true
```

Viene creata una nuova chiave di crittografia per il volume. I dati sul volume rimangono crittografati.

2. Verificare che il volume sia abilitato per la crittografia:

```
volume show -is-encrypted true
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando visualizza i volumi crittografati su cluster1:

```
cluster1::> volume show -is-encrypted true
```

| Vserver | Volume | Aggregate | State  | Type  | Size  | Available | Used  |
|---------|--------|-----------|--------|-------|-------|-----------|-------|
| -----   | -----  | -----     | -----  | ----- | ----- | -----     | ----- |
| vs1     | voll1  | aggr2     | online | RW    | 200GB | 160.0GB   | 20%   |

## Ruotare le chiavi di autenticazione per NetApp Storage Encryption

È possibile ruotare le chiavi di autenticazione quando si utilizza NetApp Storage Encryption (NSE).

### A proposito di questa attività

La rotazione delle chiavi di autenticazione in un ambiente NSE è supportata se si utilizza External Key Manager (KMIP).



La rotazione delle chiavi di autenticazione in un ambiente NSE non è supportata da Onboard Key Manager (OKM).

### Fasi

1. Utilizzare `security key-manager create-key` per generare nuove chiavi di autenticazione.

Prima di poter modificare le chiavi di autenticazione, è necessario generare nuove chiavi di autenticazione.

2. Utilizzare `storage encryption disk modify -disk * -data-key-id` per modificare le chiavi di autenticazione.

## Eliminare un volume crittografato

È possibile utilizzare `volume delete` comando per eliminare un volume crittografato.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster. In alternativa, puoi essere un amministratore SVM a cui l'amministratore del cluster ha delegato l'autorità. Per ulteriori informazioni, vedere ["delegare l'autorità per eseguire il comando di spostamento del volume"](#).

- Il volume deve essere offline.

## Fase

### 1. Eliminazione di un volume crittografato:

```
volume delete -vserver SVM_name -volume volume_name
```

Per la sintassi completa dei comandi, vedere la pagina man del comando.

Il seguente comando elimina un volume crittografato denominato vol1:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Invio `yes` quando viene richiesto di confermare l'eliminazione.

Il sistema elimina la chiave di crittografia per il volume dopo 24 ore.

Utilizzare `volume delete` con `-force true` opzione per eliminare un volume e distruggere immediatamente la chiave di crittografia corrispondente. Questo comando richiede privilegi avanzati. Per ulteriori informazioni, consulta la pagina man.

## Al termine

È possibile utilizzare `volume recovery-queue` comando per ripristinare un volume cancellato durante il periodo di conservazione dopo l'emissione di `volume delete` comando:

```
volume recovery-queue SVM_name -volume volume_name
```

["Come utilizzare la funzione Volume Recovery \(Ripristino volume\)"](#)

## Eliminare in modo sicuro i dati su un volume crittografato

### Elimina in modo sicuro i dati su una panoramica dei volumi crittografati

A partire da ONTAP 9.4, è possibile utilizzare l'eliminazione sicura per eseguire lo scrubbing dei dati senza interruzioni su volumi abilitati per NVE. Lo scrubbing dei dati su un volume crittografato garantisce che non sia possibile ripristinarli dal supporto fisico, ad esempio in caso di "ssaccheggio", in cui le tracce dei dati potrebbero essere state lasciate indietro quando i blocchi sono stati sovrascritti o per eliminare in modo sicuro i dati di un tenant vuoto.

L'eliminazione sicura funziona solo per i file precedentemente cancellati sui volumi abilitati per NVE. Non è possibile eseguire lo scrubbing di un volume non crittografato. È necessario utilizzare i server KMIP per fornire le chiavi, non il gestore delle chiavi integrato.

## Considerazioni per l'utilizzo della rimozione sicura

- I volumi creati in un aggregato abilitato per NetApp aggregate Encryption (NAE) non supportano l'eliminazione sicura.
- L'eliminazione sicura funziona solo per i file precedentemente cancellati sui volumi abilitati per NVE.

- Non è possibile eseguire lo scrubbing di un volume non crittografato.
- È necessario utilizzare i server KMIP per fornire le chiavi, non il gestore delle chiavi integrato.

L'eliminazione sicura funziona in modo diverso a seconda della versione di ONTAP in uso.

#### ONTAP 9.8 e versioni successive

- L'eliminazione sicura è supportata da MetroCluster e FlexGroup.
- Se il volume da rimuovere è l'origine di una relazione SnapMirror, non è necessario interrompere la relazione SnapMirror per eseguire un'eliminazione sicura.
- Il metodo di ricEncryption è diverso per i volumi che utilizzano la protezione dei dati SnapMirror rispetto ai volumi che non utilizzano la protezione dei dati SnapMirror o quelli che utilizzano la protezione estesa dei dati SnapMirror.
  - Per impostazione predefinita, i volumi che utilizzano la modalità di protezione dati SnapMirror (DP) crittografano nuovamente i dati utilizzando il metodo di ricifratura dello spostamento del volume.
  - Per impostazione predefinita, i volumi che non utilizzano la protezione dei dati SnapMirror o i volumi che utilizzano la modalità XDP (Extended Data Protection) di SnapMirror utilizzano il metodo di riscrittazione in-place.
  - È possibile modificare queste impostazioni predefinite utilizzando `secure purge re-encryption-method [volume-move|in-place-rekey]` comando.
- Per impostazione predefinita, tutte le copie Snapshot nei volumi FlexVol vengono eliminate automaticamente durante l'operazione di eliminazione sicura. Per impostazione predefinita, le istantanee nei volumi e nei volumi FlexGroup che utilizzano la protezione dei dati SnapMirror non vengono eliminate automaticamente durante l'operazione di eliminazione sicura. È possibile modificare queste impostazioni predefinite utilizzando `secure purge delete-all-snapshots [true|false]` comando.

#### ONTAP 9.7 e versioni precedenti:

- L'eliminazione sicura non supporta quanto segue:
  - FlexClone
  - SnapVault
  - FabricPool
- Se il volume da rimuovere è l'origine di una relazione SnapMirror, è necessario interrompere la relazione SnapMirror prima di poter eliminare il volume.

Se nel volume sono presenti copie Snapshot occupate, è necessario rilasciare le copie Snapshot prima di poter eliminare il volume. Ad esempio, potrebbe essere necessario separare un volume FlexClone dal volume padre.

- Il corretto richiamo della funzione di eliminazione sicura attiva uno spostamento del volume che crittografa nuovamente i dati rimanenti non eliminati con una nuova chiave.

Il volume spostato rimane nell'aggregato corrente. La vecchia chiave viene automaticamente distrutta, garantendo che i dati rimossi non possano essere ripristinati dal supporto di storage.

A partire da ONTAP 9.4, è possibile utilizzare la funzione Secure-purge per i dati “scrub” senza interruzioni su volumi abilitati per NVE.

### A proposito di questa attività

Il completamento dell'eliminazione sicura può richiedere da diversi minuti a molte ore, a seconda della quantità di dati contenuti nei file cancellati. È possibile utilizzare `volume encryption secure-purge show` per visualizzare lo stato dell'operazione. È possibile utilizzare `volume encryption secure-purge abort` per terminare l'operazione.



Per eseguire un'eliminazione sicura su un host SAN, è necessario eliminare l'intero LUN contenente i file da eliminare oppure è necessario essere in grado di perforare i LUN per i blocchi che appartengono ai file che si desidera eliminare. Se non è possibile eliminare il LUN o se il sistema operativo host non supporta i fori di punzonatura nel LUN, non è possibile eseguire un'eliminazione sicura.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

### Fasi

1. Eliminare i file o il LUN che si desidera eliminare in modo sicuro.
  - Su un client NAS, eliminare i file che si desidera eliminare in modo sicuro.
  - Su un host SAN, eliminare il LUN che si desidera eliminare in modo sicuro o perforare i fori nel LUN per i blocchi che appartengono ai file che si desidera eliminare.
2. Sul sistema storage, passare al livello di privilegio avanzato:

```
set -privilege advanced
```

3. Se i file che si desidera eliminare in modo sicuro si trovano in snapshot, eliminare le snapshot:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

4. Eliminare in modo sicuro i file cancellati:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Il seguente comando elimina in modo sicuro i file cancellati su `vol1` Su `SVMvs1`:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume  
vol1
```

5. Verificare lo stato dell'operazione di eliminazione sicura:

```
volume encryption secure-purge show
```

A partire da ONTAP 9.8, è possibile utilizzare un purge sicuro per i dati “scrub” senza interruzioni su volumi abilitati per NVE con una relazione asincrona SnapMirror.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

### A proposito di questa attività

Il completamento dell'eliminazione sicura può richiedere da diversi minuti a molte ore, a seconda della quantità di dati contenuti nei file cancellati. È possibile utilizzare `volume encryption secure-purge show` per visualizzare lo stato dell'operazione. È possibile utilizzare `volume encryption secure-purge abort` per terminare l'operazione.



Per eseguire un'eliminazione sicura su un host SAN, è necessario eliminare l'intero LUN contenente i file da eliminare oppure è necessario essere in grado di perforare i LUN per i blocchi che appartengono ai file che si desidera eliminare. Se non è possibile eliminare il LUN o se il sistema operativo host non supporta i fori di punzonatura nel LUN, non è possibile eseguire un'eliminazione sicura.

### Fasi

1. Nel sistema di archiviazione, passare al livello di privilegi avanzato:

```
set -privilege advanced
```

2. Eliminare i file o il LUN che si desidera eliminare in modo sicuro.
  - Su un client NAS, eliminare i file che si desidera eliminare in modo sicuro.
  - Su un host SAN, eliminare il LUN che si desidera eliminare in modo sicuro o perforare i fori nel LUN per i blocchi che appartengono ai file che si desidera eliminare.

3. Preparare il volume di destinazione nella relazione asincrona per la rimozione sicura:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

Ripetere questo passaggio su ciascun volume nella relazione di SnapMirror asincrona.

4. Se i file che si desidera eliminare in modo sicuro si trovano nelle copie Snapshot, eliminare le copie Snapshot:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

5. Se i file che si desidera eliminare in modo sicuro si trovano nelle copie Snapshot di base, procedere come segue:

- a. Creare una copia Snapshot sul volume di destinazione nella relazione SnapMirror asincrona:

```
volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume  
volume_name
```

- b. Aggiornare SnapMirror per spostare in avanti la copia Snapshot di base:

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

Ripetere questo passaggio per ogni volume nella relazione di SnapMirror asincrona.

- a. Ripetere i passaggi (a) e (b) pari al numero di copie Snapshot di base più una.

Ad esempio, se si dispone di due copie Snapshot di base, ripetere i passaggi (a) e (b) tre volte.

- b. Verificare che la copia Snapshot di base sia presente:

```
snapshot show -vserver SVM_name -volume volume_name
```

- c. Eliminare la copia Snapshot di base:

```
snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot
```

#### 6. Eliminare in modo sicuro i file cancellati:

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

Ripetere questo passaggio su ciascun volume nella relazione di SnapMirror asincrona.

Il seguente comando elimina in modo sicuro i file cancellati su "vol1" su SVM "vs1":

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume  
vol1
```

#### 7. Verificare lo stato dell'operazione di eliminazione sicura:

```
volume encryption secure-purge show
```

### Eseguire lo scrubbing dei dati su un volume crittografato con una relazione SnapMirror sincrona

A partire da ONTAP 9,8, puoi utilizzare una pulizia sicura per "scrub" senza interruzioni dei dati su volumi abilitati per NVE con una relazione di SnapMirror sincrono.

#### A proposito di questa attività

Il completamento di una rimozione sicura potrebbe richiedere da diversi minuti a molte ore, a seconda della quantità di dati contenuti nei file cancellati. È possibile utilizzare `volume encryption secure-purge show` per visualizzare lo stato dell'operazione. È possibile utilizzare `volume encryption secure-purge abort` per terminare l'operazione.



Per eseguire un'eliminazione sicura su un host SAN, è necessario eliminare l'intero LUN contenente i file da eliminare oppure è necessario essere in grado di perforare i LUN per i blocchi che appartengono ai file che si desidera eliminare. Se non è possibile eliminare il LUN o se il sistema operativo host non supporta i fori di punzonatura nel LUN, non è possibile eseguire un'eliminazione sicura.

#### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.

- Per questa attività sono richiesti privilegi avanzati.

## Fasi

1. Sul sistema storage, passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Eliminare i file o il LUN che si desidera eliminare in modo sicuro.
  - Su un client NAS, eliminare i file che si desidera eliminare in modo sicuro.
  - Su un host SAN, eliminare il LUN che si desidera eliminare in modo sicuro o perforare i fori nel LUN per i blocchi che appartengono ai file che si desidera eliminare.
3. Preparare il volume di destinazione nella relazione asincrona per la rimozione sicura:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

Ripetere questo passaggio per l'altro volume nella relazione di Synchronous SnapMirror.

4. Se i file che si desidera eliminare in modo sicuro si trovano nelle copie Snapshot, eliminare le copie Snapshot:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
```

5. Se il file di eliminazione sicuro si trova nelle copie Snapshot di base o comuni, aggiornare SnapMirror per spostare la copia Snapshot comune in avanti:

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

Esistono due copie Snapshot comuni, quindi questo comando deve essere emesso due volte.

6. Se il file di eliminazione sicuro si trova nella copia Snapshot coerente con l'applicazione, eliminare la copia Snapshot su entrambi i volumi nella relazione SnapMirror sincrona:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
```

Eseguire questa operazione su entrambi i volumi.

7. Eliminare in modo sicuro i file cancellati:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

Ripetere questo passaggio su ciascun volume nella relazione SnapMirror sincrona.

Il seguente comando elimina in modo sicuro i file cancellati su "vol1" su SMV "vs1".

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume  
vol1
```

8. Verificare lo stato dell'operazione di eliminazione sicura:

```
volume encryption secure-purge show
```

## Modificare la passphrase di gestione della chiave integrata

È consigliabile modificare periodicamente la passphrase di gestione delle chiavi integrate. Copiare la nuova passphrase di gestione della chiave integrata in una posizione sicura all'esterno del sistema di storage per un utilizzo futuro.

### Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- Per questa attività sono richiesti privilegi avanzati.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Modificare la passphrase di gestione della chiave integrata:

| Per questa versione di ONTAP... | Utilizzare questo comando...                                |
|---------------------------------|-------------------------------------------------------------|
| ONTAP 9.6 e versioni successive | <code>security key-manager onboard update-passphrase</code> |
| ONTAP 9.5 e versioni precedenti | <code>security key-manager update-passphrase</code>         |

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando ONTAP 9.6 consente di modificare la passphrase di gestione delle chiavi integrata per `cluster1`:

```
cluster1::> security key-manager onboard update-passphrase
Warning: This command will reconfigure the cluster passphrase for
onboard key management for Vserver "cluster1".
Do you want to continue? {y|n}: y
Enter current passphrase:
Enter new passphrase:
```

3. Invio `y` quando viene richiesto di modificare la passphrase di gestione della chiave integrata.
4. Inserire la passphrase corrente al prompt della passphrase corrente.
5. Al prompt della nuova passphrase, immettere una passphrase compresa tra 32 e 256 caratteri oppure, per "cc-mode", una passphrase compresa tra 64 e 256 caratteri.

Se la passphrase "cc-mode" specificata è inferiore a 64 caratteri, si verifica un ritardo di cinque secondi prima che l'operazione di configurazione del gestore delle chiavi visualizzi nuovamente il prompt della



passphrase.

6. Al prompt di conferma della passphrase, immettere nuovamente la passphrase.

### Al termine

In un ambiente MetroCluster, è necessario aggiornare la passphrase sul cluster partner:

- In ONTAP 9.5 e versioni precedenti, è necessario eseguire `security key-manager update-passphrase` con la stessa passphrase sul cluster partner.
- In ONTAP 9.6 e versioni successive, viene richiesto di eseguire `security key-manager onboard sync` con la stessa passphrase sul cluster partner.

Copiare la passphrase di gestione della chiave integrata in una posizione sicura all'esterno del sistema di storage per un utilizzo futuro.

È necessario eseguire il backup manuale delle informazioni di gestione delle chiavi ogni volta che si modifica la passphrase di gestione delle chiavi integrata.

["Backup manuale delle informazioni di gestione delle chiavi integrate"](#)

### Eseguire il backup manuale delle informazioni di gestione delle chiavi integrate

Ogni volta che si configura la passphrase di Onboard Key Manager, è necessario copiare le informazioni di gestione delle chiavi integrate in una posizione sicura all'esterno del sistema di storage.

### Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono richiesti privilegi avanzati.

### A proposito di questa attività

Viene eseguito automaticamente il backup di tutte le informazioni di gestione delle chiavi nel database replicato (RDB) del cluster. È inoltre necessario eseguire il backup manuale delle informazioni di gestione delle chiavi per utilizzarle in caso di disastro.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Visualizzare le informazioni di backup della gestione delle chiavi per il cluster:

| Per questa versione di ONTAP... | Utilizzare questo comando...                          |
|---------------------------------|-------------------------------------------------------|
| ONTAP 9.6 e versioni successive | <code>security key-manager onboard show-backup</code> |
| ONTAP 9.5 e versioni precedenti | <code>security key-manager backup show</code>         |

Per la sintassi completa dei comandi, vedere le pagine `man`.

+

[illegible]

- ## Ripristinare le chiavi di crittografia integrate per la gestione delle chiavi

## Prima di iniziare

- Se si utilizza NSE con un server KMIP (Key Management) esterno, è necessario eliminare il database del gestore delle chiavi esterno. Per ulteriori informazioni, vedere ["transizione alla gestione delle chiavi integrata dalla gestione delle chiavi esterna"](#)
- Per eseguire questa attività, è necessario essere un amministratore del cluster.



Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSe non crittografa i dati che risiedono nel modulo Flash cache.

#### ONTAP 9.8 e versioni successive con volume root crittografato



Se si esegue ONTAP 9.8 o versione successiva e il volume root non è crittografato, seguire la procedura per ONTAP 9.6 o versione successiva.

Se si utilizza ONTAP 9.8 e versioni successive e il volume root è crittografato, è necessario impostare una passphrase di ripristino per la gestione delle chiavi integrata nel menu di avvio. Questo processo è necessario anche se si esegue una sostituzione dei supporti di avvio.

1. Avviare il nodo dal menu di boot e selezionare l'opzione (10) Set onboard key management recovery secrets.
2. Invio `y` per utilizzare questa opzione.
3. Quando richiesto, inserire la passphrase di gestione della chiave integrata per il cluster.
4. Quando richiesto, inserire i dati della chiave di backup.

Il nodo torna al menu di boot.

5. Dal menu di avvio, selezionare opzione (1) Normal Boot.

#### ONTAP 9.6 e versioni successive

1. Verificare che la chiave debba essere ripristinata:  
`security key-manager key query -node node`
2. Ripristinare la chiave:  
`security key-manager onboard sync`

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando ONTAP 9.6 sincronizza le chiavi nella gerarchia di chiavi integrate:

```
cluster1::> security key-manager onboard sync
```

```
Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":: <32..256 ASCII characters long text>
```

3. Al prompt della passphrase, inserire la passphrase di gestione della chiave integrata per il cluster.

#### ONTAP 9.5 e versioni precedenti

1. Verificare che la chiave debba essere ripristinata:

```
security key-manager key show
```

2. Se si utilizza ONTAP 9.8 e versioni successive e il volume root è crittografato, attenersi alla seguente procedura:

Se si utilizza ONTAP 9.6 o 9.7, o se si utilizza ONTAP 9.8 o versione successiva e il volume root non è crittografato, ignorare questo passaggio.

3. Ripristinare la chiave:

```
security key-manager setup -node node
```

Per la sintassi completa dei comandi, vedere le pagine man.

4. Al prompt della passphrase, inserire la passphrase di gestione della chiave integrata per il cluster.

## Ripristinare le chiavi di crittografia esterne per la gestione delle chiavi

È possibile ripristinare manualmente le chiavi di crittografia della gestione esterna delle chiavi e inviarle a un nodo diverso. Questa operazione potrebbe essere utile se si sta riavviando un nodo temporaneamente inattivo quando sono state create le chiavi per il cluster.

### A proposito di questa attività

In ONTAP 9.6 e versioni successive, è possibile utilizzare `security key-manager key query -node node_name` per verificare se la chiave deve essere ripristinata.

In ONTAP 9.5 e versioni precedenti, è possibile utilizzare `security key-manager key show` per verificare se la chiave deve essere ripristinata.



Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSe non crittografa i dati che risiedono nel modulo Flash cache.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

### Fasi

1. Se si utilizza ONTAP 9.8 o versione successiva e il volume root è crittografato, procedere come segue:

Se si utilizza ONTAP 9.7 o versioni precedenti o se si utilizza ONTAP 9.8 o versioni successive e il volume root non è crittografato, ignorare questo passaggio.

- a. Impostare il bootargs:

```
setenv kmip.init.ipaddr <ip-address>+
setenv kmip.init.netmask <netmask>+
setenv kmip.init.gateway <gateway>+
setenv kmip.init.interface e0M+
boot_ontap
```

- b. Avviare il nodo dal menu di boot e selezionare l'opzione (11) Configure node for external key management.
- c. Seguire le istruzioni per inserire il certificato di gestione.

Una volta inserite tutte le informazioni del certificato di gestione, il sistema torna al menu di avvio.

d. Dal menu di avvio, selezionare opzione (1) Normal Boot.

## 2. Ripristinare la chiave:

| Per questa versione di ONTAP...                   | Utilizzare questo comando...                                                                       |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------|
| ONTAP 9.6 e versioni successive                   | <code>`security key-manager external restore -vserver SVM -node node -key-server host_name`</code> |
| IP_address:port -key-id key_id -key -tag key_tag` | ONTAP 9.5 e versioni precedenti                                                                    |



node per impostazione predefinita, tutti i nodi. Per la sintassi completa dei comandi, vedere le pagine man. Questo comando non è supportato quando è attivata la gestione delle chiavi integrate.

Il seguente comando ONTAP 9.6 ripristina le chiavi di autenticazione esterne per la gestione delle chiavi in tutti i nodi in `cluster1`:

```
cluster1::> security key-manager external restore
```

## Sostituire i certificati SSL

Tutti i certificati SSL hanno una data di scadenza. È necessario aggiornare i certificati prima che scadano per evitare la perdita di accesso alle chiavi di autenticazione.

### Prima di iniziare

- È necessario aver ottenuto il certificato pubblico e la chiave privata sostitutivi per il cluster (certificato del client KMIP).
- È necessario aver ottenuto il certificato pubblico sostitutivo per il server KMIP (certificato KMIP server-ca).
- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- In un ambiente MetroCluster, è necessario sostituire il certificato SSL KMIP su entrambi i cluster.



È possibile installare i certificati client e server sostitutivi sul server KMIP prima o dopo l'installazione dei certificati sul cluster.

### Fasi

1. Installare il nuovo certificato KMIP server-ca:

```
security certificate install -type server-ca -vserver <>
```

2. Installare il nuovo certificato del client KMIP:

```
security certificate install -type client -vserver <>
```

3. Aggiornare la configurazione del gestore delle chiavi per utilizzare i certificati appena installati:

```
security key-manager external modify -vserver <> -client-cert <> -server-ca  
-certs <>
```

Se si esegue ONTAP 9.6 o versione successiva in un ambiente MetroCluster e si desidera modificare la configurazione del gestore delle chiavi nella SVM amministrativa, è necessario eseguire il comando su entrambi i cluster della configurazione.



L'aggiornamento della configurazione del gestore delle chiavi per utilizzare i certificati appena installati restituisce un errore se le chiavi pubbliche/private del nuovo certificato client sono diverse dalle chiavi installate in precedenza. Consultare l'articolo della Knowledge base "[Le chiavi pubbliche o private del nuovo certificato client sono diverse dal certificato client esistente](#)" per istruzioni su come ignorare questo errore.

### Sostituire un'unità FIPS o SED

È possibile sostituire un'unità FIPS o SED nello stesso modo in cui si sostituisce un disco normale. Assicurarsi di assegnare nuove chiavi di autenticazione dei dati all'unità sostitutiva. Per un'unità FIPS, potrebbe essere necessario assegnare una nuova chiave di autenticazione FIPS 140-2.



Se è in uso una coppia ha "[Crittografia dei dischi SAS o NVMe \(SED, NSE, FIPS\)](#)", è necessario seguire le istruzioni riportate nell'argomento "[Ripristino di un'unità FIPS o SED in modalità non protetta](#)". Per tutti i dischi all'interno della coppia ha prima dell'inizializzazione del sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

### Prima di iniziare

- È necessario conoscere l'ID della chiave di autenticazione utilizzata dal disco.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

### Fasi

1. Assicurarsi che il disco sia stato contrassegnato come guasto:

```
storage disk show -broken
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage disk show -broken
```

```
Original Owner: cluster1-01
```

```
Checksum Compatibility: block
```

|          |        |         |      |       |      |      |       |       |       |         | Usable |
|----------|--------|---------|------|-------|------|------|-------|-------|-------|---------|--------|
| Physical |        |         |      |       |      |      |       |       |       |         |        |
| Disk     | Outage | Reason  | HA   | Shelf | Bay  | Chan | Pool  | Type  | RPM   | Size    |        |
| Size     |        |         |      |       |      |      |       |       |       |         |        |
| -----    | ----   | -----   | ---- | ----  | ---- | ---- | ----- | ----- | ----- | -----   | -----  |
| 0.0.0    | admin  | failed  | 0b   | 1     | 0    | A    | Pool0 | FCAL  | 10000 | 132.8GB |        |
| 133.9GB  |        |         |      |       |      |      |       |       |       |         |        |
| 0.0.7    | admin  | removed | 0b   | 2     | 6    | A    | Pool1 | FCAL  | 10000 | 132.8GB |        |
| 134.2GB  |        |         |      |       |      |      |       |       |       |         |        |
| [...]    |        |         |      |       |      |      |       |       |       |         |        |

2. Rimuovere il disco guasto e sostituirlo con un nuovo disco FIPS o SED, seguendo le istruzioni nella guida hardware del modello di shelf di dischi in uso.
3. Assegnare la proprietà del disco appena sostituito:

```
storage disk assign -disk disk_name -owner node
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Verificare che il nuovo disco sia stato assegnato:

```
storage encryption disk show
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.0    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1     open 0x0
[...]
```

5. Assegnare le chiavi di autenticazione dei dati all'unità FIPS o SED.

"Assegnazione di una chiave di autenticazione dei dati a un disco FIPS o SED (gestione esterna delle chiavi)"

6. Se necessario, assegnare una chiave di autenticazione FIPS 140-2 all'unità FIPS.

"Assegnazione di una chiave di autenticazione FIPS 140-2 a un disco FIPS"

## Rendere i dati su un disco FIPS o SED inaccessibili

### Rendere i dati su un disco FIPS o panoramica SED inaccessibili

Se si desidera rendere i dati su un'unità FIPS o SED permanentemente inaccessibili, mantenendo lo spazio inutilizzato dell'unità disponibile per i nuovi dati, è possibile disinfettare il disco. Se si desidera rendere i dati inaccessibili in modo permanente e non è necessario riutilizzare il disco, è possibile distruggerli.

- Pulizia dei dischi

Quando si disigenizza un'unità con crittografia automatica, il sistema modifica la chiave di crittografia del disco in un nuovo valore casuale, ripristina lo stato di blocco all'accensione su false e imposta l'ID della chiave su un valore predefinito, ovvero l'ID protetto del produttore 0x0 (unità SAS) o una chiave nulla (unità NVMe). In questo modo, i dati sul disco non sono accessibili e non possono essere recuperati. È possibile riutilizzare i dischi sanitizzati come dischi di riserva non azzerati.

- Distruggere il disco

Quando si distrugge un disco FIPS o SED, il sistema imposta la chiave di crittografia del disco su un valore casuale sconosciuto e blocca il disco in modo irreversibile. In questo modo, il disco risulta inutilizzabile in modo permanente e i dati in esso contenuti sono inaccessibili in modo permanente.

È possibile sanificare o distruggere singole unità con crittografia automatica o tutte le unità con crittografia automatica per un nodo.



## Sanificare un disco FIPS o SED

Se si desidera rendere i dati su un'unità FIPS o SED permanentemente inaccessibili e utilizzare l'unità per i nuovi dati, è possibile utilizzare `storage encryption disk sanitize` comando per la pulizia del disco.

### A proposito di questa attività

Quando si disigienizza un'unità con crittografia automatica, il sistema modifica la chiave di crittografia del disco in un nuovo valore casuale, ripristina lo stato di blocco all'accensione su false e imposta l'ID della chiave su un valore predefinito, ovvero l'ID protetto del produttore 0x0 (unità SAS) o una chiave nulla (unità NVMe). In questo modo, i dati sul disco non sono accessibili e non possono essere recuperati. È possibile riutilizzare i dischi sanitizzati come dischi di riserva non azzerati.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

### Fasi

1. Migrare tutti i dati che devono essere conservati in un aggregato su un altro disco.
2. Eliminare l'aggregato sull'unità FIPS o SED da sanificare:

```
storage aggregate delete -aggregate aggregate_name
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identificare l'ID del disco per l'unità FIPS o SED da sanificare:

```
storage encryption disk show -fields data-key-id,fips-key-id,owner
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1     data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2    data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Se un disco FIPS è in esecuzione in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID 0x0 predefinito:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0
```

Info: Starting modify on 1 disk.

View the status of the operation by using the  
storage encryption disk show-status command.

## 5. Igienizzare il disco:

```
storage encryption disk sanitize -disk disk_id
```

È possibile utilizzare questo comando per sanificare solo i dischi hot spare o rotti. Per sanificare tutti i dischi, indipendentemente dal tipo, utilizzare `-force-all-state` opzione. Per la sintassi completa dei comandi, vedere la pagina `man`.



ONTAP richiede di inserire una frase di conferma prima di continuare. Inserire la frase esattamente come mostrato sullo schermo.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2
```

Warning: This operation will cryptographically sanitize 1 spare or  
broken self-encrypting disk on 1 node.

To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.

View the status of the operation using the  
storage encryption disk show-status command.

## Distruggere un disco FIPS o SED

Se si desidera rendere i dati su un'unità FIPS o SED permanentemente inaccessibili e non è necessario riutilizzarli, è possibile utilizzare `storage encryption disk destroy` comando per distruggere il disco.

### A proposito di questa attività

Quando si distrugge un disco FIPS o SED, il sistema imposta la chiave di crittografia del disco su un valore casuale sconosciuto e blocca l'unità in modo irreversibile. In questo modo, il disco risulta praticamente inutilizzabile e i dati in esso contenuti permanentemente inaccessibili. Tuttavia, è possibile ripristinare le impostazioni predefinite del disco utilizzando l'ID fisico sicuro (PSID) stampato sull'etichetta del disco. Per ulteriori informazioni, vedere ["Restituzione di un disco FIPS o SED in caso di smarrimento delle chiavi di autenticazione"](#).



Non distruggere un disco FIPS o SED a meno che non si disponga del servizio non-Returnable Disk Plus (NRD Plus). La distruzione di un disco annulla la garanzia.

## Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

## Fasi

1. Migrare tutti i dati che devono essere conservati in un aggregato su un altro disco diverso.
2. Eliminare l'aggregato sull'unità FIPS o SED da distruggere:

```
storage aggregate delete -aggregate aggregate_name
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage aggregate delete -aggregate aggr1
```

3. Identificare l'ID del disco per l'unità FIPS o SED da distruggere:

```
storage encryption disk show
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----
-----
0.0.0    data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
0.0.1    data
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
1.10.2   data
F1CB30AFF1CB30B0010100000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Distruggere il disco:

```
storage encryption disk destroy -disk disk_id
```

Per la sintassi completa dei comandi, vedere la pagina man.



Viene richiesto di inserire una frase di conferma prima di continuare. Inserire la frase esattamente come mostrato sullo schermo.

```
cluster1::> storage encryption disk destroy -disk 1.10.2
```

Warning: This operation will cryptographically destroy 1 spare or broken self-encrypting disks on 1 node.

You cannot reuse destroyed disks unless you revert them to their original state using the PSID value.

To continue, enter

destroy disk

:destroy disk

Info: Starting destroy on 1 disk.

View the status of the operation by using the "storage encryption disk show-status" command.

#### Dati di emergenza ridotti su un'unità FIPS o SED

In caso di emergenza di sicurezza, è possibile impedire immediatamente l'accesso a un disco FIPS o SED, anche se il sistema storage o il server KMIP non sono in grado di fornire alimentazione.

#### Prima di iniziare

- Se si utilizza un server KMIP privo di alimentazione, il server KMIP deve essere configurato con un elemento di autenticazione facilmente distrutto (ad esempio, una smart card o un'unità USB).
- Per eseguire questa attività, è necessario essere un amministratore del cluster.

#### Fase

1. Eseguire la cancellazione di emergenza dei dati su un disco FIPS o SED:

|       |           |
|-------|-----------|
| Se... | Quindi... |
|-------|-----------|

|                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                        |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>Il sistema di storage è alimentato e hai tempo per portare il sistema di storage offline senza problemi</p> | <ol style="list-style-type: none"> <li>Se il sistema storage è configurato come coppia ha, disattivare il Takeover.</li> <li>Portare tutti gli aggregati offline ed eliminarli.</li> <li>Impostare il livello di privilegio su Advanced:<br/> <pre>set -privilege advanced</pre> </li> <li>Se il disco è in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID predefinito:<br/> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> </li> <li>Arrestare il sistema storage.</li> <li>Avviare in modalità di manutenzione.</li> <li>Sanificare o distruggere i dischi: <ol style="list-style-type: none"> <li>Se si desidera rendere i dati sui dischi inaccessibili e continuare a riutilizzare i dischi, disinfettare i dischi:<br/> <pre>disk encrypt sanitize -all</pre> </li> <li>Se si desidera rendere i dati sui dischi inaccessibili e non è necessario salvarli, distruggere i dischi:<br/> <pre>disk encrypt destroy disk_id1 disk_id2 ...</pre> </li> </ol> </li> </ol> | <p>Il sistema storage è alimentato e i dati devono essere immediatamente sottratti</p> |
|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>a. <b>Se si desidera rendere i dati sui dischi inaccessibili e continuare a riutilizzare i dischi, eseguire la pulizia dei dischi:</b></p> <p>b. Se il sistema storage è configurato come coppia ha, disattivare il Takeover.</p> <p>c. Impostare il livello di privilegio su Advanced (avanzato):</p> <pre>set -privilege advanced</pre> <p>d. Se il disco è in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID predefinito:</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. Igienizzare il disco:</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre> | <p>a. <b>Se si desidera rendere i dati sui dischi inaccessibili e non è necessario salvarli, distruggere i dischi:</b></p> <p>b. Se il sistema storage è configurato come coppia ha, disattivare il Takeover.</p> <p>c. Impostare il livello di privilegio su Advanced (avanzato):</p> <pre>set -privilege advanced</pre> <p>d. Distruggere i dischi:</p> <pre>storage encryption disk destroy -disk * -force-all-states true</pre> | <p>Il sistema di storage esegue una panoramica, lasciando il sistema in uno stato di disattivazione permanente con tutti i dati cancellati. Per utilizzare di nuovo il sistema, è necessario riconfigurarlo.</p> |
| <p>L'alimentazione è disponibile per il server KMIP ma non per il sistema storage</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>a. Accedere al server KMIP.</p> <p>b. Distruggere tutte le chiavi associate ai dischi FIPS o ai SED che contengono i dati a cui si desidera impedire l'accesso. In questo modo si impedisce l'accesso alle chiavi di crittografia del disco da parte del sistema di storage.</p>                                                                                                                                                 | <p>L'alimentazione del server KMIP o del sistema storage non è disponibile</p>                                                                                                                                   |

Per la sintassi completa dei comandi, vedere le pagine man.

### Restituire un'unità FIPS o SED al servizio quando le chiavi di autenticazione vengono perse

Il sistema considera un'unità FIPS o SED guasta se si perdono le chiavi di autenticazione in modo permanente e non è possibile recuperarle dal server KMIP. Sebbene non sia possibile accedere o ripristinare i dati sul disco, è possibile adottare le misure necessarie

per rendere nuovamente disponibile lo spazio inutilizzato di SED per i dati.

**Prima di iniziare**

Per eseguire questa attività, è necessario essere un amministratore del cluster.

**A proposito di questa attività**

Utilizzare questo processo solo se si è certi che le chiavi di autenticazione dell'unità FIPS o SED vengano perse in modo permanente e che non sia possibile ripristinarle.

Se i dischi sono partizionati, prima di poter avviare questo processo è necessario che siano dispartizionati.



Il comando per dispartizionare un disco è disponibile solo a livello di DIAG e deve essere eseguito solo sotto la supervisione del supporto NetApp. **Si consiglia vivamente di contattare il supporto NetApp prima di procedere.** è inoltre possibile consultare l'articolo della Knowledge base ["Come dispartizionare un disco spare in ONTAP"](#).

**Fasi**

- 1. Restituire un'unità FIPS o SED al servizio:

|                   |                             |
|-------------------|-----------------------------|
| Se i SEDS sono... | Seguire questa procedura... |
|-------------------|-----------------------------|

|                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Non in modalità di compliance FIPS o in modalità di compliance FIPS e la chiave FIPS è disponibile</p> | <ol style="list-style-type: none"> <li>a. Impostare il livello di privilegio su Advanced (avanzato):<br/> <code>set -privilege advanced</code></li> <li>b. Reimpostare la chiave FIPS sull'ID protetto predefinito 0x0:<br/> <code>storage encryption disk modify -fips-key-id 0x0 -disk <i>disk_id</i></code></li> <li>c. Verificare che l'operazione sia riuscita:<br/> <code>`storage encryption disk show-status`</code> Se l'operazione non riesce, utilizzare la procedura PSID descritta in questo argomento.</li> <li>d. Sanificare il disco danneggiato:<br/> <code>storage encryption disk sanitize -disk <i>disk_id</i></code> Verificare che l'operazione sia riuscita con il comando <code>`storage encryption disk show-status`</code> prima di passare alla fase successiva.</li> <li>e. Annullare l'esecuzione di un errore sul disco crittografato:<br/> <code>storage disk unfail -spare true -disk <i>disk_id</i></code></li> <li>f. Verificare se il disco dispone di un proprietario:<br/> <code>storage disk show -disk <i>disk_id</i></code><br/><br/> Se il disco non dispone di un proprietario, assegnarne uno.<br/> <code>storage disk assign -owner node -disk <i>disk_id</i></code> <ol style="list-style-type: none"> <li>i. Immettere il nodeshell per il nodo proprietario dei dischi che si desidera disinfettare:<br/><br/> <code>system node run -node <i>node_name</i></code> </li> </ol> Eseguire <code>disk sanitize release</code> comando. </li> <li>g. Uscire dalla nodeshell. Annulla errore del disco:<br/> <code>storage disk unfail -spare true -disk <i>disk_id</i></code></li> <li>h. Verificare che il disco sia ora uno spare e pronto per essere riutilizzato in un aggregato:<br/> <code>storage disk show -disk <i>disk_id</i></code></li> </ol> |
|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



|                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>In modalità di compliance FIPS, la chiave FIPS non è disponibile e i SED hanno un PSID stampato sull'etichetta</p> | <ol style="list-style-type: none"> <li>a. Ottenere il PSID del disco dall'etichetta del disco.</li> <li>b. Impostare il livello di privilegio su Advanced (avanzato):<br/> <code>set -privilege advanced</code></li> <li>c. Ripristinare le impostazioni predefinite del disco:<br/> <code>storage encryption disk revert-to-original-state -disk <i>disk_id</i> -psid <i>disk_physical_secure_id</i></code> Verificare che l'operazione sia riuscita con il comando <code>storage encryption disk show-status</code> prima di passare alla fase successiva.</li> <li>d. Se si utilizza ONTAP 9.8P5 o versione precedente, passare alla fase successiva. Se si esegue ONTAP 9.8P6 o versione successiva, annullare la procedura di pulizia del disco.<br/> <code>storage disk unfail -disk <i>disk_id</i></code></li> <li>e. Verificare se il disco dispone di un proprietario:<br/> <code>storage disk show -disk <i>disk_id</i></code><br/><br/>           Se il disco non dispone di un proprietario, assegnarne uno.<br/> <code>storage disk assign -owner node -disk <i>disk_id</i></code><br/><br/> <ol style="list-style-type: none"> <li>i. Immettere il nodeshell per il nodo proprietario dei dischi che si desidera disinfettare:<br/><br/> <code>system node run -node <i>node_name</i></code></li> </ol>           Eseguire <code>disk sanitize release</code> comando.</li> <li>f. Uscire dalla nodeshell.. Annulla errore del disco:<br/> <code>storage disk unfail -spare true -disk <i>disk_id</i></code></li> <li>g. Verificare che il disco sia ora uno spare e pronto per essere riutilizzato in un aggregato:<br/> <code>storage disk show -disk <i>disk_id</i></code></li> </ol> |
|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Per la sintassi completa dei comandi, vedere ["riferimento al comando"](#).

### Consente di ripristinare un'unità FIPS o SED in modalità non protetta

Un'unità FIPS o SED è protetta da accessi non autorizzati solo se l'ID della chiave di autenticazione del nodo è impostato su un valore diverso da quello predefinito. È possibile ripristinare un'unità FIPS o SED in modalità non protetta utilizzando `storage encryption disk modify` Per impostare l'ID della chiave sul valore predefinito.

Se una coppia ha utilizza dischi SAS o NVMe con crittografia (SED, NSE, FIPS), è necessario seguire questa procedura per tutti i dischi all'interno della coppia ha prima di inizializzare il sistema (opzioni di avvio 4 o 9). Il mancato rispetto di questa procedura potrebbe causare la perdita di dati in futuro se i dischi vengono riutilizzati.

### Prima di iniziare

Per eseguire questa attività, è necessario essere un amministratore del cluster.

## Fasi

1. Impostare il livello di privilegio su Advanced (avanzato):

```
set -privilege advanced
```

2. Se un disco FIPS è in esecuzione in modalità di conformità FIPS, impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID 0x0 predefinito:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id 0x0
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

Confermare l'operazione con il comando:

```
storage encryption disk show-status
```

Ripetere il comando `show-status` fino a quando i numeri in "Disks incominciati" (dischi iniziati) e "Disks Done" (dischi eseguiti) non sono gli stessi.

```
cluster1:: storage encryption disk show-status
```

|          | FIPS       | Latest  | Start              |       | Execution  | Disks |   |
|----------|------------|---------|--------------------|-------|------------|-------|---|
| Disks    | Disks      |         |                    |       |            |       |   |
| Node     | Support    | Request | Timestamp          |       | Time (sec) | Begun |   |
| Done     | Successful |         |                    |       |            |       |   |
| -----    | -----      | -----   | -----              | ----- | -----      | ----- |   |
| -----    | -----      |         |                    |       |            |       |   |
| cluster1 | true       | modify  | 1/18/2022 15:29:38 | 3     |            | 14    | 5 |
| 5        |            |         |                    |       |            |       |   |

1 entry was displayed.

3. Impostare nuovamente l'ID della chiave di autenticazione dei dati per il nodo sul valore MSID 0x0 predefinito:

```
storage encryption disk modify -disk disk_id -data-key-id 0x0
```

Il valore di `-data-key-id` Deve essere impostato su 0x0 se si sta ripristinando un'unità SAS o NVMe in modalità non protetta.

È possibile utilizzare `security key-manager query` Per visualizzare gli ID chiave.

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id 0x0
```

Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.

Confermare l'operazione con il comando:

```
storage encryption disk show-status
```

Ripetere il comando show-status fino a quando i numeri non coincidono. L'operazione è completa quando i numeri in "dischi iniziati" e "dischi completati" sono gli stessi.

### Modalità di manutenzione

A partire da ONTAP 9.7, è possibile modificare la chiave di un disco FIPS dalla modalità di manutenzione. Utilizzare la modalità di manutenzione solo se non è possibile utilizzare le istruzioni dell'interfaccia utente di ONTAP descritte nella sezione precedente.

#### Fasi

1. Impostare nuovamente l'ID della chiave di autenticazione FIPS per il nodo sul valore MSID 0x0 predefinito:

```
disk encrypt rekey_fips 0x0 disklist
```

2. Impostare nuovamente l'ID della chiave di autenticazione dei dati per il nodo sul valore MSID 0x0 predefinito:

```
disk encrypt rekey 0x0 disklist
```

3. Verificare che la chiave di autenticazione FIPS sia stata reinserita correttamente:

```
disk encrypt show_fips
```

4. Confermare che la chiave di autenticazione dei dati è stata risigilitata correttamente con:

```
disk encrypt show
```

L'output visualizza probabilmente l'ID chiave MSID 0x0 predefinito o il valore di 64 caratteri posseduto dal server delle chiavi. Il `Locked?` il campo si riferisce al blocco dei dati.

| Disk    | FIPS Key ID | Locked? |
|---------|-------------|---------|
| 0a.01.0 | 0x0         | Yes     |

### Rimuovere una connessione di gestione delle chiavi esterna

È possibile scollegare un server KMIP da un nodo quando non è più necessario. Ad

esempio, è possibile scollegare un server KMIP durante la transizione alla crittografia del volume.

**A proposito di questa attività**

Quando si disconnette un server KMIP da un nodo in una coppia ha, il sistema disconnette automaticamente il server da tutti i nodi del cluster.



Se si prevede di continuare a utilizzare la gestione delle chiavi esterne dopo aver scollegato un server KMIP, assicurarsi che sia disponibile un altro server KMIP per la fornitura delle chiavi di autenticazione.

**Prima di iniziare**

Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.

**Fase**

- 1. Disconnettere un server KMIP dal nodo corrente:

| Per questa versione di ONTAP...   | Utilizzare questo comando...                                                                     |
|-----------------------------------|--------------------------------------------------------------------------------------------------|
| ONTAP 9.6 e versioni successive   | <code>`security key-manager external remove-servers -vserver SVM -key -servers host_name`</code> |
| <code>IP_address:port,...`</code> | ONTAP 9.5 e versioni precedenti                                                                  |

In un ambiente MetroCluster, è necessario ripetere questi comandi su entrambi i cluster per la SVM amministrativa.

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando ONTAP 9.6 disattiva le connessioni a due server di gestione delle chiavi esterni per `cluster1`, il primo nome `ks1`, in attesa sulla porta predefinita 5696, la seconda con l'indirizzo IP 10.0.0.20, in attesa sulla porta 24482:

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

**Modificare le proprietà del server di gestione delle chiavi esterno**

A partire da ONTAP 9.6, è possibile utilizzare `security key-manager external modify-server` Comando per modificare il timeout i/o e il nome utente di un server di gestione delle chiavi esterno.

**Prima di iniziare**

- Per eseguire questa attività, è necessario essere un amministratore del cluster o di SVM.
- Per questa attività sono richiesti privilegi avanzati.
- In un ambiente MetroCluster, è necessario ripetere questi passaggi su entrambi i cluster per la SVM amministrativa.

## Fasi

1. Sul sistema storage, passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Modificare le proprietà del server di gestione delle chiavi esterno per il cluster:

```
security key-manager external modify-server -vserver admin_SVM -key-server  
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



Il valore di timeout viene espresso in secondi. Se si modifica il nome utente, viene richiesto di inserire una nuova password. Se si esegue il comando al prompt di login del cluster, *admin\_SVM* Per impostazione predefinita, viene impostata la SVM amministrativa del cluster corrente. È necessario essere l'amministratore del cluster per modificare le proprietà del server del gestore delle chiavi esterno.

Il seguente comando modifica il valore di timeout a 45 secondi per *cluster1* server di gestione delle chiavi esterno in attesa sulla porta predefinita 5696:

```
cluster1::> security key-manager external modify-server -vserver  
cluster1 -key-server ks1.local -timeout 45
```

3. Modificare le proprietà del server di gestione delle chiavi esterne per una SVM (solo NVE):

```
security key-manager external modify-server -vserver SVM -key-server  
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



Il valore di timeout viene espresso in secondi. Se si modifica il nome utente, viene richiesto di inserire una nuova password. Se si esegue il comando al prompt di accesso SVM, *SVM* Per impostazione predefinita, viene impostata la SVM corrente. Per modificare le proprietà del server del gestore delle chiavi esterno, è necessario essere l'amministratore del cluster o SVM.

Il seguente comando consente di modificare il nome utente e la password di *svm1* server di gestione delle chiavi esterno in attesa sulla porta predefinita 5696:

```
svm1::> security key-manager external modify-server -vserver svm11 -key  
-server ks1.local -username svm1user  
Enter the password:  
Reenter the password:
```

4. Ripetere l'ultimo passaggio per eventuali SVM aggiuntive.

## Transizione alla gestione esterna delle chiavi dalla gestione integrata delle chiavi

Se si desidera passare alla gestione esterna delle chiavi dalla gestione integrata delle chiavi, è necessario eliminare la configurazione di gestione integrata delle chiavi prima di attivare la gestione esterna delle chiavi.

## Prima di iniziare

- Per la crittografia basata su hardware, è necessario ripristinare il valore predefinito delle chiavi dati di tutti i dischi FIPS o SED.

["Ripristino di un'unità FIPS o SED in modalità non protetta"](#)

- Per la crittografia basata su software, è necessario annullare la crittografia di tutti i volumi.

["Annullamento della crittografia dei dati del volume"](#)

- Per eseguire questa attività, è necessario essere un amministratore del cluster.

## Fase

1. Eliminare la configurazione di gestione delle chiavi integrata per un cluster:

| Per questa versione di ONTAP... | Utilizzare questo comando...                                   |
|---------------------------------|----------------------------------------------------------------|
| ONTAP 9.6 e versioni successive | <code>security key-manager onboard disable -vserver SVM</code> |
| ONTAP 9.5 e versioni precedenti | <code>security key-manager delete-key-database</code>          |

Per la sintassi completa dei comandi, vedere ["Pagine di manuale di ONTAP"](#).

## Transizione alla gestione delle chiavi integrata dalla gestione esterna delle chiavi

Se si desidera passare alla gestione delle chiavi integrata dalla gestione delle chiavi esterna, è necessario eliminare la configurazione di gestione delle chiavi esterne prima di poter attivare la gestione delle chiavi integrata.

## Prima di iniziare

- Per la crittografia basata su hardware, è necessario ripristinare il valore predefinito delle chiavi dati di tutti i dischi FIPS o SED.

["Ripristino di un'unità FIPS o SED in modalità non protetta"](#)

- È necessario eliminare tutte le connessioni di gestione delle chiavi esterne.

["Eliminazione di una connessione di gestione delle chiavi esterna"](#)

- Per eseguire questa attività, è necessario essere un amministratore del cluster.

## Procedura

I passaggi necessari per eseguire la transizione della gestione delle chiavi dipendono dalla versione di ONTAP in uso.

### ONTAP 9.6 e versioni successive

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Utilizzare il comando:

```
security key-manager external disable -vserver admin_SVM
```



In un ambiente MetroCluster, è necessario ripetere il comando su entrambi i cluster per la SVM amministrativa.

### ONTAP 9.5 e versioni precedenti

Utilizzare il comando:

```
security key-manager delete-kmip-config
```

### Cosa accade quando i server di gestione delle chiavi non sono raggiungibili durante il processo di avvio

ONTAP prende alcune precauzioni per evitare comportamenti indesiderati nel caso in cui un sistema storage configurato per NSE non riesca a raggiungere nessuno dei server di gestione delle chiavi specificati durante il processo di avvio.

Se il sistema di storage è configurato per NSE, i SED vengono ridigitati e bloccati e i SED sono accesi, il sistema di storage deve recuperare le chiavi di autenticazione richieste dai server di gestione delle chiavi per autenticarsi ai SED prima di poter accedere ai dati.

Il sistema storage tenta di contattare i server di gestione delle chiavi specificati per un massimo di tre ore. Se il sistema storage non riesce a raggiungerne uno dopo tale periodo, il processo di avvio si interrompe e il sistema storage si arresta.

Se il sistema di storage contatta correttamente qualsiasi server di gestione delle chiavi specificato, tenta di stabilire una connessione SSL per un massimo di 15 minuti. Se il sistema di storage non riesce a stabilire una connessione SSL con un server di gestione delle chiavi specificato, il processo di avvio si interrompe e il sistema di storage si arresta.

Mentre il sistema di storage tenta di contattare e connettersi ai server di gestione delle chiavi, visualizza informazioni dettagliate sui tentativi di contatto non riusciti alla CLI. È possibile interrompere i tentativi di contatto in qualsiasi momento premendo Ctrl-C.

Come misura di sicurezza, i SED consentono solo un numero limitato di tentativi di accesso non autorizzati, dopodiché disattivano l'accesso ai dati esistenti. Se il sistema di storage non riesce a contattare alcun server di gestione delle chiavi specificato per ottenere le chiavi di autenticazione appropriate, può solo tentare di autenticare con la chiave predefinita, il che causa un tentativo di errore e un panico. Se il sistema di storage è configurato per il riavvio automatico in caso di panico, entra in un loop di avvio che porta a tentativi di autenticazione non riusciti continui sui SED.

L'arresto del sistema storage in questi scenari è progettato per impedire al sistema storage di entrare in un loop di avvio e di perdere dati non intenzionale come conseguenza del blocco permanente dei SED dovuto al superamento del limite di sicurezza di un certo numero di tentativi di autenticazione consecutivi non riusciti. Il limite e il tipo di protezione di blocco dipendono dalle specifiche di produzione e dal tipo di SED:

| TIPO SED                                                                   | Numero di tentativi consecutivi di autenticazione non riusciti che hanno determinato il blocco | Tipo di protezione di blocco quando viene raggiunto il limite di sicurezza                                                             |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| DISCO RIGIDO                                                               | 1024                                                                                           | Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile. |
| X440_PHM2800 MCTO SSD NSE da 800 GB con revisioni del firmware NA00 o NA01 | 5                                                                                              | Temporaneo. Il blocco è valido solo fino a quando il disco non viene spento e riacceso.                                                |
| X577_PHM2800 MCTO SSD NSE da 800 GB con revisioni del firmware NA00 o NA01 | 5                                                                                              | Temporaneo. Il blocco è valido solo fino a quando il disco non viene spento e riacceso.                                                |
| X440_PHM2800MCTO SSD NSE da 800 GB con revisioni del firmware superiori    | 1024                                                                                           | Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile. |
| X577_PHM2800MCTO SSD NSE da 800 GB con revisioni del firmware superiori    | 1024                                                                                           | Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile. |
| Tutti gli altri modelli di SSD                                             | 1024                                                                                           | Permanente. I dati non possono essere recuperati, anche quando la chiave di autenticazione appropriata diventa nuovamente disponibile. |

Per tutti i tipi SED, un'autenticazione corretta azzerà il numero di proy.

Se si verifica questo scenario in cui il sistema storage viene arrestato a causa di un errore di accesso a uno dei server di gestione delle chiavi specificati, prima di continuare l'avvio del sistema storage è necessario identificare e correggere la causa dell'errore di comunicazione.

### **Disattivare la crittografia per impostazione predefinita**

A partire da ONTAP 9.7, la crittografia aggregata e del volume è attivata per impostazione predefinita se si dispone di una licenza di crittografia del volume (VE) e si utilizza un gestore di chiavi integrato o esterno. Se necessario, è possibile disattivare la crittografia per impostazione predefinita per l'intero cluster.

#### **Prima di iniziare**

Per eseguire questa attività, è necessario essere un amministratore del cluster o un amministratore SVM al quale l'amministratore del cluster ha delegato l'autorità.

#### **Fase**



1. Per disattivare la crittografia per impostazione predefinita per l'intero cluster in ONTAP 9.7 o versioni successive, eseguire il seguente comando:

```
options -option-name encryption.data_at_rest_encryption.disable_by_default  
-option-value on
```

# Protezione dei dati e disaster recovery

## Protezione dei dati con System Manager

### Panoramica sulla protezione dei dati con System Manager

Gli argomenti di questa sezione illustrano come configurare e gestire la protezione dei dati con Gestione di sistema in ONTAP 9.7 e versioni successive.

Se si utilizza Gestione sistema in ONTAP 9.7 o versioni precedenti, vedere ["Documentazione classica di Gestore di sistema ONTAP"](#)

Proteggi i tuoi dati creando e gestendo copie Snapshot, mirror, vault e relazioni mirror-and-vault.

*SnapMirror* è una tecnologia di disaster recovery progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. Come suggerisce il nome, SnapMirror crea una replica, o mirror, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di disastro nel sito primario.

Un *vault* è progettato per la replica delle copie Snapshot disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. A differenza di una relazione SnapMirror, in cui la destinazione contiene di solito solo le copie Snapshot attualmente nel volume di origine, una destinazione del vault conserva in genere le copie Snapshot point-in-time create in un periodo molto più lungo.

A partire da ONTAP 9.10.1, è possibile creare relazioni di protezione dei dati tra i bucket S3 utilizzando S3 SnapMirror. I bucket di destinazione possono essere su sistemi ONTAP locali o remoti o su sistemi non ONTAP come StorageGRID e AWS. Per ulteriori informazioni, vedere ["Panoramica di S3 SnapMirror"](#).

### Creare policy di protezione dei dati personalizzate

È possibile creare policy di protezione dei dati personalizzate con System Manager quando le policy di protezione predefinite esistenti non sono adatte alle proprie esigenze. A partire da ONTAP 9.11.1, è possibile utilizzare Gestore di sistema per creare policy personalizzate di mirroring e vault, per visualizzare e selezionare policy legacy. Questa funzionalità è disponibile anche in ONTAP 9.8P12 e nelle patch successive di ONTAP 9.8.

Creare policy di protezione personalizzate sul cluster di origine e di destinazione.

#### Fasi

1. Fare clic su **Protection > Local Policy Settings** (protezione > Impostazioni policy locali).
2. Nella sezione **Criteri di protezione**, fare clic su ➔.
3. Nel riquadro **Criteri di protezione**, fare clic su + Add.
4. Inserire il nuovo nome del criterio e selezionare l'ambito del criterio.
5. Scegliere un tipo di policy. Per aggiungere una policy di solo vault o solo mirror, scegliere **Asynchronous** e fare clic su **Usa un tipo di policy legacy**.
6. Compilare i campi obbligatori.
7. Fare clic su **Save** (Salva).

8. Ripetere questi passaggi sull'altro cluster.

## Configurare le copie Snapshot

È possibile creare policy di copia Snapshot per specificare il numero massimo di copie Snapshot create automaticamente e la frequenza di creazione. Il criterio specifica quando creare copie Snapshot, quante copie conservare e come assegnarle un nome.

Questa procedura crea un criterio di copia Snapshot solo sul cluster locale.

### Fasi

1. Fare clic su **protezione > Panoramica > Impostazioni policy locali**.
2. In **Snapshot Policies**, fare clic su ➔, quindi fare clic su **+ Add**.
3. Digitare il nome del criterio, selezionare l'ambito del criterio e in **Pianificazioni**, fare clic su **+ Add** per inserire i dettagli della pianificazione.

## Calcola lo spazio recuperabile prima di eliminare le copie Snapshot

A partire da ONTAP 9.10.1, è possibile utilizzare Gestore di sistema per selezionare le copie Snapshot che si desidera eliminare e calcolare lo spazio recuperabile prima di eliminarle.

### Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare il volume dal quale si desidera eliminare le copie Snapshot.
3. Fare clic su **copie Snapshot**.
4. Selezionare una o più copie Snapshot.
5. Fare clic su **Calcola spazio recuperabile**.

## Attivare o disattivare l'accesso del client alla directory di copia Snapshot

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per attivare o disattivare i sistemi client per accedere a una directory di copia Snapshot su un volume. L'abilitazione dell'accesso rende la directory di copia Snapshot visibile ai client e consente ai client Windows di mappare un disco alla directory Snapshot Copies per visualizzarne e accedervi.


È possibile attivare o disattivare l'accesso alla directory di copia Snapshot di un volume modificando le impostazioni del volume o le impostazioni di condivisione del volume.

### Abilitare o disabilitare l'accesso del client alla directory di copia Snapshot modificando un volume

Per impostazione predefinita, la directory di copia Snapshot di un volume è accessibile ai client.

### Fasi


1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare il volume contenente la directory Snapshot Copies che si desidera visualizzare o nascondere.

3. Fare clic su  E selezionare **Modifica**.
4. Nella sezione **Snapshot Copies (Local) Settings**, selezionare o deselezionare **Show the Snapshot Copies directory to clients** (Mostra la directory Snapshot Copies ai client).
5. Fare clic su **Save** (Salva).

### Abilitare o disabilitare l'accesso del client alla directory di copia Snapshot modificando una condivisione

Per impostazione predefinita, la directory di copia Snapshot di un volume è accessibile ai client.

#### Fasi

1. Fare clic su **Storage > Shares**.
2. Selezionare il volume contenente la directory Snapshot Copies che si desidera visualizzare o nascondere.
3. Fare clic su  E selezionare **Modifica**.
4. Nella sezione **Proprietà condivisione**, selezionare o deselezionare **Consenti ai client di accedere alla directory Snapshot Copies**.
5. Fare clic su **Save** (Salva).



### Preparazione per il mirroring e il vaulting


È possibile proteggere i dati replicandoli in un cluster remoto per il backup dei dati e il disaster recovery.

Sono disponibili diversi criteri di protezione predefiniti. Se si desidera utilizzare policy personalizzate, è necessario aver creato le policy di protezione.



#### Fasi

1. Nel cluster locale, fare clic su **protezione > Panoramica**.
2. Espandere **Impostazioni Intercluster**. Fare clic su **Add Network Interfaces** (Aggiungi interfacce di rete) e aggiungere interfacce di rete intercluster per il cluster.  
  
Ripetere questo passaggio sul cluster remoto.
3. Nel cluster remoto, fare clic su **protezione > Panoramica**. Fare clic su  Nella sezione Cluster Peers (peer cluster), fare clic su **generate Passphrase** (genera passphrase)
4. Copiare la passphrase generata e incollarla nel cluster locale.
5. Nel cluster locale, in Cluster Peers, fare clic su **Peer Clusters** e eseguire il peer dei cluster locali e remoti.
6. In alternativa, sotto Storage VM Peers, fare clic su  E poi **Peer Storage VM** per eseguire il peer delle VM di storage.
7. Fare clic su **Protect Volumes** (Proteggi volumi) per proteggere i volumi. Per proteggere i LUN, fare clic su

**Storage > LUN**, selezionare un LUN da proteggere, quindi fare clic su  **Protect**.

Selezionare la policy di protezione in base al tipo di protezione dei dati desiderata.

8. Per verificare che i volumi e le LUN siano protetti correttamente dal cluster locale, fare clic su **Storage > Volumes** o **Storage > LUN** e espandere la vista volume/LUN.

### Altri modi per farlo in ONTAP

| Per eseguire queste attività con...                                      | Guarda questo contenuto...                                                       |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti) | <a href="#">"Panoramica sulla preparazione del disaster recovery dei volumi"</a> |
| L'interfaccia della riga di comando di ONTAP                             | <a href="#">"Creare una relazione peer del cluster"</a>                          |

## Configurare mirror e vault

Creare un mirror e un vault di un volume per proteggere i dati in caso di disastro e avere più versioni archiviate dei dati su cui eseguire il rollback. A partire da ONTAP 9.11.1, è possibile utilizzare Gestione sistema per selezionare policy di vault e mirror pre-create e personalizzate, per visualizzare e selezionare policy legacy e per ignorare le pianificazioni di trasferimento definite in una policy di protezione quando si proteggono volumi e macchine virtuali di storage. Questa funzionalità è disponibile anche in ONTAP 9.8P12 e nelle patch successive di ONTAP 9.8.




Se si utilizza ONTAP 9.8P12 o versione successiva della patch per ONTAP 9.8 e si configura SnapMirror utilizzando Gestione di sistema, è necessario utilizzare ONTAP 9.9.1P13 o versione successiva e ONTAP 9.10.1P10 o versioni successive se si intende eseguire l'aggiornamento a ONTAP 9.9.1 o ONTAP 9.10.1.

Questa procedura crea un criterio di protezione dei dati su un cluster remoto. Il cluster di origine e il cluster di destinazione utilizzano interfacce di rete intercluster per lo scambio di dati. La procedura presuppone ["vengono create le interfacce di rete tra cluster e i cluster contenenti i volumi vengono peering"](#) (accoppiato). È inoltre possibile eseguire il peer delle macchine virtuali storage per la protezione dei dati; tuttavia, se le macchine virtuali storage non sono in peering, ma le autorizzazioni sono attivate, le macchine virtuali storage vengono automaticamente messe in peering quando viene creata la relazione di protezione.



### Fasi

1. Selezionare il volume o il LUN da proteggere: Fare clic su **Storage > Volumes** o **Storage > LUN**, quindi fare clic sul nome del volume o del LUN desiderato.
2. Fare clic su  **Protect**.
3. Selezionare il cluster di destinazione e la VM di storage.
4. Il criterio asincrono viene selezionato per impostazione predefinita. Per selezionare un criterio sincrono, fare clic su **altre opzioni**.

5. Fare clic su **Protect** (protezione).
6. Fare clic sulla scheda **SnapMirror (locale o remoto)** del volume o LUN selezionato per verificare che la protezione sia impostata correttamente.

#### Informazioni correlate

- ["Creazione ed eliminazione di volumi di test del failover SnapMirror"](#).

#### Altri modi per farlo in ONTAP


| Per eseguire queste attività con...                                      | Guarda questo contenuto...                                       |
|--------------------------------------------------------------------------|------------------------------------------------------------------|
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti) | <a href="#">"Panoramica del backup del volume con SnapVault"</a> |
| L'interfaccia della riga di comando di ONTAP                             | <a href="#">"Creare una relazione di replica"</a>                |

## Risincronizzare una relazione di protezione

Quando il volume di origine è nuovamente disponibile dopo un disastro, è possibile risincronizzare i dati dal volume di destinazione e ristabilire la relazione di protezione.

Questa procedura sostituisce i dati nel volume di origine originale in una relazione asincrona, in modo da poter iniziare nuovamente a servire i dati dal volume di origine e riprendere la relazione di protezione originale.

#### Fasi


1. Fare clic su **protezione > Relazioni**, quindi sulla relazione interrotta che si desidera risincronizzare.
2. Fare clic su  Quindi selezionare **Resync**.
3. In **Relazioni**, monitorare l'avanzamento della risincronizzazione controllando lo stato della relazione. Lo stato diventa "mirrored" al termine della risincronizzazione.

## Ripristinare un volume da una copia Snapshot precedente

In caso di perdita o danneggiamento dei dati in un volume, è possibile eseguire il rollback dei dati eseguendo il ripristino da una copia Snapshot precedente.

Questa procedura sostituisce i dati correnti sul volume di origine con i dati di una versione di copia Snapshot precedente. Eseguire questa attività sul cluster di destinazione.

#### Fasi

1. Fare clic su **protezione > Relazioni**, quindi fare clic sul nome del volume di origine.
2. Fare clic su  Quindi selezionare **Ripristina**.
3. In **Source** (origine), il volume di origine viene selezionato per impostazione predefinita. Fare clic su **Other Volume** (Altro volume) se si desidera scegliere un volume diverso dall'origine.
4. In **destinazione**, scegliere la copia Snapshot che si desidera ripristinare.
5. Se l'origine e la destinazione si trovano in cluster diversi, sul cluster remoto fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

## Altri modi per farlo in ONTAP


| Per eseguire queste attività con...                                      | Guarda questo contenuto...                                                              |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti) | <a href="#">"Panoramica del ripristino del volume con SnapVault"</a>                    |
| L'interfaccia della riga di comando di ONTAP                             | <a href="#">"Ripristinare il contenuto di un volume da una destinazione SnapMirror"</a> |

## Ripristino da copie Snapshot

È possibile ripristinare un volume a un punto precedente eseguendo il ripristino da una copia Snapshot.

Questa procedura ripristina un volume da una copia Snapshot.

### Fasi


1. Fare clic su **Storage** e selezionare un volume.
2. In **Snapshot Copies**, fare clic su  Accanto alla copia Snapshot che si desidera ripristinare e selezionare **Restore** (Ripristina).

## Ripristinare su un nuovo volume

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per ripristinare i dati di backup sul volume di destinazione su un volume diverso dall'origine originale.

Quando si esegue il ripristino su un volume diverso, è possibile selezionare un volume esistente o crearne uno nuovo.

### Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Fare clic su  E fare clic su **Restore**.
3. Nella sezione **origine**, selezionare **Altro volume** e selezionare il cluster e la Storage VM.
4. Selezionare **Existing volume** (volume esistente) o **Create a new volume** (Crea nuovo volume).
5. Se si sta creando un nuovo volume, immettere il nome del volume.
6. Nella sezione **destinazione**, selezionare la copia Snapshot da ripristinare.
7. Fare clic su **Save** (Salva).
8. In **Relazioni**, monitorare l'avanzamento del ripristino visualizzando **Stato trasferimento** per la relazione.

## Risincronizzazione inversa di una relazione di protezione

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per eseguire un'operazione di risincronizzazione inversa per eliminare una relazione di protezione esistente e invertire le funzioni dei volumi di origine e di destinazione. Quindi si utilizza il volume di destinazione per fornire i dati durante la riparazione o la sostituzione dell'origine, l'aggiornamento dell'origine e il ripristino della configurazione originale dei sistemi.



System Manager non supporta la risincronizzazione inversa con relazioni intracluster. È possibile utilizzare l'interfaccia utente di ONTAP per eseguire operazioni di risincronizzazione inversa con relazioni intracluster.

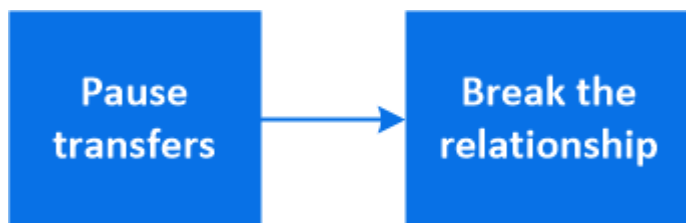
Quando si esegue un'operazione di risincronizzazione inversa, tutti i dati sul volume di origine più recenti dei dati nella copia Snapshot comune vengono cancellati.

#### Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Fare clic su E fare clic su **Reverse Resync**.
3. In **Relazioni**, monitorare l'avanzamento della risincronizzazione inversa visualizzando **Stato trasferimento** per la relazione.

### Fornire i dati da una destinazione SnapMirror

Per fornire dati da una destinazione mirror quando un'origine non è disponibile, interrompere i trasferimenti pianificati verso la destinazione, quindi interrompere la relazione SnapMirror per rendere la destinazione scrivibile.



#### Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**, quindi fare clic sul nome del volume desiderato.
2. Fare clic su .
3. Stop scheduled transfer (Interrompi trasferimenti pianificati): Fare clic su **Pause**
4. Rendere scrivibile la destinazione: Fare clic su **Interrompi**.
5. Andare alla pagina principale **Relazioni** per verificare che lo stato della relazione sia visualizzato come "interrotto".

#### Fasi successive:

Quando il volume di origine disattivato è nuovamente disponibile, è necessario risincronizzare la relazione per copiare i dati correnti nel volume di origine originale. Questo processo sostituisce i dati sul volume di origine originale.

#### Altri modi per farlo in ONTAP

| Per eseguire queste attività con...                                      | Guarda questo contenuto...                                    |
|--------------------------------------------------------------------------|---------------------------------------------------------------|
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti) | <a href="#">"Panoramica sul disaster recovery dei volumi"</a> |
| L'interfaccia della riga di comando di ONTAP                             | <a href="#">"Attivare il volume di destinazione"</a>          |



## Configurare il disaster recovery delle macchine virtuali dello storage

Con System Manager, è possibile creare una relazione di disaster recovery per le macchine virtuali di storage (DR per le macchine virtuali di storage) per replicare una configurazione delle macchine virtuali di storage in un'altra. In caso di disastro nel sito primario, è possibile attivare rapidamente la VM di storage di destinazione.

Completare questa procedura dalla destinazione. Se è necessario creare un nuovo criterio di protezione, ad esempio, quando la VM dello storage di origine ha SMB configurato, è necessario utilizzare System Manager per creare il criterio e selezionare l'opzione **Identity Preserve** nella finestra **Add Protection Policy**. Per ulteriori informazioni, vedere ["Creare policy di protezione dei dati personalizzate"](#).



### Fasi

1. Nel cluster di destinazione, fare clic su **protezione > Relazioni**.
2. In **Relazioni**, fare clic su Proteggi e scegliere **Storage VM (DR)**.
3. Selezionare un criterio di protezione. Se è stato creato un criterio di protezione personalizzato, selezionarlo, quindi scegliere il cluster di origine e la VM di storage che si desidera replicare. È inoltre possibile creare una nuova VM di storage di destinazione immettendo un nuovo nome per la VM di storage.
4. Fare clic su **Save** (Salva).

## Fornire i dati da una destinazione DR SVM

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per attivare una VM di storage di destinazione dopo un disastro. L'attivazione della VM di storage di destinazione rende i volumi di destinazione SVM scrivibili e consente di inviare i dati ai client.

### Fasi

1. Se il cluster di origine è accessibile, verificare che SVM sia stato arrestato: Selezionare **Storage > Storage VM** e selezionare la colonna **state** per SVM.
2. Se lo stato SVM di origine è "in esecuzione", interromperlo: Selezionare  E scegliere **Stop**.
3. Sul cluster di destinazione, individuare la relazione di protezione desiderata: Accedere a **protezione > Relazioni**.
4. Fare clic su  E scegliere **Activate Destination Storage VM**.

## Riattivare una VM di storage di origine

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per riattivare una VM di storage di origine dopo un disastro. La riattivazione della VM di storage di origine interrompe la VM di storage di destinazione e riattiva la replica dall'origine alla destinazione.

### A proposito di questa attività


Quando si riattiva la VM dello storage di origine, System Manager esegue le seguenti operazioni in background:

- Crea una relazione DR SVM inversa dalla destinazione originale all'origine utilizzando la risincronizzazione

di SnapMirror

- Arresta la SVM di destinazione
- Aggiorna la relazione di SnapMirror
- Interrompe la relazione di SnapMirror
- Riavvia la SVM originale
- Effettua una risincronizzazione di SnapMirror dell'origine originale verso la destinazione originale
- Elimina le relazioni di SnapMirror

#### Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Fare clic su  E fare clic su **Riattiva VM storage di origine**.
3. In **Relazioni**, monitorare l'avanzamento della riattivazione dell'origine visualizzando **Stato trasferimento** per la relazione di protezione.


### Risincronizzare una VM di storage di destinazione

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per risincronizzare i dati e i dettagli di configurazione dalla VM di storage di origine alla VM di storage di destinazione in una relazione di protezione interrotta e ristabilire la relazione.

ONTAP 9.11.1 introduce un'opzione per evitare la ricostruzione completa del data warehouse quando si esegue una prova di disaster recovery, consentendo di tornare più rapidamente alla produzione.

L'operazione di risincronizzazione viene eseguita solo dalla destinazione della relazione originale. La risincronizzazione elimina tutti i dati nella VM di storage di destinazione più recenti dei dati nella VM di storage di origine.

#### Fasi

1. Selezionare la relazione di protezione desiderata: Fare clic su **protezione > Relazioni**.
2. Facoltativamente, selezionare **Perform a quick resync** (Esegui una risincronizzazione rapida) per ignorare la ricostruzione completa del data warehouse durante una prova di disaster recovery.
3. Fare clic su  E fare clic su **Resync**.
4. In **Relazioni**, monitorare l'avanzamento della risincronizzazione visualizzando **Stato trasferimento** per la relazione.

### Eseguire il backup dei dati nel cloud utilizzando SnapMirror

A partire da ONTAP 9.9.1, puoi eseguire il backup dei dati nel cloud e ripristinare i dati dal cloud storage a un volume diverso utilizzando Gestione di sistema. Puoi utilizzare StorageGRID o ONTAP S3 come archivio di oggetti cloud.

Prima di utilizzare la funzione SnapMirror Cloud, è necessario richiedere una chiave di licenza API di SnapMirror Cloud al sito di supporto NetApp: ["Richiedere la chiave di licenza API di SnapMirror Cloud"](#). Seguendo le istruzioni, fornisci una semplice descrizione dell'opportunità di business e richiedi la chiave API inviando un'email all'indirizzo email fornito. Entro 24 ore riceverai una risposta via email con ulteriori istruzioni su come acquisire la chiave API.

## Aggiungere un archivio di oggetti cloud

Prima di configurare i backup di SnapMirror Cloud, è necessario aggiungere un archivio di oggetti cloud StorageGRID o ONTAP S3.

### Fasi

1. Fare clic su **protezione > Panoramica > Cloud Object Stores**.
2. Fare clic su **+ Add**.

## Eseguire il backup utilizzando il criterio predefinito

È possibile configurare rapidamente un backup di SnapMirror Cloud per un volume esistente utilizzando la policy di protezione cloud predefinita, DailyBackup.

### Fasi

1. Fare clic su **protezione > Panoramica** e selezionare **Backup dei volumi nel cloud**.
2. Se è la prima volta che si esegue il backup nel cloud, inserire la chiave di licenza API di SnapMirror Cloud nel campo della licenza, come indicato.
3. Fare clic su **Authenticate and Continue** (autentica e continua)
4. Selezionare un volume di origine.
5. Selezionare un archivio di oggetti cloud.
6. Fare clic su **Save** (Salva).

## Creare una policy di backup cloud personalizzata

Se non si desidera utilizzare la policy cloud predefinita di DailyBackup per i backup di SnapMirror Cloud, è possibile creare una policy personalizzata.

### Fasi

1. Fare clic su **protezione > Panoramica > Impostazioni policy locali** e selezionare **Criteri di protezione**.
2. Fare clic su **Add** (Aggiungi) e inserire i nuovi dettagli della policy.
3. Nella sezione **Policy Type**, selezionare **Backup to Cloud** per indicare che si sta creando una policy cloud.
4. Fare clic su **Save** (Salva).

## Creare un backup dalla pagina volumi

È possibile utilizzare la pagina System Manager **Volumes** per selezionare e creare backup cloud per più volumi contemporaneamente o quando si desidera utilizzare una policy di protezione personalizzata.

### Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare i volumi di cui si desidera eseguire il backup nel cloud e fare clic su **Protect**.
3. Nella finestra **Protect Volume** (Proteggi volume), fare clic su **More Options** (altre opzioni).
4. Selezionare un criterio.

È possibile selezionare il criterio predefinito, DailyBackup o un criterio cloud personalizzato creato.


5. Selezionare un archivio di oggetti cloud.

6. Fare clic su **Save** (Salva).

## Eseguire il ripristino dal cloud

È possibile utilizzare System Manager per ripristinare i dati di backup dallo storage cloud a un volume diverso nel cluster di origine.


### Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Selezionare la scheda **Backup nel cloud**.
3. Fare clic su  Accanto al volume di origine che si desidera ripristinare e selezionare **Restore** (Ripristina).
4. In **Source** (origine), selezionare una VM di storage e immettere il nome del volume in cui si desidera ripristinare i dati.
5. In **destinazione**, selezionare la copia Snapshot che si desidera ripristinare.
6. Fare clic su **Save** (Salva).

## Eliminare una relazione SnapMirror Cloud

È possibile utilizzare System Manager per eliminare una relazione cloud.


### Fasi

1. Fare clic su **Storage > Volumes** (archiviazione > volumi) e selezionare il volume che si desidera eliminare.
2. Fare clic su  Accanto al volume di origine e selezionare **Delete** (Elimina).
3. Selezionare **Delete the cloud object store endpoint (opzionale)** se si desidera eliminare l'endpoint dell'archivio di oggetti cloud.
4. Fare clic su **Delete** (Elimina).

## Rimuovere un archivio di oggetti cloud

È possibile utilizzare System Manager per rimuovere un archivio di oggetti cloud se non fa parte di una relazione di backup cloud. Quando un archivio di oggetti cloud fa parte di una relazione di backup cloud, non può essere cancellato.

### Fasi

1. Fare clic su **protezione > Panoramica > Cloud Object Stores**.
2. Selezionare l'archivio di oggetti che si desidera eliminare, quindi fare clic su  E selezionare **Delete** (Elimina).

## Eseguire il backup dei dati utilizzando Cloud Backup

A partire da ONTAP 9.9.1, puoi utilizzare Gestione sistema per eseguire il backup dei dati nel cloud utilizzando il backup nel cloud.



Cloud Backup supporta volumi di lettura/scrittura FlexVol e volumi di protezione dei dati (DP). I volumi FlexGroup e SnapLock non sono supportati.

### Prima di iniziare

Per creare un account in BlueXP, attenersi alle seguenti procedure. Per l'account di servizio, è necessario

creare il ruolo di "account Admin". (Gli altri ruoli dell'account di servizio non dispongono dei privilegi necessari per stabilire una connessione da System Manager).

1. "Creare un account in BlueXP".
2. "Creare un connettore in BlueXP" con uno dei seguenti cloud provider:
  - Microsoft Azure
  - Amazon Web Services (AWS)
  - Piattaforma Google Cloud (GCP)
  - StorageGRID (ONTAP 9.10.1)



A partire da ONTAP 9.10.1, è possibile selezionare StorageGRID come provider di backup cloud, ma solo se BlueXP è implementato on-premise. BlueXP Connector deve essere installato on-premise e disponibile tramite l'applicazione Software-as-a-Service (SaaS) BlueXP.

3. "Iscriviti a Cloud Backup Service in BlueXP" (richiede la licenza appropriata).
4. "Generare una chiave di accesso e una chiave segreta utilizzando BlueXP".

## Registrare il cluster con BlueXP

È possibile registrare il cluster con BlueXP utilizzando BlueXP o System Manager.

### Fasi

1. In System Manager, accedere a **Panoramica sulla protezione**.
2. In **Cloud Backup Service**, fornire i seguenti dettagli:
  - ID client
  - Chiave segreta del client
3. Selezionare **Registra e continua**.

## Attiva Cloud Backup

Una volta registrato il cluster con BlueXP, è necessario attivare Cloud Backup e avviare il primo backup nel cloud.

### Fasi

1. In Gestione sistema, fare clic su **protezione > Panoramica**, quindi scorrere fino alla sezione **Cloud Backup Service**.
2. Inserire **ID client** e **Segreto client**.



A partire da ONTAP 9.10.1, puoi scoprire il costo dell'utilizzo del cloud facendo clic su **ulteriori informazioni sul costo dell'utilizzo del cloud**.

3. Fare clic su **Connetti e attiva Cloud Backup Service**.
4. Nella pagina **Enable Cloud Backup Service** (attiva protocollo), fornire i seguenti dettagli, a seconda del provider selezionato.

|                              |                             |
|------------------------------|-----------------------------|
| Per questo cloud provider... | Inserire i seguenti dati... |
|------------------------------|-----------------------------|

|                                                                                                    |                                                                                                                                                                                       |
|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure                                                                                              | <ul style="list-style-type: none"> <li>• ID abbonamento Azure</li> <li>• Regione</li> <li>• Nome del gruppo di risorse (esistente o nuovo)</li> </ul>                                 |
| AWS                                                                                                | <ul style="list-style-type: none"> <li>• ID account AWS</li> <li>• Tasto di accesso</li> <li>• Chiave segreta</li> <li>• Regione</li> </ul>                                           |
| Google Cloud Project (GCP)                                                                         | <ul style="list-style-type: none"> <li>• Nome del progetto Google Cloud</li> <li>• Chiave Google Cloud Access</li> <li>• Chiave segreta di Google Cloud</li> <li>• Regione</li> </ul> |
| StorageGRID (ONTAP 9.10.1 e versioni successive e solo per l'implementazione on-premise di BlueXP) | <ul style="list-style-type: none"> <li>• Server</li> <li>• Chiave di accesso SG</li> <li>• Chiave segreta SG</li> </ul>                                                               |

5. Selezionare una **policy di protezione**:

- **Policy esistente**: Scegliere una policy esistente.
- **New Policy**: Specificare un nome e impostare una pianificazione di trasferimento.



A partire da ONTAP 9.10.1, è possibile specificare se si desidera attivare l'archiviazione con Azure o AWS.



Se si attiva l'archiviazione per un volume con Azure o AWS, non è possibile disattivarla.

Se si abilita l'archiviazione per Azure o AWS, specificare quanto segue:

- Il numero di giorni trascorsi i quali il volume viene archiviato.
- Il numero di backup da conservare nell'archivio. Specificare "0" (zero) per archiviare fino all'ultimo backup.
- Per AWS, selezionare la classe di storage di archiviazione.

6. Selezionare i volumi di cui si desidera eseguire il backup.

7. Selezionare **Salva**.

## Modificare il criterio di protezione utilizzato per Cloud Backup

È possibile modificare i criteri di protezione utilizzati con Cloud Backup.

### Fasi

1. In Gestione sistema, fare clic su **protezione > Panoramica**, quindi scorrere fino alla sezione **Cloud Backup Service**.

2. Fare clic su , Quindi **Modifica**.

3. Selezionare una **policy di protezione**:

- **Policy esistente**: Scegliere una policy esistente.
- **New Policy**: Specificare un nome e impostare una pianificazione di trasferimento.



A partire da ONTAP 9.10.1, è possibile specificare se si desidera attivare l'archiviazione con Azure o AWS.



Se si attiva l'archiviazione per un volume con Azure o AWS, non è possibile disattivarla.

Se si abilita l'archiviazione per Azure o AWS, specificare quanto segue:

- Il numero di giorni trascorsi i quali il volume viene archiviato.
- Il numero di backup da conservare nell'archivio. Specificare "0" (zero) per archiviare fino all'ultimo backup.
- Per AWS, selezionare la classe di storage di archiviazione.

4. Selezionare **Salva**.

## Proteggi nuovi volumi o LUN sul cloud

Quando si crea un nuovo volume o LUN, è possibile stabilire una relazione di protezione di SnapMirror che consenta il backup nel cloud per il volume o il LUN.

### Prima di iniziare

- È necessario disporre di una licenza SnapMirror.
- È necessario configurare le LIF di intercluster.
- NTP deve essere configurato.
- Il cluster deve eseguire ONTAP 9.9.1.

### A proposito di questa attività

Non è possibile proteggere nuovi volumi o LUN sul cloud per le seguenti configurazioni di cluster:

- Il cluster non può trovarsi in un ambiente MetroCluster.
- SVM-DR non supportato.
- Impossibile eseguire il backup di FlexGroups utilizzando Cloud Backup.

### Fasi

1. Quando si effettua il provisioning di un volume o di un LUN, nella pagina **Protection** di System Manager, selezionare la casella di controllo **Enable SnapMirror (Local or Remote)** (attiva SnapMirror (locale o remoto)\*).
2. Selezionare il tipo di criterio Cloud Backup.
3. Se il backup cloud non è attivato, selezionare **Enable Cloud Backup Service** (attiva backup cloud).

## Proteggere i volumi o le LUN esistenti nel cloud

È possibile stabilire una relazione di protezione di SnapMirror per i volumi e le LUN esistenti.

## Fasi

1. Selezionare un volume o un LUN esistente e fare clic su **Protect** (protezione).
2. Nella pagina **Protect Volumes**, specificare **Backup using Cloud Backup Service** per il criterio di protezione.
3. Fare clic su **Protect** (protezione).
4. Nella pagina **protezione**, selezionare la casella di controllo **attiva SnapMirror (locale o remoto)**.
5. Selezionare **Enable Cloud Backup Service** (attiva protocollo).

## Ripristinare i dati dai file di backup

È possibile eseguire operazioni di gestione del backup, come il ripristino dei dati, l'aggiornamento delle relazioni e l'eliminazione delle relazioni, solo quando si utilizza l'interfaccia BlueXP. Fare riferimento a ["Ripristino dei dati dai file di backup"](#) per ulteriori informazioni.

# Peering di cluster e SVM con CLI

## Panoramica del peering di cluster e SVM con CLI

È possibile creare relazioni peer tra cluster di origine e di destinazione e tra macchine virtuali storage di origine e di destinazione (SVM). È necessario creare relazioni peer tra queste entità prima di poter replicare le copie Snapshot utilizzando SnapMirror.

ONTAP 9.3 offre miglioramenti che semplificano il modo in cui si configurano le relazioni peer tra cluster e SVM. Le procedure di peering del cluster e delle SVM sono disponibili per tutte le versioni di ONTAP 9. Utilizzare la procedura appropriata per la versione di ONTAP in uso.

Le procedure vengono eseguite utilizzando l'interfaccia della riga di comando (CLI), non System Manager o uno strumento di scripting automatico.

## Preparatevi per il peering di cluster e SVM

### Nozioni di base sul peering

È necessario creare *relazioni peer* tra cluster di origine e di destinazione e tra SVM di origine e di destinazione prima di poter replicare le copie Snapshot utilizzando SnapMirror. Una relazione peer definisce le connessioni di rete che consentono a cluster e SVM di scambiare dati in modo sicuro.

I cluster e le SVM nelle relazioni tra pari comunicano sulla rete intercluster utilizzando *LIF (Intercluster Logical Interface)*. Una LIF intercluster è una LIF che supporta il servizio di interfaccia di rete "intercluster-core" e viene generalmente creata utilizzando la policy del servizio di interfaccia di rete "intercluster predefinito". È necessario creare LIF intercluster su ogni nodo dei cluster sottoposti a peering.

Le LIF di intercluster utilizzano i percorsi che appartengono alla SVM di sistema a cui sono assegnate. ONTAP crea automaticamente una SVM di sistema per le comunicazioni a livello di cluster all'interno di un IPspace.

Sono supportate entrambe le topologie fan-out e cascata. In una topologia a cascata, è necessario creare solo reti di intercluster tra i cluster primario e secondario e tra i cluster secondario e terziario. Non è necessario creare una rete di intercluster tra il cluster primario e il cluster terzo.





È possibile (ma non consigliabile) che un amministratore rimuova il servizio intercluster-core dalla policy di servizio intercluster predefinita. In questo caso, i LIF creati utilizzando "intercluster predefinito" non saranno effettivamente LIF intercluster. Per confermare che la policy di servizio dell'intercluster predefinito contiene il servizio intercluster-core, utilizzare il seguente comando:

```
network interface service-policy show -policy default-intercluster
```

## Prerequisiti per il peering del cluster

Prima di configurare il peering del cluster, verificare che la connettività, la porta, l'indirizzo IP, la subnet, il firewall, e i requisiti di naming dei cluster sono soddisfatti.



A partire da ONTAP 9.6, la crittografia peer del cluster fornisce il supporto per la crittografia GCM TLS 1.2 AES-256 per la replica dei dati per impostazione predefinita. I cifrari di sicurezza predefiniti ("PSK-AES256-GCM-SHA384") sono necessari per il funzionamento del peering del cluster anche se la crittografia è disattivata.

A partire da ONTAP 9.11.1, le crittografia di sicurezza DHE-PSK sono disponibili per impostazione predefinita.

## Requisiti di connettività

Ogni LIF di intercluster sul cluster locale deve essere in grado di comunicare con ogni LIF di intercluster sul cluster remoto.

Sebbene non sia necessario, è in genere più semplice configurare gli indirizzi IP utilizzati per le LIF di intercluster nella stessa subnet. Gli indirizzi IP possono risiedere nella stessa sottorete dei file LIF dei dati o in una sottorete diversa. La subnet utilizzata in ciascun cluster deve soddisfare i seguenti requisiti:

- La subnet deve appartenere al dominio di trasmissione che contiene le porte utilizzate per la comunicazione tra cluster.
- La subnet deve disporre di un numero sufficiente di indirizzi IP da allocare a un LIF intercluster per nodo.

Ad esempio, in un cluster a quattro nodi, la subnet utilizzata per la comunicazione tra cluster deve avere quattro indirizzi IP disponibili.

Ciascun nodo deve disporre di una LIF intercluster con un indirizzo IP sulla rete intercluster.

Le LIF di intercluster possono avere un indirizzo IPv4 o IPv6.



ONTAP consente di migrare le reti peering da IPv4 a IPv6, consentendo la presenza simultanea di entrambi i protocolli nelle LIF dell'intercluster. Nelle versioni precedenti, tutte le relazioni tra cluster per un intero cluster erano IPv4 o IPv6. Ciò significava che la modifica dei protocolli era un evento potenzialmente disgregativo.

## Requisiti delle porte

È possibile utilizzare porte dedicate per la comunicazione tra cluster o condividere le porte utilizzate dalla rete dati. Le porte devono soddisfare i seguenti requisiti:

- Tutte le porte utilizzate per comunicare con un determinato cluster remoto devono trovarsi nello stesso IPspace.

È possibile utilizzare più IPspaces per eseguire il peer con più cluster. La connettività full-mesh a coppie è necessaria solo all'interno di un IPspace.

- Il dominio di broadcast utilizzato per la comunicazione tra cluster deve includere almeno due porte per nodo in modo che la comunicazione tra cluster possa eseguire il failover da una porta a un'altra.

Le porte aggiunte a un dominio di broadcast possono essere porte di rete fisiche, VLAN o gruppi di interfacce (ifgrps).

- Tutte le porte devono essere cablate.
- Tutte le porte devono essere in buono stato.
- Le impostazioni MTU delle porte devono essere coerenti.

#### Requisiti del firewall



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

I firewall e i criteri di firewall tra cluster devono consentire i seguenti protocolli:

- Traffico ICMP bidirezionale
- Traffico TCP avviato in modo bidirezionale verso gli indirizzi IP di tutti i LIF intercluster sulle porte 11104 e 11105
- HTTPS bidirezionale tra le LIF dell'intercluster

Sebbene HTTPS non sia richiesto quando si imposta il peering del cluster utilizzando la CLI, HTTPS è richiesto in seguito se si utilizza System Manager per configurare la protezione dei dati.

L'impostazione predefinita `intercluster` La policy firewall consente l'accesso tramite il protocollo HTTPS e da tutti gli indirizzi IP (0.0.0.0/0). Se necessario, è possibile modificare o sostituire la policy.

#### Requisito del cluster

I cluster devono soddisfare i seguenti requisiti:

- Un cluster non può trovarsi in una relazione peer con più di 255 cluster.

#### Utilizzare porte condivise o dedicate

È possibile utilizzare porte dedicate per la comunicazione tra cluster o condividere le porte utilizzate dalla rete dati. Per decidere se condividere le porte, è necessario considerare la larghezza di banda della rete, l'intervallo di replica e la disponibilità delle porte.



È possibile condividere le porte su un cluster peered utilizzando le porte dedicate sull'altro.

#### Larghezza di banda della rete

Se si dispone di una rete ad alta velocità, ad esempio 10 GbE, potrebbe essere disponibile una larghezza di banda LAN locale sufficiente per eseguire la replica utilizzando le stesse porte 10 GbE utilizzate per l'accesso ai dati.

Anche in questo caso, è necessario confrontare la larghezza di banda WAN disponibile con la larghezza di banda della LAN. Se la larghezza di banda WAN disponibile è significativamente inferiore a 10 GbE, potrebbe essere necessario utilizzare porte dedicate.



L'unica eccezione a questa regola potrebbe essere rappresentata dal fatto che tutti o molti nodi del cluster replicano i dati, nel qual caso l'utilizzo della larghezza di banda è in genere distribuito tra i nodi.

Se non si utilizzano porte dedicate, le dimensioni massime dell'unità di trasmissione (MTU) della rete di replica dovrebbero essere le stesse della dimensione MTU della rete dati.

#### **Intervallo di replica**

Se la replica avviene in ore non di punta, dovresti essere in grado di utilizzare le porte dati per la replica anche senza una connessione LAN a 10 GbE.

Se la replica avviene durante il normale orario di lavoro, è necessario considerare la quantità di dati che verranno replicati e se richiede una larghezza di banda così elevata da causare conflitti con i protocolli dati. Se l'utilizzo della rete da parte dei protocolli di dati (SMB, NFS, iSCSI) è superiore al 50%, è necessario utilizzare porte dedicate per la comunicazione tra cluster, per consentire prestazioni non degradate in caso di failover del nodo.

#### **Disponibilità delle porte**

Se si determina che il traffico di replica interferisce con il traffico dati, è possibile migrare le LIF di intercluster su qualsiasi altra porta condivisa compatibile con intercluster sullo stesso nodo.

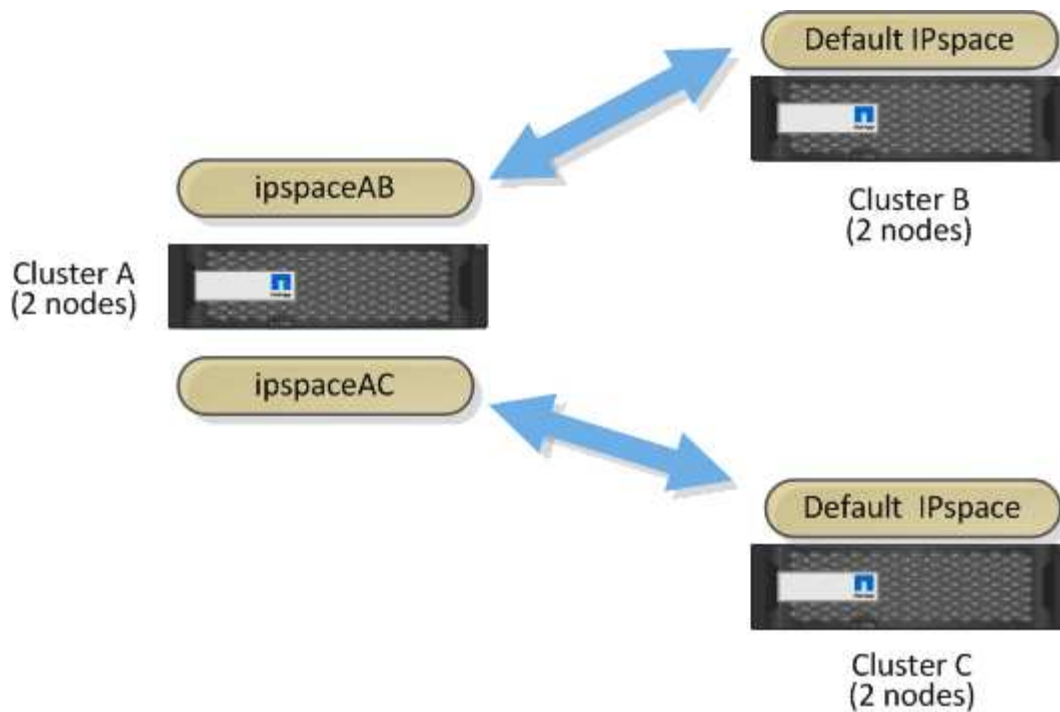
È inoltre possibile dedicare le porte VLAN per la replica. La larghezza di banda della porta è condivisa tra tutte le VLAN e la porta base.

#### **Utilizzare IPspaces personalizzati per isolare il traffico di replica**

È possibile utilizzare IPspaces personalizzati per separare le interazioni di un cluster con i peer. Detta *connettività intercluster designata*, questa configurazione consente ai service provider di isolare il traffico di replica in ambienti multi-tenant.

Si supponga, ad esempio, di voler separare il traffico di replica tra il cluster A e il cluster B dal traffico di replica tra il cluster A e il cluster C. A tale scopo, è possibile creare due IPspaces sul cluster A.

Un IPSpace contiene le LIF intercluster utilizzate per comunicare con il cluster B. L'altro contiene le LIF di intercluster utilizzate per comunicare con il cluster C, come mostrato nell'illustrazione seguente.



Per una configurazione IPspace personalizzata, consultare la *Guida alla gestione di rete*.

## Configurare le LIF tra cluster

### Configurare le LIF tra cluster su porte dati condivise

È possibile configurare le LIF di intercluster sulle porte condivise con la rete dati. In questo modo si riduce il numero di porte necessarie per la rete tra cluster.

#### Fasi

1. Elencare le porte nel cluster:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina *man*.

L'esempio seguente mostra le porte di rete in `cluster01`:

```
cluster01::> network port show
```

|              |       |         |                  |       |       | Speed      |
|--------------|-------|---------|------------------|-------|-------|------------|
| (Mbps)       |       |         |                  |       |       |            |
| Node         | Port  | IPspace | Broadcast Domain | Link  | MTU   | Admin/Oper |
| -----        | ----- | -----   | -----            | ----- | ----- |            |
| cluster01-01 |       |         |                  |       |       |            |
|              | e0a   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000  |
| cluster01-02 |       |         |                  |       |       |            |
|              | e0a   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000  |

2. Creazione di LIF intercluster da una SVM di amministrazione (IPSpace predefinito) o da una SVM di sistema (IPSpace personalizzato):

| Opzione                                    | Descrizione                                                                                                                                                                                                                |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>In ONTAP 9.6 e versioni successive:</b> | <code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -service -policy default-intercluster -home -node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code> |
| <b>In ONTAP 9.5 e versioni precedenti:</b> | <code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role intercluster -home-node <i>node</i> -home -port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i></code>                    |

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_icl01` e `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verificare che le LIF dell'intercluster siano state create:

| Opzione                                    | Descrizione                                                              |
|--------------------------------------------|--------------------------------------------------------------------------|
| <b>In ONTAP 9.6 e versioni successive:</b> | <code>network interface show -service-policy default-intercluster</code> |
| <b>In ONTAP 9.5 e versioni precedenti:</b> | <code>network interface show -role intercluster</code>                   |

Per la sintassi completa dei comandi, vedere la pagina [man](#).

```
cluster01::> network interface show -service-policy default-intercluster
Current Is
Vserver      Logical      Status      Network      Current
Home
-----
cluster01
      cluster01_icl01
              up/up      192.168.1.201/24      cluster01-01      e0c
true
      cluster01_icl02
              up/up      192.168.1.202/24      cluster01-02      e0c
true
```

4. Verificare che le LIF dell'intercluster siano ridondanti:

| Opzione                             | Descrizione                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------|
| In ONTAP 9.6 e versioni successive: | <code>network interface show -service-policy default-intercluster -failover</code> |
| In ONTAP 9.5 e versioni precedenti: | <code>network interface show -role intercluster -failover</code>                   |

Per la sintassi completa dei comandi, vedere la pagina `man`.

L'esempio seguente mostra che le LIF dell'intercluster `cluster01_icl01` e `cluster01_icl02` su `e0c` viene eseguito il failover della porta su `e0d` porta.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

| Vserver          | Logical<br>Interface | Home<br>Node:Port | Failover<br>Policy                                      | Failover<br>Group |
|------------------|----------------------|-------------------|---------------------------------------------------------|-------------------|
| cluster01        | cluster01_icl01      | cluster01-01:e0c  | local-only                                              |                   |
| 192.168.1.201/24 |                      |                   | Failover Targets: cluster01-01:e0c,<br>cluster01-01:e0d |                   |
|                  | cluster01_icl02      | cluster01-02:e0c  | local-only                                              |                   |
| 192.168.1.201/24 |                      |                   | Failover Targets: cluster01-02:e0c,<br>cluster01-02:e0d |                   |

### Configurare le LIF di intercluster su porte dedicate

È possibile configurare le LIF tra cluster su porte dedicate. In genere, aumenta la larghezza di banda disponibile per il traffico di replica.

#### Fasi

1. Elencare le porte nel cluster:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

L'esempio seguente mostra le porte di rete in `cluster01`:

```
cluster01::> network port show
```

| (Mbps)       |      | Speed   |                  |      |      |            |
|--------------|------|---------|------------------|------|------|------------|
| Node         | Port | IPspace | Broadcast Domain | Link | MTU  | Admin/Oper |
| -----        |      |         |                  |      |      |            |
| cluster01-01 |      |         |                  |      |      |            |
|              | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0e  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0f  | Default | Default          | up   | 1500 | auto/1000  |
| cluster01-02 |      |         |                  |      |      |            |
|              | e0a  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0b  | Cluster | Cluster          | up   | 1500 | auto/1000  |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0e  | Default | Default          | up   | 1500 | auto/1000  |
|              | e0f  | Default | Default          | up   | 1500 | auto/1000  |

## 2. Determinare quali porte sono disponibili per la comunicazione tra cluster:

```
network interface show -fields home-port,curr-port
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte e0e e. e0f Non sono stati assegnati LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01-01_clus1 e0a       e0a
Cluster cluster01-01_clus2 e0b       e0b
Cluster cluster01-02_clus1 e0a       e0a
Cluster cluster01-02_clus2 e0b       e0b
cluster01
    cluster_mgmt           e0c       e0c
cluster01
    cluster01-01_mgmt1     e0c       e0c
cluster01
    cluster01-02_mgmt1     e0c       e0c
```

## 3. Creare un gruppo di failover per le porte dedicate:



```
network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical_or_logical_ports
```

Nell'esempio seguente vengono assegnati i port e0e e. e0f al gruppo di failover intercluster01 Sul sistema SVM cluster01:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verificare che il gruppo di failover sia stato creato:

```
network interface failover-groups show
```

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface failover-groups show

Vserver          Group          Failover
-----
Targets
-----
Cluster
Cluster
cluster01-01:e0a, cluster01-01:e0b,
cluster01-02:e0a, cluster01-02:e0b
cluster01
Default
cluster01-01:e0c, cluster01-01:e0d,
cluster01-02:e0c, cluster01-02:e0d,
cluster01-01:e0e, cluster01-01:e0f
cluster01-02:e0e, cluster01-02:e0f
intercluster01
cluster01-01:e0e, cluster01-01:e0f
cluster01-02:e0e, cluster01-02:e0f
```

5. Creare LIF intercluster sulla SVM di sistema e assegnarle al gruppo di failover.

| Opzione                             | Descrizione                                                                                                                                                                                          |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| In ONTAP 9.6 e versioni successive: | network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group |

| Opzione                             | Descrizione                                                                                                                                                                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| In ONTAP 9.5 e versioni precedenti: | <code>network interface create -vserver <i>system_SVM</i> -lif <i>LIF_name</i> -role <i>intercluster</i> -home-node <i>node</i> -home-port <i>port</i> -address <i>port_IP</i> -netmask <i>netmask</i> -failover-group <i>failover_group</i></code> |

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_icl01` e `cluster01_icl02` nel gruppo di failover `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verificare che le LIF dell'intercluster siano state create:

| Opzione                             | Descrizione                                                                     |
|-------------------------------------|---------------------------------------------------------------------------------|
| In ONTAP 9.6 e versioni successive: | <code>network interface show -service-policy <i>default-intercluster</i></code> |
| In ONTAP 9.5 e versioni precedenti: | <code>network interface show -role <i>intercluster</i></code>                   |

Per la sintassi completa dei comandi, vedere la pagina `man`.

```

cluster01::> network interface show -service-policy default-intercluster

          Logical      Status      Network      Current
Current Is
Vserver   Interface  Admin/Oper Address/Mask      Node      Port
Home
-----
cluster01
          cluster01_icl01
                up/up      192.168.1.201/24  cluster01-01  e0e
true
          cluster01_icl02
                up/up      192.168.1.202/24  cluster01-02  e0f
true

```

7. Verificare che le LIF dell'intercluster siano ridondanti:

| Opzione                             | Descrizione                                                           |
|-------------------------------------|-----------------------------------------------------------------------|
| In ONTAP 9.6 e versioni successive: | network interface show -service-policy default-intercluster -failover |
| In ONTAP 9.5 e versioni precedenti: | network interface show -role intercluster -failover                   |

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che le LIF dell'intercluster cluster01\_icl01 e cluster01\_icl02 Su SVMe0e viene eseguito il failover della porta su e0f porta.

```

cluster01::> network interface show -service-policy default-intercluster
-failover

          Logical      Home      Failover      Failover
Vserver   Interface  Node:Port  Policy      Group
-----
cluster01
          cluster01_icl01  cluster01-01:e0e  local-only
intercluster01
                                Failover Targets:  cluster01-01:e0e,
  cluster01-01:e0f
          cluster01_icl02  cluster01-02:e0e  local-only
intercluster01
                                Failover Targets:  cluster01-02:e0e,
  cluster01-02:e0f

```

Configurare le LIF di intercluster in spazi IPpersonalizzati

È possibile configurare le LIF di intercluster in spazi IPpersonalizzati. In questo modo è possibile isolare il traffico di replica in ambienti multitenant.

Quando si crea un IPSpace personalizzato, il sistema crea una SVM (System Storage Virtual Machine) che funge da contenitore per gli oggetti di sistema in tale IPSpace. È possibile utilizzare la nuova SVM come container per qualsiasi LIF di intercluster nel nuovo IPSpace. Il nuovo SVM ha lo stesso nome dell'IPSpace personalizzato.

Fasi

- 1. Elencare le porte nel cluster:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le porte di rete in cluster01:

cluster01::> network port show

|              |       |         |                  |       |       | Speed      |
|--------------|-------|---------|------------------|-------|-------|------------|
| (Mbps)       |       |         |                  |       |       |            |
| Node         | Port  | IPspace | Broadcast Domain | Link  | MTU   | Admin/Oper |
| -----        | ----- | -----   | -----            | ----- | ----- |            |
| cluster01-01 |       |         |                  |       |       |            |
|              | e0a   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0e   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0f   | Default | Default          | up    | 1500  | auto/1000  |
| cluster01-02 |       |         |                  |       |       |            |
|              | e0a   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0b   | Cluster | Cluster          | up    | 1500  | auto/1000  |
|              | e0c   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0d   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0e   | Default | Default          | up    | 1500  | auto/1000  |
|              | e0f   | Default | Default          | up    | 1500  | auto/1000  |

- 2. Creare spazi IP personalizzati sul cluster:

```
network ipspace create -ipspace ipspace
```

Nell'esempio seguente viene creato l'IPSpace personalizzato ipspace-IC1:

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

3. Determinare quali porte sono disponibili per la comunicazione tra cluster:

```
network interface show -fields home-port,curr-port
```

Per la sintassi completa dei comandi, vedere la pagina [man](#).

L'esempio seguente mostra le porte e0e e. e0f Non sono stati assegnati LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                home-port curr-port
-----
Cluster cluster01_clus1    e0a      e0a
Cluster cluster01_clus2    e0b      e0b
Cluster cluster02_clus1    e0a      e0a
Cluster cluster02_clus2    e0b      e0b
cluster01
      cluster_mgmt          e0c      e0c
cluster01
      cluster01-01_mgmt1    e0c      e0c
cluster01
      cluster01-02_mgmt1    e0c      e0c
```

4. Rimuovere le porte disponibili dal dominio di trasmissione predefinito:

```
network port broadcast-domain remove-ports -broadcast-domain Default -ports
ports
```

Una porta non può trovarsi in più di un dominio di trasmissione alla volta. Per la sintassi completa dei comandi, vedere la pagina [man](#).

Nell'esempio seguente vengono rimosse le porte e0e e. e0f dal dominio di trasmissione predefinito:

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. Verificare che le porte siano state rimosse dal dominio di trasmissione predefinito:

```
network port show
```

Per la sintassi completa dei comandi, vedere la pagina [man](#).

L'esempio seguente mostra le porte e0e e. e0f sono stati rimossi dal dominio di trasmissione predefinito:

```
cluster01::> network port show
```

|              |      |         |                  |      |      | Speed (Mbps) |
|--------------|------|---------|------------------|------|------|--------------|
| Node         | Port | IPspace | Broadcast Domain | Link | MTU  | Admin/Oper   |
| -----        |      |         |                  |      |      |              |
| cluster01-01 |      |         |                  |      |      |              |
|              | e0a  | Cluster | Cluster          | up   | 9000 | auto/1000    |
|              | e0b  | Cluster | Cluster          | up   | 9000 | auto/1000    |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000    |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000    |
|              | e0e  | Default | -                | up   | 1500 | auto/1000    |
|              | e0f  | Default | -                | up   | 1500 | auto/1000    |
|              | e0g  | Default | Default          | up   | 1500 | auto/1000    |
| cluster01-02 |      |         |                  |      |      |              |
|              | e0a  | Cluster | Cluster          | up   | 9000 | auto/1000    |
|              | e0b  | Cluster | Cluster          | up   | 9000 | auto/1000    |
|              | e0c  | Default | Default          | up   | 1500 | auto/1000    |
|              | e0d  | Default | Default          | up   | 1500 | auto/1000    |
|              | e0e  | Default | -                | up   | 1500 | auto/1000    |
|              | e0f  | Default | -                | up   | 1500 | auto/1000    |
|              | e0g  | Default | Default          | up   | 1500 | auto/1000    |

#### 6. Creare un dominio di broadcast nell'IPSpace personalizzato:

```
network port broadcast-domain create -ipspace ipspace -broadcast-domain  
broadcast_domain -mtu MTU -ports ports
```

Nell'esempio seguente viene creato il dominio di trasmissione `ipspace-IC1-bd` In IPspace `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1  
-broadcast-domain  
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,  
cluster01-02:e0e,cluster01-02:e0f
```

#### 7. Verificare che il dominio di trasmissione sia stato creato:

```
network port broadcast-domain show
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

```

cluster01::> network port broadcast-domain show
IPspace Broadcast
Name      Domain Name      MTU      Port List
-----
Cluster Cluster      9000
cluster01-01:e0a      complete
cluster01-01:e0b      complete
cluster01-02:e0a      complete
cluster01-02:e0b      complete
Default Default      1500
cluster01-01:e0c      complete
cluster01-01:e0d      complete
cluster01-01:e0f      complete
cluster01-01:e0g      complete
cluster01-02:e0c      complete
cluster01-02:e0d      complete
cluster01-02:e0f      complete
cluster01-02:e0g      complete
ipspace-IC1
    ipspace-IC1-bd
                1500
cluster01-01:e0e      complete
cluster01-01:e0f      complete
cluster01-02:e0e      complete
cluster01-02:e0f      complete

```

8. Creare LIF di intercluster sulla SVM di sistema e assegnarle al dominio di trasmissione:

| Opzione                                    | Descrizione                                                                                                                                                                      |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>In ONTAP 9.6 e versioni successive:</b> | <pre> network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask </pre> |
| <b>In ONTAP 9.5 e versioni precedenti:</b> | <pre> network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask </pre>                    |

La LIF viene creata nel dominio di trasmissione a cui è assegnata la porta home. Il dominio di broadcast dispone di un gruppo di failover predefinito con lo stesso nome del dominio di broadcast. Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono create le LIF tra cluster cluster01\_icl01 e cluster01\_icl02 nel dominio di broadcast ipspace-IC1-bd:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. Verificare che le LIF dell'intercluster siano state create:

| Opzione                             | Descrizione                                                 |
|-------------------------------------|-------------------------------------------------------------|
| In ONTAP 9.6 e versioni successive: | network interface show -service-policy default-intercluster |
| In ONTAP 9.5 e versioni precedenti: | network interface show -role intercluster                   |

Per la sintassi completa dei comandi, vedere la pagina man.

```
cluster01::> network interface show -service-policy default-intercluster
Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node      Port
Home
-----
-----
ipspace-IC1
      cluster01_icl01
              up/up      192.168.1.201/24  cluster01-01  e0e
true
      cluster01_icl02
              up/up      192.168.1.202/24  cluster01-02  e0f
true
```

10. Verificare che le LIF dell'intercluster siano ridondanti:



| Opzione                             | Descrizione                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------|
| In ONTAP 9.6 e versioni successive: | <code>network interface show -service-policy default-intercluster -failover</code> |
| In ONTAP 9.5 e versioni precedenti: | <code>network interface show -role intercluster -failover</code>                   |

Per la sintassi completa dei comandi, vedere la pagina `man`.

L'esempio seguente mostra che le LIF dell'intercluster `cluster01_icl01` e `cluster01_icl02` Su SVM `e0e` failover della porta alla porta `e0f`:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

| Vserver        | Logical<br>Interface | Home<br>Node:Port | Failover<br>Policy | Failover<br>Group |
|----------------|----------------------|-------------------|--------------------|-------------------|
| -----          | -----                | -----             | -----              | -----             |
| ipspace-IC1    |                      |                   |                    |                   |
|                | cluster01_icl01      | cluster01-01:e0e  | local-only         |                   |
| intercluster01 |                      |                   |                    |                   |
|                |                      | Failover Targets: | cluster01-01:e0e,  |                   |
|                |                      |                   | cluster01-01:e0f   |                   |
|                | cluster01_icl02      | cluster01-02:e0e  | local-only         |                   |
| intercluster01 |                      |                   |                    |                   |
|                |                      | Failover Targets: | cluster01-02:e0e,  |                   |
|                |                      |                   | cluster01-02:e0f   |                   |

## Configurare le relazioni peer

### Creare una relazione peer del cluster

È possibile utilizzare `cluster peer create` per creare una relazione peer tra un cluster locale e remoto. Una volta creata la relazione peer, è possibile eseguire `cluster peer create` sul cluster remoto per autenticarlo nel cluster locale.

#### Prima di iniziare

- È necessario aver creato le LIF di intercluster su ogni nodo dei cluster che vengono sottoposti a peering.
- I cluster devono eseguire ONTAP 9.3 o versione successiva. Se i cluster eseguono ONTAP 9.2 o versioni precedenti, fare riferimento alle procedure descritte in ["documento archiviato"](#).)



#### Fasi

Eseguire questa attività utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

## System Manager

1. Nel cluster locale, fare clic su **Cluster > Impostazioni**.
2. Nella sezione **Impostazioni intercluster**, fare clic su **Aggiungi interfacce di rete** e aggiungere interfacce di rete intercluster per il cluster.

Ripetere questo passaggio sul cluster remoto.

3. Nel cluster remoto, fare clic su **Cluster > Impostazioni**.
4. Fare clic su  Nella sezione **Cluster Peers** e selezionare **generate Passphrase**.
5. Selezionare la versione del cluster ONTAP remoto.
6. Copiare la passphrase generata.
7. Nel cluster locale, in **Cluster Peers**, fare clic su  E selezionare **cluster peer**.
8. Nella finestra **Peer cluster**, incollare la passphrase e fare clic su **Initiate cluster peering**.

## CLI

1. Sul cluster di destinazione, creare una relazione peer con il cluster di origine:

```
cluster peer create -generate-passphrase -offer-expiration  
<MM/DD/YYYY HH:MM:SS>|1...7days|1...168hours -peer-addr  
<peer_LIF_IPs > -initial-allowed-vserver-peers <svm_name>|* -ip  
<ipspace>
```

Se si specificano entrambi `-generate-passphrase` e `-peer-addr`, Solo il cluster i cui LIF intercluster sono specificati in `-peer-addr` può utilizzare la password generata.

È possibile ignorare `-ipspace` Se non si utilizza un IPspace personalizzato. Per la sintassi completa dei comandi, vedere la pagina man.

Se si crea la relazione di peering in ONTAP 9.6 o versione successiva e non si desidera crittografare le comunicazioni di peering tra cluster, è necessario utilizzare `-encryption-protocol-proposed none` opzione per disattivare la crittografia.

Nell'esempio seguente viene creata una relazione peer del cluster con un cluster remoto non specificato e viene pre-autorizzata la relazione peer con le SVM `vs1` e `vs2` sul cluster locale:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

Nell'esempio riportato di seguito viene creata una relazione peer del cluster con il cluster remoto agli indirizzi IP LIF 192.140.112.103 e 192.140.112.104 dell'intercluster e viene pre-autorizzata una relazione peer con qualsiasi SVM sul cluster locale:

```
cluster02::> cluster peer create -generate-passphrase -peer-addr
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101,192.140.112.102
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

Nell'esempio seguente viene creata una relazione peer del cluster con un cluster remoto non specificato e viene pre-autorizzata la relazione peer con le SVM<sub>vs1</sub> e <sub>vs2</sub> sul cluster locale:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
Expiration Time: 6/7/2017 08:16:10 EST
Initial Allowed Vserver Peers: vs1,vs2
Intercluster LIF IP: 192.140.112.101
Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. Nel cluster di origine, autenticare il cluster di origine nel cluster di destinazione:

```
cluster peer create -peer-addr <peer_LIF_IPs> -ipspace <ipspace>
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene autenticato il cluster locale nel cluster remoto agli indirizzi IP LIF 192.140.112.101 e 192.140.112.102 dell'intercluster:

```
cluster01::> cluster peer create -peer-addr  
192.140.112.101,192.140.112.102
```

Notice: Use a generated passphrase or choose a passphrase of 8 or more characters.

To ensure the authenticity of the peering relationship, use a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:

Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.

Inserire la passphrase per la relazione peer quando richiesto.

3. Verificare che la relazione peer del cluster sia stata creata:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance
```

```
Peer Cluster Name: cluster02  
Remote Intercluster Addresses: 192.140.112.101,  
192.140.112.102  
Availability of the Remote Cluster: Available  
Remote Cluster Name: cluster2  
Active IP Addresses: 192.140.112.101,  
192.140.112.102  
Cluster Serial Number: 1-80-123456  
Address Family of Relationship: ipv4  
Authentication Status Administrative: no-authentication  
Authentication Status Operational: absent  
Last Update Time: 02/05 21:05:41  
IPspace for the Relationship: Default
```

#### 4. Verificare la connettività e lo stato dei nodi nella relazione peer:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node          cluster-Name          Node-Name
          Ping-Status          RDB-Health Cluster-Health
Avail...
-----
cluster01-01
          cluster02          cluster02-01
          Data: interface_reachable
          ICMP: interface_reachable true          true
true
          cluster02-02
          Data: interface_reachable
          ICMP: interface_reachable true          true
true
cluster01-02
          cluster02          cluster02-01
          Data: interface_reachable
          ICMP: interface_reachable true          true
true
          cluster02-02
          Data: interface_reachable
          ICMP: interface_reachable true          true
true
```

#### Altri modi per farlo in ONTAP

| Per eseguire queste attività con...                                           | Guarda questo contenuto...                                                       |
|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive) | <a href="#">"Preparazione per il mirroring e il vaulting"</a>                    |
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)      | <a href="#">"Panoramica sulla preparazione del disaster recovery dei volumi"</a> |

#### Creare una relazione peer SVM tra cluster

È possibile utilizzare `vserver peer create` Per creare una relazione peer tra SVM su cluster locali e remoti.

#### Prima di iniziare

- I cluster di origine e di destinazione devono essere peering.
- I cluster devono eseguire ONTAP 9.3. Se i cluster eseguono ONTAP 9.2 o versioni precedenti, fare riferimento alle procedure descritte in ["documento archiviato"](#).)
- È necessario disporre di relazioni peer "pre-autorizzate" per le SVM sul cluster remoto.

Per ulteriori informazioni, vedere ["Creazione di una relazione peer del cluster"](#).

### A proposito di questa attività

In ONTAP 9,2 e versioni precedenti, puoi autorizzare una relazione di peer per una sola SVM alla volta. Ciò significa che è necessario eseguire `vserver peer accept` Comando ogni volta che autorizzi una relazione peer SVM in sospeso.

A partire da ONTAP 9.3, è possibile "pre-autorizzare" le relazioni peer per più SVM elencando le SVM in `-initial-allowed-vserver` quando si crea una relazione peer del cluster. Per ulteriori informazioni, vedere ["Creazione di una relazione peer del cluster"](#).

### Fasi

1. Nel cluster di destinazione per la protezione dei dati, visualizzare le SVM pre-autorizzate per il peering:

```
vserver peer permission show
```

```
cluster02::> vserver peer permission show
Peer Cluster          Vserver                Applications
-----
cluster02             vs1,vs2                snapmirror
```

2. Sul cluster di origine per la protezione dei dati, creare una relazione peer con una SVM pre-autorizzata sul cluster di destinazione per la protezione dei dati:

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene creata una relazione peer tra la SVM locale `pvs1` E la SVM remota pre-autorizzata `vs1`:

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
```

3. Verificare la relazione peer SVM:

```
vserver peer show
```

```
cluster01::> vserver peer show
```

|         | Peer    | Peer   |              | Peering      |
|---------|---------|--------|--------------|--------------|
| Remote  |         |        |              |              |
| Vserver | Vserver | State  | Peer Cluster | Applications |
| Vserver |         |        |              |              |
| -----   | -----   | -----  | -----        | -----        |
| -----   |         |        |              |              |
| pvs1    | vs1     | peered | cluster02    | snapmirror   |
| vs1     |         |        |              |              |

## Aggiungere una relazione peer SVM tra cluster

Se si crea una SVM dopo aver configurato una relazione peer del cluster, sarà necessario aggiungere manualmente una relazione peer per la SVM. È possibile utilizzare `vserver peer create` Per creare una relazione peer tra le SVM. Una volta creata la relazione peer, è possibile eseguire `vserver peer accept` sul cluster remoto per autorizzare la relazione peer.

### Prima di iniziare

I cluster di origine e di destinazione devono essere peering.

### A proposito di questa attività

È possibile creare relazioni peer tra le SVM nello stesso cluster per il backup dei dati locale. Per ulteriori informazioni, consultare `vserver peer create` pagina man.

Gli amministratori utilizzano occasionalmente `vserver peer reject` Comando per rifiutare una relazione peer SVM proposta. Se la relazione tra le SVM si trova in `rejected state` (stato), è necessario eliminare la relazione prima di crearne una nuova. Per ulteriori informazioni, consultare `vserver peer delete` pagina man.

### Fasi

1. Nel cluster di origine per la protezione dei dati, creare una relazione peer con una SVM nel cluster di destinazione per la protezione dei dati:

```
vserver peer create -vserver local_SVM -peer-vserver remote_SVM -applications
snapmirror|file-copy|lun-copy -peer-cluster remote_cluster
```

Nell'esempio seguente viene creata una relazione peer tra la SVM locale `pvs1` E SVM remoto `vs1`

```
cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
-applications snapmirror -peer-cluster cluster02
```

Se le SVM locali e remote hanno gli stessi nomi, è necessario utilizzare un *nome locale* per creare la relazione peer SVM:

```
cluster01::> vserver peer create -vserver vs1 -peer-vserver
vs1 -applications snapmirror -peer-cluster cluster01
-local-name cluster1vs1LocallyUniqueName
```

2. Nel cluster di origine per la protezione dei dati, verificare che la relazione peer sia stata avviata:

```
vserver peer show-all
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra che la relazione peer tra SVM<sub>pvs1</sub> E SVM<sub>vs1</sub> è stato avviato:

```
cluster01::> vserver peer show-all
```

| Vserver | Peer<br>Vserver | Peer<br>State | Peer Cluster | Peering<br>Applications |
|---------|-----------------|---------------|--------------|-------------------------|
| -----   | -----           | -----         | -----        | -----                   |
| pvs1    | vs1             | initiated     | Cluster02    | snapmirror              |

3. Sul cluster di destinazione per la protezione dei dati, visualizzare la relazione peer SVM in sospeso:

```
vserver peer show
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio riportato di seguito sono elencate le relazioni peer in sospeso per cluster02:

```
cluster02::> vserver peer show
```

| Vserver | Peer<br>Vserver | Peer<br>State |
|---------|-----------------|---------------|
| -----   | -----           | -----         |
| vs1     | pvs1            | pending       |

4. Nel cluster di destinazione per la protezione dei dati, autorizzare la relazione peer in sospeso:

```
vserver peer accept -vserver local_SVM -peer-vserver remote_SVM
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio riportato di seguito viene autorizzata la relazione peer tra la SVM locale vs1 E SVM remoto pvs1:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Verificare la relazione peer SVM:



```
vserver peer show
```

```
cluster01::> vserver peer show
```

| Remote Vserver | Peer Vserver | Peer State | Peer Cluster | Peering Applications |
|----------------|--------------|------------|--------------|----------------------|
| pvs1           | vs1          | peered     | cluster02    | snapmirror           |
| vs1            |              |            |              |                      |

## Abilitare la crittografia del peering del cluster su una relazione peer esistente

A partire da ONTAP 9.6, la crittografia del peering del cluster è attivata per impostazione predefinita su tutte le relazioni di peering del cluster appena create. La crittografia del peering dei cluster utilizza una chiave precondivisa (PSK) e TLS (Transport Security Layer) per proteggere le comunicazioni di peering tra cluster. Questo aggiunge un ulteriore livello di sicurezza tra i cluster peered.

### A proposito di questa attività

Se si aggiornano i cluster peering a ONTAP 9.6 o versione successiva e la relazione di peering è stata creata in ONTAP 9.5 o versione precedente, la crittografia di peering dei cluster deve essere attivata manualmente dopo l'aggiornamento. Entrambi i cluster della relazione di peering devono eseguire ONTAP 9.6 o versione successiva per abilitare la crittografia di peering dei cluster.

### Fasi

1. Sul cluster di destinazione, attivare la crittografia per le comunicazioni con il cluster di origine:

```
cluster peer modify source_cluster -auth-status-admin use-authentication  
-encryption-protocol-proposed tls-psk
```

2. Quando richiesto, inserire una passphrase.
3. Nel cluster di origine per la protezione dei dati, abilitare la crittografia per la comunicazione con il cluster di destinazione per la protezione dei dati:

```
cluster peer modify data_protection_destination_cluster -auth-status-admin  
use-authentication -encryption-protocol-proposed tls-psk
```

4. Quando richiesto, inserire la stessa passphrase inserita nel cluster di destinazione.

## Rimuovere la crittografia di peering del cluster da una relazione peer esistente

Per impostazione predefinita, la crittografia del peering del cluster è attivata su tutte le relazioni peer create in ONTAP 9.6 o versioni successive. Se non si desidera utilizzare la crittografia per le comunicazioni di peering tra cluster, è possibile disattivarla.

## Fasi

1. Nel cluster di destinazione, modificare le comunicazioni con il cluster di origine per interrompere l'utilizzo della crittografia di peering del cluster:

- Per rimuovere la crittografia, ma mantenere l'autenticazione, immettere:

```
cluster peer modify _source_cluster_ -auth-status-admin use-  
authentication -encryption-protocol-proposed none
```

- Per rimuovere la crittografia e l'autenticazione, immettere:

```
cluster peer modify _source_cluster_ -auth-status no-authentication
```

2. Quando richiesto, inserire una passphrase.

3. Sul cluster di origine, disattivare la crittografia per la comunicazione con il cluster di destinazione:

- Per rimuovere la crittografia, ma mantenere l'autenticazione, immettere:

```
cluster peer modify _destination_cluster_ -auth-status-admin use-  
authentication -encryption-protocol-proposed none
```

- Per rimuovere la crittografia e l'autenticazione, immettere:

```
cluster peer modify _destination_cluster_ -auth-status no-  
authentication
```

4. Quando richiesto, inserire la stessa passphrase inserita nel cluster di destinazione.

## Gestire le copie Snapshot locali

### Panoramica sulla gestione delle copie Snapshot locali

Una *copia Snapshot* è un'immagine point-in-time di sola lettura di un volume. L'immagine consuma uno spazio di storage minimo e comporta un overhead delle performance trascurabile, in quanto registra solo le modifiche apportate ai file dall'ultima copia Snapshot.

È possibile utilizzare una copia Snapshot per ripristinare l'intero contenuto di un volume o per ripristinare singoli file o LUN. Le copie Snapshot vengono memorizzate nella directory `.snapshot` sul volume.

In ONTAP 9.3 e versioni precedenti, un volume può contenere fino a 255 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume FlexVol può contenere fino a 1023 copie Snapshot.



A partire da ONTAP 9.8, i volumi FlexGroup possono contenere 1023 copie Snapshot. Per ulteriori informazioni, vedere ["Proteggere i volumi FlexGroup utilizzando le copie Snapshot"](#).

## Configurare policy Snapshot personalizzate

### Panoramica sulla configurazione dei criteri Snapshot personalizzati

Una *policy Snapshot* definisce il modo in cui il sistema crea le copie Snapshot. Il criterio specifica quando creare copie Snapshot, quante copie conservare e come assegnarle un nome. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti e nominare le copie “daily.timestamp”

Il criterio predefinito per un volume crea automaticamente le copie Snapshot secondo la seguente pianificazione, con le copie Snapshot meno recenti eliminate per fare spazio alle copie più recenti:

- Un massimo di sei copie Snapshot orarie effettuate cinque minuti dopo l'ora.
- Un massimo di due copie Snapshot giornaliere eseguite da lunedì a sabato a 10 minuti dalla mezzanotte.
- Un massimo di due copie Snapshot settimanali eseguite ogni domenica a 15 minuti dalla mezzanotte.

A meno che non si specifichi un criterio Snapshot quando si crea un volume, il volume eredita il criterio Snapshot associato alla relativa SVM (Storage Virtual Machine).

### Quando configurare un criterio Snapshot personalizzato

Se il criterio Snapshot predefinito non è appropriato per un volume, è possibile configurare un criterio personalizzato che modifica la frequenza, la conservazione e il nome delle copie Snapshot. La pianificazione sarà dettata principalmente dalla velocità di cambiamento del file system attivo.

È possibile eseguire il backup di un file system molto utilizzato come un database ogni ora, mentre si eseguono backup di file raramente utilizzati una volta al giorno. Anche per un database, in genere viene eseguito un backup completo una o due volte al giorno, eseguendo il backup dei registri delle transazioni ogni ora.

Altri fattori sono l'importanza dei file per la tua organizzazione, il tuo Service Level Agreement (SLA), il tuo Recovery Point Objective (RPO) e il tuo Recovery Time Objective (RTO). In generale, è necessario conservare solo il numero di copie Snapshot necessario.

### Creare una pianificazione del lavoro Snapshot

Una policy Snapshot richiede almeno una pianificazione del lavoro di copia Snapshot. È possibile utilizzare `job schedule cron create` per creare una pianificazione del processo.

#### A proposito di questa attività

Per impostazione predefinita, ONTAP crea i nomi delle copie Snapshot aggiungendo un indicatore data e ora al nome della pianificazione del processo.

Se si specificano valori per il giorno del mese e il giorno della settimana, i valori vengono considerati indipendentemente. Ad esempio, un programma cron con la specifica del giorno `Friday` e il giorno del mese specificato `13` Viene eseguito ogni venerdì e il 13° giorno di ogni mese, non solo ogni venerdì 13.

#### Fase

## 1. Creare una pianificazione del processo:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

A partire da ONTAP 9.10.1, è possibile includere il server virtuale per la pianificazione del processo:

```
job schedule cron create -name job_name -vserver Vserver_name -month month  
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

Nell'esempio seguente viene creata una pianificazione del processo denominata `myweekly` il sabato alle 3:00:

```
cluster1::> job schedule cron create -name myweekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

Nell'esempio seguente viene creata una pianificazione denominata `myweeklymulti` che specifica più giorni, ore e minuti:

```
job schedule cron create -name myweeklymulti -dayofweek  
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

## Creare una policy Snapshot

Un criterio Snapshot specifica quando creare copie Snapshot, quante copie conservare e come assegnarle un nome. Ad esempio, un sistema potrebbe creare una copia Snapshot ogni giorno alle 12:10, conservare le due copie più recenti e chiamarle "daily.  
*timestamp*" Una policy Snapshot può contenere fino a cinque pianificazioni di lavori.

### A proposito di questa attività

Per impostazione predefinita, ONTAP crea i nomi delle copie Snapshot aggiungendo un indicatore data e ora al nome della pianificazione del processo:

|                         |                         |
|-------------------------|-------------------------|
| daily.2017-05-14_0013/  | hourly.2017-05-15_1106/ |
| daily.2017-05-15_0012/  | hourly.2017-05-15_1206/ |
| hourly.2017-05-15_1006/ | hourly.2017-05-15_1306/ |

Se si preferisce, è possibile sostituire un prefisso con il nome della pianificazione del lavoro.

Il `snapmirror-label` Opzione per la replica di SnapMirror. Per ulteriori informazioni, vedere ["Definizione di una regola per un criterio"](#).

## Fase

## 1. Creare una policy Snapshot:

```
volume snapshot policy create -vserver SVM -policy policy_name -enabled
true|false -schedule1 schedule1_name -count1 copies_to_retain -prefix1
snapshot_prefix -snapmirror-label1 snapshot_label ... -schedule5 schedule5_name
-count5 copies_to_retain-prefix5 snapshot_prefix -snapmirror-label5
snapshot_label
```

Nell'esempio seguente viene creata una policy Snapshot denominata `snap_policy_daily` che funziona su `daily` pianificazione. Il criterio dispone di un massimo di cinque copie Snapshot, ciascuna con il nome `daily.timestamp` E l'etichetta `SnapMirror daily`:

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1 daily
```

## Gestione manuale delle copie Snapshot

### Crea ed elimina copie Snapshot manualmente

Puoi creare copie Snapshot manualmente quando non puoi aspettare la creazione di una copia Snapshot pianificata e puoi eliminare le copie Snapshot quando non sono più necessarie.

#### Creazione manuale di una copia Snapshot

Puoi creare manualmente una copia Snapshot usando System Manager o l'interfaccia a riga di comando di ONTAP.

#### System Manager

##### Fasi

1. Accedere a **archiviazione > volumi** e selezionare la scheda **Snapshot Copies**.
2. Fare clic su **+ Add**.
3. Nella finestra **Aggiungi copia istantanea**, accettare il nome predefinito della copia istantanea o modificarlo, se necessario.
4. **Facoltativo**: Aggiungere un'etichetta `SnapMirror`.
5. Fare clic su **Aggiungi**.

##### CLI

1. Creare una copia Snapshot:


```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

## Eliminazione manuale di una copia Snapshot

Puoi eliminare manualmente una copia Snapshot usando System Manager o l'interfaccia a riga di comando di ONTAP.

### System Manager

#### Fasi

1. Accedere a **archiviazione > volumi** e selezionare la scheda **Snapshot Copies**.
2. Individuare la copia Snapshot che si desidera eliminare e fare clic su  E selezionare **Elimina**.
3. Nella finestra **Elimina copia istantanea**, selezionare **Elimina copia istantanea**.
4. Fare clic su **Delete** (Elimina).

#### CLI

1. Eliminazione di una copia Snapshot:

```
volume snapshot delete -vserver <SVM> -volume <volume> -snapshot  
<snapshot_name>
```

## Gestire la riserva di copie Snapshot

### Gestire la panoramica della riserva di copia Snapshot

La *riserva di copia Snapshot* consente di riservare una percentuale di spazio su disco per le copie Snapshot, pari al 5% per impostazione predefinita. Poiché le copie Snapshot utilizzano lo spazio nel file system attivo quando la riserva di copia Snapshot viene esaurita, è possibile aumentare la riserva di copia Snapshot in base alle necessità. In alternativa, è possibile eliminare automaticamente le copie Snapshot quando la riserva è piena.

### Quando aumentare la riserva di copia Snapshot

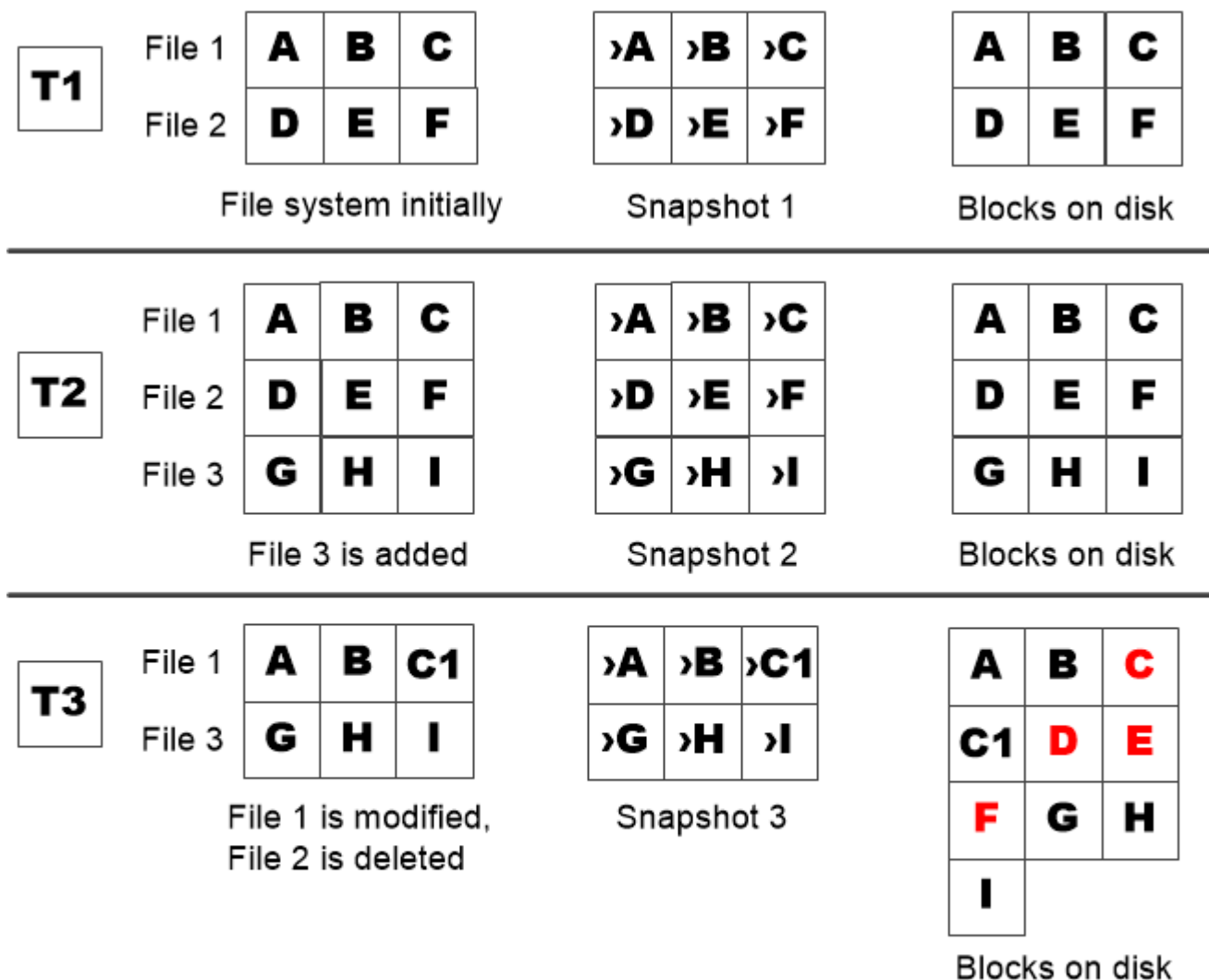
Nel decidere se aumentare la riserva Snapshot, è importante ricordare che una copia Snapshot registra solo le modifiche apportate ai file dall'ultima copia Snapshot. Consuma spazio su disco solo quando i blocchi nel file system attivo vengono modificati o cancellati.

Ciò significa che il tasso di cambiamento del file system è il fattore chiave per determinare la quantità di spazio su disco utilizzata dalle copie Snapshot. Indipendentemente dal numero di copie Snapshot create, non consumeranno spazio su disco se il file system attivo non è stato modificato.

Ad esempio, un volume FlexVol contenente registri delle transazioni del database potrebbe avere una riserva di copia Snapshot pari al 20% per tenere conto della maggiore velocità di modifica. Oltre a creare più copie Snapshot per acquisire gli aggiornamenti più frequenti del database, è necessario disporre di una riserva di copie Snapshot più ampia per gestire lo spazio su disco aggiuntivo consumato dalle copie Snapshot.



Una copia Snapshot è costituita da puntatori a blocchi anziché a copie di blocchi. Si può pensare a un puntatore come a “claim” su un blocco: ONTAP “mantiene” il blocco fino a quando la copia Snapshot non viene eliminata.



*A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.*

In che modo l'eliminazione dei file protetti può ridurre lo spazio dei file rispetto al previsto

Una copia Snapshot punta a un blocco anche dopo aver eliminato il file che ha utilizzato il blocco. Questo spiega perché una riserva di copia Snapshot esaurita potrebbe portare a un risultato controintuitivo in cui l'eliminazione di un intero file system comporta una quantità di spazio disponibile inferiore a quella occupata dal file system.

Si consideri il seguente esempio. Prima di eliminare qualsiasi file, il df l'output del comando è il seguente:

| Filesystem          | kbytes  | used    | avail  | capacity |
|---------------------|---------|---------|--------|----------|
| /vol/vol0/          | 3000000 | 3000000 | 0      | 100%     |
| /vol/vol0/.snapshot | 1000000 | 500000  | 500000 | 50%      |

Dopo aver eliminato l'intero file system ed eseguito una copia Snapshot del volume, il `df` il comando genera il seguente output:

| Filesystem          | kbytes  | used    | avail  | capacity |
|---------------------|---------|---------|--------|----------|
| /vol/vol0/          | 3000000 | 2500000 | 500000 | 83%      |
| /vol/vol0/.snapshot | 1000000 | 3500000 | 0      | 350%     |

Come mostra l'output, l'intero 3 GB utilizzato in precedenza dal file system attivo viene ora utilizzato dalle copie Snapshot, oltre ai 0.5 GB utilizzati prima dell'eliminazione.

Poiché lo spazio su disco utilizzato dalle copie Snapshot ora supera la riserva di copia Snapshot, l'overflow di 2.5 GB di "spills" nello spazio riservato ai file attivi, lasciando 0.5 GB di spazio libero per i file in cui si potrebbero ragionevolmente prevedere 3 GB.

### Monitorare il consumo dei dischi di copia Snapshot

È possibile monitorare il consumo dei dischi di copia Snapshot utilizzando `df` comando. Il comando visualizza la quantità di spazio libero nel file system attivo e la riserva di copia Snapshot.

#### Fase

1. Visualizza consumo di dischi di copia Snapshot: `df`

Il seguente esempio mostra il consumo di dischi di copia Snapshot:

```
cluster1::> df
Filesystem      kbytes  used   avail  capacity
/vol/vol0/      3000000 3000000 0        100%
/vol/vol0/.snapshot 1000000 500000 500000   50%
```

### Verificare la riserva di copia Snapshot disponibile su un volume

È possibile verificare la quantità di riserva di copia Snapshot disponibile su un volume utilizzando `snapshot-reserve-available` con il `volume show` comando.

#### Fase

1. Verificare la riserva di copia Snapshot disponibile su un volume:

```
vol show -vserver SVM -volume volume -fields snapshot-reserve-available
```

Per la sintassi completa dei comandi, vedere la pagina [man](#).



Nell'esempio seguente viene visualizzata la riserva di copia Snapshot disponibile per `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
-----
vs0      vol1      4.84GB
```

## Modificare la riserva di copia Snapshot

È possibile configurare una riserva di copia Snapshot più ampia per impedire alle copie Snapshot di utilizzare lo spazio riservato al file system attivo. È possibile ridurre la riserva di copia Snapshot quando non è più necessario tanto spazio per le copie Snapshot.

### Fase

1. Modificare la riserva di copia Snapshot:

```
volume modify -vserver SVM -volume volume -percent-snapshot-space snap_reserve
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene impostata la riserva di copia Snapshot per `vol1` al 10%:

```
cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
-space 10
```

## Eliminazione automatica delle copie Snapshot

È possibile utilizzare `volume snapshot autodelete modify` Comando per attivare l'eliminazione automatica delle copie Snapshot quando viene superata la riserva Snapshot. Per impostazione predefinita, le copie Snapshot meno recenti vengono eliminate per prime.

### A proposito di questa attività

I LUN e i cloni di file vengono cancellati quando non sono più presenti copie Snapshot da eliminare.

### Fase

1. Eliminazione automatica delle copie Snapshot:

```
volume snapshot autodelete modify -vserver SVM -volume volume -enabled
true|false -trigger volume|snap_reserve
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente vengono eliminate automaticamente le copie Snapshot per `vol1` Quando la riserva

di copia Snapshot è esaurita:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume voll  
-enabled true -trigger snap_reserve
```

## Ripristinare i file dalle copie Snapshot

### Ripristinare un file da una copia Snapshot su un client NFS o SMB

Un utente su un client NFS o SMB può ripristinare un file direttamente da una copia Snapshot senza l'intervento di un amministratore del sistema di storage.

Ogni directory del file system contiene una sottodirectory denominata `.snapshot` Accessibile agli utenti NFS e SMB. Il `.snapshot` La sottodirectory contiene le sottodirectory corrispondenti alle copie Snapshot del volume:

```
$ ls .snapshot  
daily.2017-05-14_0013/          hourly.2017-05-15_1106/  
daily.2017-05-15_0012/          hourly.2017-05-15_1206/  
hourly.2017-05-15_1006/         hourly.2017-05-15_1306/
```

Ogni sottodirectory contiene i file a cui fa riferimento la copia Snapshot. Se gli utenti eliminano o sovrascrivono accidentalmente un file, possono ripristinarlo nella directory padre di lettura/scrittura copiandolo dalla sottodirectory Snapshot alla directory di lettura/scrittura:

```
$ ls my.txt  
ls: my.txt: No such file or directory  
$ ls .snapshot  
daily.2017-05-14_0013/          hourly.2017-05-15_1106/  
daily.2017-05-15_0012/          hourly.2017-05-15_1206/  
hourly.2017-05-15_1006/         hourly.2017-05-15_1306/  
$ ls .snapshot/hourly.2017-05-15_1306/my.txt  
my.txt  
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .  
$ ls my.txt  
my.txt
```

### Abilitare e disabilitare l'accesso dei client NFS e SMB alla directory di copia Snapshot

Per determinare se la directory di copia Snapshot è visibile ai client NFS e SMB per ripristinare un file o un LUN da una copia Snapshot, è possibile attivare e disattivare l'accesso alla directory di copia Snapshot utilizzando `-snapdir-access` opzione di `volume modify` comando.

## Fasi

1. Controllare lo stato di accesso alla directory Snapshot:

```
volume show -vserver SVM_name -volume vol_name -fields snapdir-access
```

Esempio:

```
clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-access
vserver volume snapdir-access
-----
vs0      vol1    false
```

2. Attivare o disattivare l'accesso alla directory di copia Snapshot:

```
volume modify -vserver SVM_name -volume vol_name -snapdir-access true|false
```

Il seguente esempio consente l'accesso alla directory di copia Snapshot su vol1:

```
clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access true
Volume modify successful on volume vol1 of Vserver vs0.
```

## Ripristinare un singolo file da una copia Snapshot

È possibile utilizzare `volume snapshot restore-file` Comando per ripristinare un singolo file o LUN da una copia Snapshot. Se non si desidera sostituire un file esistente, è possibile ripristinare il file in una posizione diversa nel volume di lettura/scrittura padre.

### A proposito di questa attività

Se si sta ripristinando un LUN esistente, viene creato un clone del LUN e ne viene eseguito il backup sotto forma di copia Snapshot. Durante l'operazione di ripristino, è possibile leggere e scrivere sul LUN.

I file con flussi vengono ripristinati per impostazione predefinita.

## Fasi

1. Elencare le copie Snapshot in un volume:

```
volume snapshot show -vserver SVM -volume volume
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

L'esempio seguente mostra le copie Snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume voll
```

| Vserver | Volume | Snapshot               | State | Size  | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| vs1     | voll   | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|         |        | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|         |        | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

## 2. Ripristinare un file da una copia Snapshot:

```
volume snapshot restore-file -vserver SVM -volume volume -snapshot snapshot  
-path file_path -restore-path destination_path
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio riportato di seguito viene ripristinato il file `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume voll  
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

## Ripristinare parte di un file da una copia Snapshot

È possibile utilizzare `volume snapshot partial-restore-file` Comando per ripristinare un intervallo di dati da una copia Snapshot a un LUN o a un file container NFS o SMB, presupponendo di conoscere l'offset di byte iniziale dei dati e il numero di byte. È possibile utilizzare questo comando per ripristinare uno dei database su un host che memorizza più database nello stesso LUN.

A partire da ONTAP 9.12.1, il ripristino parziale è disponibile per i volumi in una relazione SM-BC.

### Fasi

1. Elencare le copie Snapshot in un volume:

```
volume snapshot show -vserver SVM -volume volume
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente mostra le copie Snapshot in `voll`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

| Vserver | Volume | Snapshot               | State | Size  | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| vs1     | vol1   | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|         |        | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|         |        | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

## 2. Ripristinare parte di un file da una copia Snapshot:

```
volume snapshot partial-restore-file -vserver SVM -volume volume -snapshot  
snapshot -path file_path -start-byte starting_byte -byte-count byte_count
```

L'offset di byte iniziale e il conteggio di byte devono essere multipli di 4,096.

Nell'esempio seguente vengono ripristinati i primi 4,096 byte del file `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume  
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0  
-byte-count 4096
```

## Ripristinare il contenuto di un volume da una copia Snapshot

È possibile utilizzare `volume snapshot restore` Comando per ripristinare il contenuto di un volume da una copia Snapshot.

### A proposito di questa attività

Se il volume presenta relazioni SnapMirror, replicare manualmente tutte le copie mirror del volume immediatamente dopo il ripristino da una copia Snapshot. In caso contrario, le copie mirror non possono essere utilizzabili e devono essere eliminate e ricreate.

## 1. Elencare le copie Snapshot in un volume:

```
volume snapshot show -vserver SVM -volume volume
```

L'esempio seguente mostra le copie Snapshot in `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1
```

| Vserver | Volume | Snapshot               | State | Size  | Total% | Used% |
|---------|--------|------------------------|-------|-------|--------|-------|
| vs1     | vol1   | hourly.2013-01-25_0005 | valid | 224KB | 0%     | 0%    |
|         |        | daily.2013-01-25_0010  | valid | 92KB  | 0%     | 0%    |
|         |        | hourly.2013-01-25_0105 | valid | 228KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0205 | valid | 236KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0305 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0405 | valid | 244KB | 0%     | 0%    |
|         |        | hourly.2013-01-25_0505 | valid | 244KB | 0%     | 0%    |

7 entries were displayed.

## 2. Ripristinare il contenuto di un volume da una copia Snapshot:

```
volume snapshot restore -vserver SVM -volume volume -snapshot snapshot
```

Nell'esempio riportato di seguito viene ripristinato il contenuto di vol1:

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1 -snapshot  
daily.2013-01-25_0010
```

# Replica del volume SnapMirror

## Nozioni di base sul disaster recovery asincrono di SnapMirror

*SnapMirror* è una tecnologia di disaster recovery progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. Come suggerisce il nome, SnapMirror crea una replica, o *mirror*, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di disastro nel sito primario.

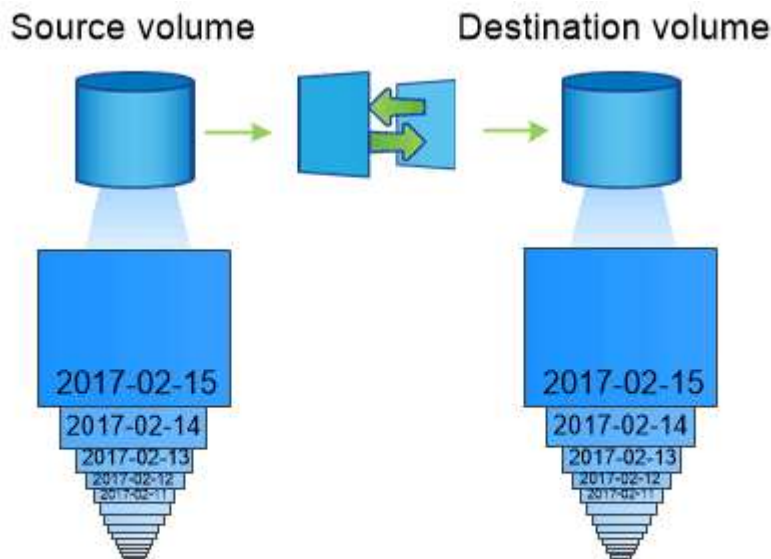
Se il sito primario è ancora disponibile per la fornitura dei dati, è possibile semplicemente trasferire di nuovo i dati necessari e non servire i client dal mirror. Come implica il caso di utilizzo del failover, i controller sul sistema secondario devono essere equivalenti o quasi equivalenti ai controller sul sistema primario per fornire i dati in modo efficiente dallo storage mirrorato.

## Relazioni di data Protection

I dati vengono mirrorati a livello di volume. La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene chiamata *relazione di protezione dei dati*. I cluster in cui risiedono i volumi e le SVM che servono i dati dei volumi devono essere *peering*. Una relazione peer consente lo scambio di cluster e SVM dati in modo sicuro.

["Peering di cluster e SVM"](#)

La figura seguente illustra le relazioni di protezione dei dati di SnapMirror.



*A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.*

### Ambito delle relazioni di protezione dei dati

È possibile creare una relazione di protezione dei dati direttamente tra i volumi o tra le SVM che possiedono i volumi. In una relazione di protezione dei dati SVM, la configurazione SVM completa o parziale, dalle esportazioni NFS e dalle condivisioni SMB a RBAC, viene replicata, così come i dati nei volumi di proprietà di SVM.

È inoltre possibile utilizzare SnapMirror per applicazioni speciali di protezione dei dati:

- Una copia *mirror per la condivisione del carico* del volume root SVM garantisce che i dati rimangano accessibili in caso di interruzione o failover di un nodo.
- Una relazione di protezione dei dati tra *volumi SnapLock* consente di replicare i file WORM sullo storage secondario.

#### "Archiviazione e conformità con la tecnologia SnapLock"

- A partire da ONTAP 9.13.1, è possibile utilizzare SnapMirror asincrono per la protezione [gruppi di coerenza](#). A partire da ONTAP 9.14.1, puoi utilizzare SnapMirror asincrono per replicare le snapshot granulari del volume nel cluster di destinazione usando la relazione del gruppo di coerenza. Per ulteriori informazioni, vedere [Configurare la protezione asincrona di SnapMirror](#).

### Come vengono inizializzate le relazioni di protezione dei dati di SnapMirror

La prima volta che si richiama SnapMirror, esegue un *trasferimento baseline* dal volume di origine al volume di destinazione. La *policy SnapMirror* per la relazione definisce il contenuto della linea di base e gli eventuali aggiornamenti.

Trasferimento di riferimento con il criterio predefinito di SnapMirror `MirrorAllSnapshots` prevede i seguenti passaggi:

- Creare una copia Snapshot del volume di origine.

- Trasferire la copia Snapshot e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.
- Trasferire le copie Snapshot rimanenti, meno recenti, sul volume di origine al volume di destinazione per l'utilizzo in caso di danneggiamento del mirror "Active".

### Come vengono aggiornate le relazioni di protezione dei dati di SnapMirror

Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. La conservazione rispecchia la policy Snapshot sull'origine.

Ad ogni aggiornamento in MirrorAllSnapshots SnapMirror crea una copia Snapshot del volume di origine e trasferisce la copia Snapshot e le copie Snapshot eseguite dall'ultimo aggiornamento. Nel seguente output da `snapmirror policy show` comando per MirrorAllSnapshots policy, tenere presente quanto segue:

- Create Snapshot è "true", a indicare che MirrorAllSnapshots Crea una copia Snapshot quando SnapMirror aggiorna la relazione.
- MirrorAllSnapshots Dispone delle regole "sm\_created" e "all\_source\_snapshot", che indicano che sia la copia Snapshot creata da SnapMirror che le copie Snapshot eseguite dall'ultimo aggiornamento vengono trasferite quando SnapMirror aggiorna la relazione.

```
cluster_dst:> snapmirror policy show -policy MirrorAllSnapshots -instance

                Vserver: vs0
SnapMirror Policy Name: MirrorAllSnapshots
SnapMirror Policy Type: async-mirror
        Policy Owner: cluster-admin
            Tries Limit: 8
        Transfer Priority: normal
Ignore accesstime Enabled: false
    Transfer Restartability: always
Network Compression Enabled: false
        Create Snapshot: true
            Comment: Asynchronous SnapMirror policy for mirroring
all snapshots
                        and the latest active file system.
    Total Number of Rules: 2
            Total Keep: 2
                Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
sm_created                1  false      0  -
all_source_snapshots      1  false      0  -
```



Policy MirrorLatest

Preconfigurato MirrorLatest la policy funziona esattamente come MirrorAllSnapshots, Ad eccezione del fatto che solo la copia Snapshot creata da SnapMirror viene trasferita all’inizializzazione e all’aggiornamento.

| Schedule Prefix | Rules: SnapMirror Label | Keep | Preserve | Warn |
|-----------------|-------------------------|------|----------|------|
| -----           | -----                   | ---- | -----    | ---- |
| -               | sm_created              | 1    | false    | 0 -  |

Nozioni di base sul disaster recovery sincrono di SnapMirror

A partire da ONTAP 9.5, la tecnologia SnapMirror Synchronous (SM-S) è supportata su tutte le piattaforme FAS e AFF con almeno 16 GB di memoria e su tutte le piattaforme ONTAP Select. La tecnologia SnapMirror Synchronous è una funzionalità concessa in licenza per nodo che fornisce la replica sincrona dei dati a livello di volume.

Questa funzionalità soddisfa i requisiti normativi e nazionali per la replica sincrona in settori finanziari, sanitari e altri settori regolamentati in cui non è richiesta alcuna perdita di dati.

Operazioni di SnapMirror Synchronous consentite

Il limite del numero di operazioni di replica sincrona di SnapMirror per coppia ha dipende dal modello di controller.

La tabella seguente elenca il numero di operazioni sincroni di SnapMirror consentite per coppia ha in base al tipo di piattaforma e alla release di ONTAP.

| Piattaforma  | Versioni precedenti a ONTAP 9.9.1 | ONTAP 9.9.1 | ONTAP 9.10.1 | Da ONTAP 9.11.1 a ONTAP 9.14.1 |
|--------------|-----------------------------------|-------------|--------------|--------------------------------|
| AFF          | 80                                | 160         | 200          | 400                            |
| ASA          | 80                                | 160         | 200          | 400                            |
| FAS          | 40                                | 80          | 80           | 80                             |
| ONTAP Select | 20                                | 40          | 40           | 40                             |

Funzionalità supportate

La tabella seguente indica le funzionalità supportate con SnapMirror Synchronous e le release ONTAP in cui è disponibile il supporto.

| Funzione                                                                                                                                   | Release supportata per la prima volta | Ulteriori informazioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Antivirus sul volume primario della relazione sincrona di SnapMirror                                                                       | ONTAP 9.6                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Replica delle copie Snapshot creata dall'applicazione                                                                                      | ONTAP 9.7                             | Se una copia Snapshot viene contrassegnata con l'etichetta appropriata al momento della <code>snapshot create</code> Operazione, utilizzando l'interfaccia CLI o l'API ONTAP, SnapMirror Synchronous replica le copie Snapshot, create dall'utente o con script esterni, dopo aver terminato le applicazioni. Le copie Snapshot pianificate create utilizzando una policy Snapshot non vengono replicate. Per ulteriori informazioni sulla replica delle copie Snapshot create dall'applicazione, consultare l'articolo della Knowledge base: <a href="#">"Come replicare gli snapshot creati dall'applicazione con SnapMirror Synchronous"</a> . |
| Clona eliminazione automatica                                                                                                              | ONTAP 9.6                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Gli aggregati FabricPool con policy di tiering Nessuno, Snapshot o Auto sono supportati con origine e destinazione sincrone di SnapMirror. | ONTAP 9.5                             | Il volume di destinazione in un aggregato FabricPool non può essere impostato su tutti i criteri di tiering.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| FC                                                                                                                                         | ONTAP 9.5                             | Su tutte le reti per le quali la latenza non supera i 10ms ms.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| FC-NVMe                                                                                                                                    | ONTAP 9.7                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Cloni dei file                                                                                                                             | ONTAP 9.7                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| FPolicy sul volume primario della relazione sincrona di SnapMirror                                                                         | ONTAP 9.6                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Quote hard e soft sul volume primario della relazione di SnapMirror Synchronous                                                            | ONTAP 9.6                             | Le regole di quota non vengono replicate nella destinazione, pertanto il database di quota non viene replicato nella destinazione.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Relazioni sincrone all'interno del cluster                                                                                                 | ONTAP 9.14.1                          | L'high Availability viene fornita quando i volumi di origine e destinazione vengono posizionati su diverse coppie ha.<br>In caso di guasto dell'intero cluster, l'accesso ai volumi non sarà possibile fino al ripristino del cluster. Le relazioni sincrone intra-cluster di SnapMirror contribuiranno al limite complessivo della simultaneità <a href="#">Relazioni per coppia ha</a> .                                                                                                                                                                                                                                                        |
| ISCSI                                                                                                                                      | ONTAP 9.5                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Cloni LUN e cloni namespace NVMe                                                                                                           | ONTAP 9.7                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Cloni LUN supportati dalle copie Snapshot create dalle applicazioni                                                                        | ONTAP 9.7                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                                                                      |              |                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Accesso al protocollo misto (NFS v3 e SMB)                                           | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                              |
| Ripristino NDMP/NDMP                                                                 | ONTAP 9.13.1 | Sia il cluster di origine che quello di destinazione devono eseguire ONTAP 9.13.1 o versione successiva per utilizzare NDMP con SnapMirror Synchronous. Per ulteriori informazioni, vedere <a href="#">Trasferire i dati utilizzando la copia ndmp</a> .                                                     |
| Operazioni sincrone SnapMirror senza interruzioni (NDO) solo su piattaforme AFF/ASA. | ONTAP 9.12.1 | Il supporto per operazioni senza interruzioni consente di eseguire molte attività di manutenzione comuni senza pianificare i tempi di inattività. Le operazioni supportate includono takeover e giveback e spostamento del volume, a condizione che un singolo nodo sopravviva tra ciascuno dei due cluster. |
| NFS v4,2                                                                             | ONTAP 9.10.1 |                                                                                                                                                                                                                                                                                                              |
| NFS v4,3                                                                             | ONTAP 9.5    |                                                                                                                                                                                                                                                                                                              |
| NFS v4.0                                                                             | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                              |
| NFS v4,1                                                                             | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                              |
| NVMe/TCP                                                                             | 9.10.1       |                                                                                                                                                                                                                                                                                                              |
| Rimozione della limitazione di frequenza delle operazioni con metadati elevati       | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                              |
| Sicurezza per i dati sensibili in transito con crittografia TLS 1.2                  | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                              |
| Ripristino di file singoli e file parziale                                           | ONTAP 9.13.1 |                                                                                                                                                                                                                                                                                                              |
| SMB 2.0 o versione successiva                                                        | ONTAP 9.6    |                                                                                                                                                                                                                                                                                                              |
| Cascata del mirror sincrono di SnapMirror                                            | ONTAP 9.6    | Il rapporto dal volume di destinazione della relazione di SnapMirror Synchronous deve essere una relazione di SnapMirror asincrono.                                                                                                                                                                          |

|                                                                  |              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disaster recovery SVM                                            | ONTAP 9.6    | <p>* Una fonte di SnapMirror Synchronous può anche essere un'origine di disaster recovery SVM, ad esempio una configurazione fan-out con SnapMirror Synchronous come una tappa e il disaster recovery SVM come l'altra.</p> <p>* Un'origine SnapMirror Synchronous non può essere una destinazione di disaster recovery SVM perché SnapMirror Synchronous non supporta la catena di un'origine di data Protection. È necessario rilasciare la relazione sincrona prima di eseguire la risincronizzazione in caso di disaster recovery delle SVM nel cluster di destinazione.</p> <p>* Una destinazione SnapMirror Synchronous non può essere un'origine di disaster recovery SVM perché il disaster recovery SVM non supporta la replica dei volumi DP. Una risincronizzazione in flip dell'origine sincrona causerebbe il disaster recovery della SVM, escludendo il volume DP nel cluster di destinazione.</p> |
| Ripristino basato su nastro sul volume di origine                | ONTAP 9.13.1 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Parità di timestamp tra volumi di origine e destinazione per NAS | ONTAP 9.6    | <p>Se è stato eseguito l'aggiornamento da ONTAP 9,5 a ONTAP 9,6, l'indicatore data e ora viene replicato solo per i file nuovi e modificati nel volume di origine. L'indicatore orario dei file esistenti nel volume di origine non viene sincronizzato.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Funzionalità non supportate

Le seguenti funzionalità non sono supportate con le relazioni di SnapMirror sincrone:

- Gruppi di coerenza
- Sistemi DP\_Optimized (DPO)
- Volumi FlexGroup
- Volumi FlexCache
- Rallentamento globale
- In una configurazione fan-out, una sola relazione può essere una relazione sincrona di SnapMirror; tutte le altre relazioni del volume di origine devono essere relazioni asincrone di SnapMirror.
- Spostamento delle LUN
- Configurazioni MetroCluster
- I LUN di accesso MISTI SAN e NVMe e gli spazi dei nomi NVMe non sono supportati sullo stesso volume o SVM.
- SnapCenter
- Volumi SnapLock
- Copie Snapshot a prova di manomissione

- Backup o ripristino su nastro utilizzando dump e SMTape sul volume di destinazione
- Throughput floor (QoS min) per volumi di origine
- SnapRestore volume
- Vol

## Modalità operative

SnapMirror Synchronous dispone di due modalità operative in base al tipo di policy SnapMirror utilizzata:

- **Sync mode** in modalità Sync, le operazioni di i/o dell'applicazione vengono inviate in parallelo ai sistemi di storage primario e secondario. Se la scrittura sullo storage secondario non viene completata per qualsiasi motivo, l'applicazione può continuare a scrivere sullo storage primario. Quando la condizione di errore viene corretta, la tecnologia SnapMirror Synchronous risincronizza automaticamente con lo storage secondario e riprende la replica dallo storage primario allo storage secondario in modalità sincrona. In modalità Sync, RPO=0 e RTO sono molto bassi fino a quando non si verifica un errore di replica secondario, in cui RPO e RTO diventano indeterminati, ma pari al tempo necessario per riparare il problema che ha causato il fallimento della replica secondaria e il completamento della risincronizzazione.
- **Modalità StrictSync** SnapMirror Synchronous può funzionare in modalità StrictSync. Se la scrittura sullo storage secondario non viene completata per qualsiasi motivo, l'i/o dell'applicazione non riesce, garantendo che lo storage primario e secondario siano identici. L'i/o dell'applicazione verso il primario riprende solo dopo che la relazione SnapMirror ritorna a InSync stato. In caso di guasto dello storage primario, l'i/o dell'applicazione può essere ripristinato sullo storage secondario, dopo il failover, senza perdita di dati. In modalità StrictSync, l'RPO è sempre zero e l'RTO è molto basso.

## Stato della relazione

Lo stato di una relazione sincrona di SnapMirror è sempre in InSync stato durante il normale funzionamento. Se il trasferimento di SnapMirror non riesce per qualsiasi motivo, la destinazione non è sincronizzata con l'origine e può andare al OutofSync stato.

Per le relazioni sincroni di SnapMirror, il sistema verifica automaticamente lo stato della relazione (InSync oppure OutofSync) a intervalli fissi. Se lo stato della relazione è OutofSync, ONTAP attiva automaticamente il processo di risincronizzazione automatica per riportare la relazione a InSync stato. La risincronizzazione automatica viene attivata solo se il trasferimento non riesce a causa di un'operazione, ad esempio un failover dello storage non pianificato all'origine o alla destinazione o un'interruzione della rete. Operazioni avviate dall'utente come `snapmirror quiesce` e `snapmirror break` non attivano la risincronizzazione automatica.

Se lo stato della relazione diventa OutofSync Per una relazione sincrona di SnapMirror in modalità StrictSync, tutte le operazioni di i/o sul volume primario vengono interrotte. Il OutofSync lo stato per la relazione sincrona di SnapMirror in modalità Sync non è disgregante per il principale e le operazioni di i/o sono consentite sul volume primario.

## Informazioni correlate

["Report tecnico NetApp 4733: Configurazione sincrona e Best practice di SnapMirror"](#)

## Informazioni sui carichi di lavoro supportati dalle policy di StrictSync e Sync

Le policy StrictSync e Sync supportano tutte le applicazioni basate su LUN con protocolli FC, iSCSI e FC-NVMe, nonché i protocolli NFSv3 e NFSv4 per applicazioni aziendali come database, VMware, quota, SMB e così via. A partire da ONTAP 9.6, SnapMirror

Synchronous può essere utilizzato per i file service aziendali come EDA (Electronic Design Automation), home directory e carichi di lavoro di build del software.

In ONTAP 9.5, per una policy di sincronizzazione, è necessario considerare alcuni aspetti importanti durante la selezione dei carichi di lavoro NFSv3 o NFSv4. La quantità di operazioni di lettura o scrittura dei dati da parte dei carichi di lavoro non è una considerazione, in quanto la policy Sync può gestire elevati carichi di lavoro io in lettura o scrittura. In ONTAP 9.5, i carichi di lavoro che presentano una creazione di file, una creazione di directory, modifiche ai permessi dei file o modifiche ai permessi delle directory eccessive potrebbero non essere adatti (tali carichi di lavoro vengono definiti carichi di lavoro con metadati elevati). Un tipico esempio di workload con metadati elevati è un workload DevOps in cui è possibile creare più file di test, eseguire l'automazione ed eliminare i file. Un altro esempio è rappresentato dal carico di lavoro di creazione parallela che genera più file temporanei durante la compilazione. L'impatto di un elevato tasso di attività di scrittura dei metadati è che può causare la temporanea interruzione della sincronizzazione tra i mirror, che blocca gli iOS di lettura e scrittura dal client.

A partire da ONTAP 9.6, queste limitazioni vengono rimosse e SnapMirror Synchronous può essere utilizzato per i carichi di lavoro dei file service aziendali che includono ambienti multiutente, come home directory e carichi di lavoro di build del software.

#### **Informazioni correlate**

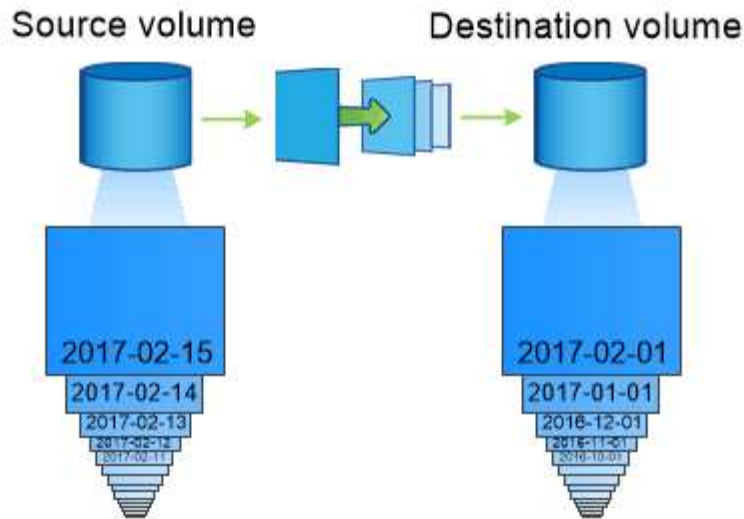
["Procedure consigliate e configurazione sincrona di SnapMirror"](#)

## **Archiviazione del vault con la tecnologia SnapMirror**

I criteri di vault di SnapMirror sostituiscono la tecnologia SnapVault in ONTAP 9.3 e versioni successive. Si utilizza un criterio di vault SnapMirror per la replica delle copie Snapshot disk-to-disk per la conformità agli standard e altri scopi correlati alla governance. A differenza di una relazione SnapMirror, in cui la destinazione contiene di solito solo le copie Snapshot attualmente nel volume di origine, una destinazione del vault conserva in genere le copie Snapshot point-in-time create in un periodo molto più lungo.

È possibile conservare copie Snapshot mensili dei dati per un periodo di 20 anni, ad esempio per rispettare le normative contabili governative per la propria azienda. Poiché non è necessario fornire dati dallo storage del vault, è possibile utilizzare dischi più lenti e meno costosi sul sistema di destinazione.

La figura seguente illustra le relazioni di protezione dei dati del vault SnapMirror.



*A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.*

#### **Come vengono inizializzate le relazioni di protezione dei dati del vault**

Il criterio SnapMirror per la relazione definisce il contenuto della linea di base e gli eventuali aggiornamenti.

Un trasferimento di riferimento con la policy di default del vault `XDPDefault` esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e i blocchi di dati a cui fa riferimento al volume di destinazione. A differenza delle relazioni SnapMirror, un backup del vault non include copie Snapshot precedenti nella linea di base.

#### **Come vengono aggiornate le relazioni di protezione dei dati del vault**

Gli aggiornamenti sono asincroni, in base alla pianificazione configurata. Le regole definite nella policy per la relazione identificano quali nuove copie Snapshot includere negli aggiornamenti e quante copie conservare. Le etichette definite nella policy ("monthly," ad esempio) devono corrispondere a una o più etichette definite nella policy Snapshot sull'origine. In caso contrario, la replica non riesce.

Ad ogni aggiornamento in `XDPDefault` SnapMirror trasferisce le copie Snapshot eseguite dall'ultimo aggiornamento, a condizione che le etichette corrispondano alle etichette definite nelle regole dei criteri. Nel seguente output da `snapmirror policy show` comando per `XDPDefault` policy, tenere presente quanto segue:

- `Create Snapshot` è "false", a indicare che `XDPDefault` Non crea una copia Snapshot quando SnapMirror aggiorna la relazione.
- `XDPDefault` Dispone di regole "daily" e "settimanale", che indicano che tutte le copie Snapshot con etichette corrispondenti sull'origine vengono trasferite quando SnapMirror aggiorna la relazione.

```
cluster_dst:> snapmirror policy show -policy XDPDefault -instance

                Vserver: vs0
SnapMirror Policy Name: XDPDefault
SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                Tries Limit: 8
                Transfer Priority: normal
Ignore accesstime Enabled: false
Transfer Restartability: always
Network Compression Enabled: false
                Create Snapshot: false
                Comment: Default policy for XDP relationships with
daily and weekly
                        rules.
                Total Number of Rules: 2
                Total Keep: 59
                Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
                        daily                7   false    0 -
-
                        weekly              52   false    0 -
-
```

## Nozioni di base sulla replica unificata di SnapMirror

SnapMirror *replica unificata* consente di configurare il disaster recovery e l'archiviazione sullo stesso volume di destinazione. Quando la replica unificata è appropriata, offre vantaggi in termini di riduzione della quantità di storage secondario necessaria, limitazione del numero di trasferimenti di riferimento e riduzione del traffico di rete.

### Come vengono inizializzate le relazioni unificate di protezione dei dati

Come con SnapMirror, la protezione unificata dei dati esegue un trasferimento di riferimento la prima volta che lo si richiama. Il criterio SnapMirror per la relazione definisce il contenuto della linea di base e gli eventuali aggiornamenti.

Un trasferimento di riferimento in base alla policy di protezione dei dati unificata predefinita `MirrorAndVault` esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e i blocchi di dati a cui fa riferimento al volume di destinazione. Come l'archiviazione del vault, la protezione unificata dei dati non include copie Snapshot precedenti nella linea di base.

### Come vengono aggiornate le relazioni unificate di protezione dei dati

Ad ogni aggiornamento in `MirrorAndVault` Policy, SnapMirror crea una copia Snapshot del volume di



origine e trasferisce la copia Snapshot e le copie Snapshot eseguite dall'ultimo aggiornamento, a condizione che le etichette corrispondano alle etichette definite nelle regole dei criteri di Snapshot. Nel seguente output da `snapmirror policy show` comando per `MirrorAndVault` policy, tenere presente quanto segue:

- `Create Snapshot` è “true”, a indicare che `MirrorAndVault` Crea una copia Snapshot quando `SnapMirror` aggiorna la relazione.
- `MirrorAndVault` Dispone delle regole “sm\_created”, “daily” e “settimanale”, che indicano che sia la copia Snapshot creata da `SnapMirror` che le copie Snapshot con le etichette corrispondenti sull'origine vengono trasferite quando `SnapMirror` aggiorna la relazione.

```
cluster_dst:> snapmirror policy show -policy MirrorAndVault -instance

                Vserver: vs0
    SnapMirror Policy Name: MirrorAndVault
    SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                Tries Limit: 8
        Transfer Priority: normal
    Ignore accesstime Enabled: false
        Transfer Restartability: always
    Network Compression Enabled: false
                Create Snapshot: true
                Comment: A unified Synchronous SnapMirror and
SnapVault policy for
                                mirroring the latest file system and daily
and weekly snapshots.
        Total Number of Rules: 3
                Total Keep: 59
                Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
                                sm_created      1  false      0  -
-
                                daily              7  false      0  -
-
                                weekly             52  false      0  -
-
```

**Politica Unified7year**

Preconfigurato `Unified7year` la policy funziona esattamente come `MirrorAndVault`, Ad eccezione del fatto che una quarta regola trasferisce le copie Snapshot mensili e le conserva per sette anni.

| Schedule Prefix | Rules: SnapMirror Label | Keep | Preserve | Warn |
|-----------------|-------------------------|------|----------|------|
| -----           | -----                   | ---- | -----    | ---- |
| -               | sm_created              | 1    | false    | 0 -  |
| -               | daily                   | 7    | false    | 0 -  |
| -               | weekly                  | 52   | false    | 0 -  |
| -               | monthly                 | 84   | false    | 0 -  |
| -               |                         |      |          |      |

### Proteggersi da possibili danneggiamenti dei dati

La replica unificata limita il contenuto del trasferimento di riferimento alla copia Snapshot creata da SnapMirror all'inizializzazione. A ogni aggiornamento, SnapMirror crea un'altra copia Snapshot dell'origine e trasferisce tale copia Snapshot e le nuove copie Snapshot che presentano etichette corrispondenti alle etichette definite nelle regole dei criteri Snapshot.

È possibile proteggersi dalla possibilità che una copia Snapshot aggiornata venga danneggiata creando una copia dell'ultima copia Snapshot trasferita sulla destinazione. Questa "copia locale" viene conservata indipendentemente dalle regole di conservazione sull'origine, in modo che anche se l'istantanea originariamente trasferita da SnapMirror non è più disponibile sull'origine, una copia di essa sarà disponibile sulla destinazione.

### Quando utilizzare la replica unificata dei dati

È necessario valutare i vantaggi derivanti dal mantenimento di un mirror completo rispetto ai vantaggi offerti dalla replica unificata nella riduzione della quantità di storage secondario, nella limitazione del numero di trasferimenti di riferimento e nella riduzione del traffico di rete.

Il fattore chiave per determinare l'adeguatezza della replica unificata è il tasso di cambiamento del file system attivo. Un mirror tradizionale potrebbe essere più adatto a un volume che contiene copie Snapshot orarie dei log delle transazioni del database, ad esempio.

### XDP sostituisce DP come impostazione predefinita di SnapMirror

A partire da ONTAP 9.3, la modalità XDP (Extended Data Protection) di SnapMirror sostituisce la modalità DP (Data Protection) di SnapMirror come impostazione predefinita.

Prima di eseguire l'aggiornamento a ONTAP 9.12.1, è necessario convertire le relazioni di tipo DP esistenti in XDP prima di poter eseguire l'aggiornamento a ONTAP 9.12.1 e versioni successive. Per ulteriori informazioni, vedere ["Convertire una relazione di tipo DP esistente in XDP"](#).

Fino a ONTAP 9.3, SnapMirror invocato in modalità DP e SnapMirror richiamato in modalità XDP utilizzavano diversi motori di replica, con diversi approcci alla dipendenza dalla versione:

- SnapMirror invocato in modalità DP utilizzava un motore di replica *dipendente dalla versione* in cui la

versione di ONTAP doveva essere la stessa sullo storage primario e secondario:

```
cluster_dst:> snapmirror create -type DP -source-path ... -destination  
-path ...
```

- SnapMirror invocato in modalità XDP utilizzava un motore di replica *version-Flexible* che supportava diverse versioni di ONTAP sullo storage primario e secondario:

```
cluster_dst:> snapmirror create -type XDP -source-path ...  
-destination-path ...
```

Con i miglioramenti delle performance, i benefici significativi di SnapMirror flessibile per la versione superano il leggero vantaggio nel throughput di replica ottenuto con la modalità dipendente dalla versione. Per questo motivo, a partire da ONTAP 9.3, la modalità XDP è stata impostata come nuova impostazione predefinita e tutte le invocazioni della modalità DP sulla riga di comando o in script nuovi o esistenti vengono automaticamente convertite in modalità XDP.

Le relazioni esistenti non vengono influenzate. Se una relazione è già di tipo DP, continuerà ad essere di tipo DP. A partire da ONTAP 9.5, MirrorAndVault è il nuovo criterio predefinito quando non viene specificata alcuna modalità di protezione dei dati o quando viene specificata la modalità XDP come tipo di relazione. La tabella seguente mostra il comportamento che ci si può aspettare.

| Se si specifica... | Il tipo è... | Il criterio predefinito (se non si specifica un criterio) è... |
|--------------------|--------------|----------------------------------------------------------------|
| DP                 | XDP          | MirrorAllSnapshot (DR SnapMirror)                              |
| Niente             | XDP          | MirrorAndVault (replica unificata)                             |
| XDP                | XDP          | MirrorAndVault (replica unificata)                             |

Come mostrato nella tabella, i criteri predefiniti assegnati a XDP in diverse circostanze garantiscono che la conversione mantenga l'equivalenza funzionale dei tipi precedenti. Naturalmente, è possibile utilizzare policy diverse in base alle esigenze, incluse le policy per la replica unificata:

| Se si specifica... | E la policy è...  | Il risultato è... |
|--------------------|-------------------|-------------------|
| DP                 | MirrorAllSnapshot | Dr. SnapMirror    |
| XDPDefault         | SnapVault         | MirrorAndVault    |
| Replica unificata  | XDP               | MirrorAllSnapshot |
| Dr. SnapMirror     | XDPDefault        | SnapVault         |

Le uniche eccezioni alla conversione sono le seguenti:

- Le relazioni di protezione dei dati SVM continuano a essere impostate per impostazione predefinita sulla modalità DP in ONTAP 9.3 e versioni precedenti.

A partire da ONTAP 9.4, le relazioni di protezione dei dati SVM passano per impostazione predefinita alla modalità XDP.

- Le relazioni di protezione dei dati per la condivisione del carico del volume root continuano a essere predefinite in modalità DP.
- Le relazioni di protezione dei dati di SnapLock continuano a essere impostate per impostazione predefinita sulla modalità DP in ONTAP 9.4 e versioni precedenti.

A partire da ONTAP 9.5, le relazioni di protezione dei dati di SnapLock passano per impostazione predefinita alla modalità XDP.

- Le invocazioni esplicite di DP continuano a essere predefinite in modalità DP se si imposta la seguente opzione a livello di cluster:

```
options replication.create_data_protection_rels.enable on
```

Questa opzione viene ignorata se non si richiama esplicitamente DP.

## Quando un volume di destinazione cresce automaticamente

Durante il trasferimento di un mirror per la protezione dei dati, le dimensioni del volume di destinazione aumentano automaticamente se il volume di origine è cresciuto, a condizione che nell'aggregato sia presente spazio disponibile che contiene il volume.

Questo comportamento si verifica indipendentemente da qualsiasi impostazione di crescita automatica sulla destinazione. Non puoi limitare la crescita del volume o impedire a ONTAP di crescere.

Per impostazione predefinita, i volumi di protezione dei dati sono impostati su `grow_shrink` modalità di dimensionamento automatico, che consente al volume di crescere o ridursi in risposta alla quantità di spazio utilizzato. La dimensione automatica massima per i volumi di protezione dei dati è uguale alla dimensione massima FlexVol e dipende dalla piattaforma. Ad esempio:

- FAS6220, volume DP predefinito max-autodize = 70 TB
- FAS8200, volume DP predefinito max-autodize = 100 TB

Per ulteriori informazioni, vedere ["NetApp Hardware Universe"](#).

## Implementazioni di protezione dei dati fan-out e cascata

È possibile utilizzare un'implementazione *fan-out* per estendere la protezione dei dati a più sistemi secondari. È possibile utilizzare un'implementazione *Cascade* per estendere la protezione dei dati ai sistemi terziari.

Le implementazioni fan-out e cascata supportano qualsiasi combinazione di DR SnapMirror, SnapVault o replica unificata; tuttavia, le relazioni sincrone SnapMirror (supportate a partire da ONTAP 9.5) supportano solo implementazioni fan-out con una o più relazioni SnapMirror asincrone e non supportano implementazioni a cascata. Solo una relazione nella configurazione fan-out può essere una relazione sincrona di SnapMirror,

mentre tutte le altre relazioni del volume di origine devono essere relazioni asincrone di SnapMirror. [Continuità aziendale di SnapMirror](#) (Supportato a partire da ONTAP 9.8) supporta anche le configurazioni fan-out.



È possibile utilizzare un'implementazione *fan-in* per creare relazioni di protezione dei dati tra più sistemi primari e un singolo sistema secondario. Ogni relazione deve utilizzare un volume diverso sul sistema secondario.

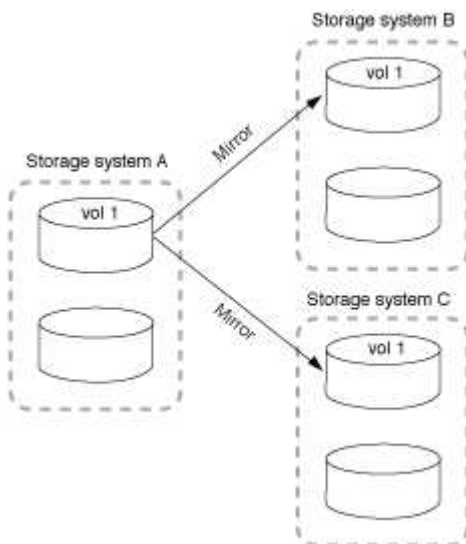


Tenere presente che la risincronizzazione dei volumi che fanno parte di una configurazione fan-out o a cascata può richiedere più tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.

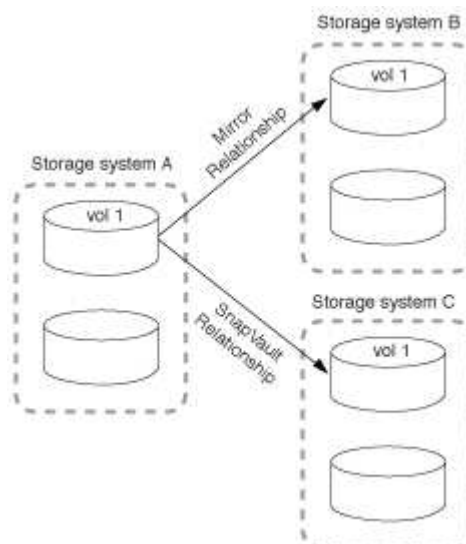
## Come funzionano le implementazioni fan-out

SnapMirror supporta le implementazioni fan-out di *mirror multipli* e *mirror-vault*.

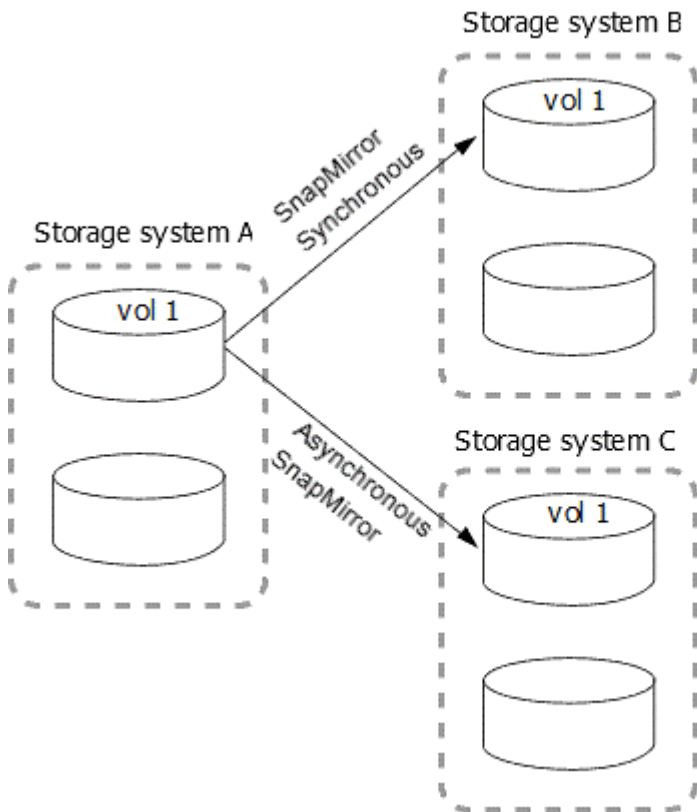
Un'implementazione fan-out con mirror multipli consiste in un volume di origine che ha una relazione di mirroring con più volumi secondari.



Un'implementazione fan-out del vault mirror è costituita da un volume di origine che ha una relazione di mirroring con un volume secondario e una relazione SnapVault con un volume secondario diverso.



A partire da ONTAP 9.5, è possibile avere implementazioni fan-out con relazioni sincrone di SnapMirror; tuttavia, solo una relazione nella configurazione fan-out può essere una relazione sincrona di SnapMirror, tutte le altre relazioni dal volume di origine devono essere relazioni asincrone di SnapMirror.

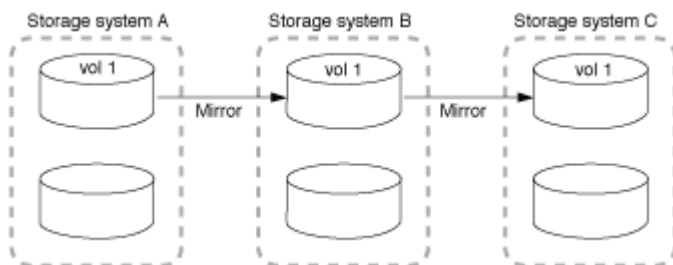


### Come funzionano le implementazioni a cascata

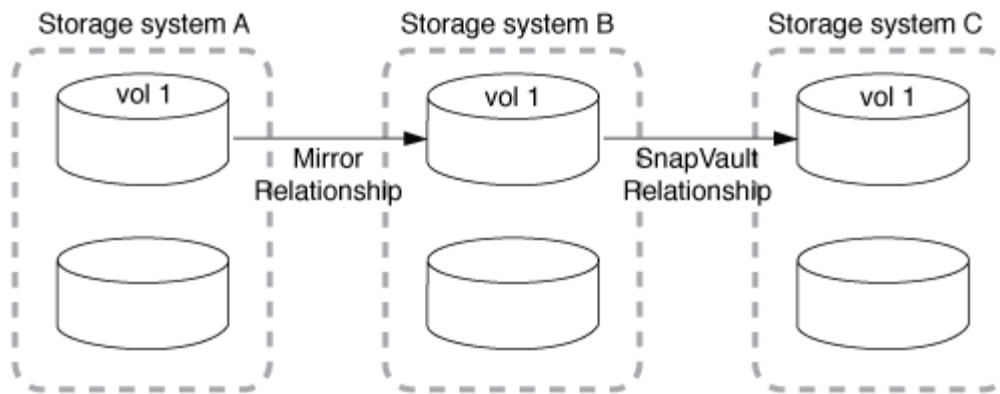
SnapMirror supporta le implementazioni a cascata di *mirror-mirror*, *mirror-vault*, *vault-mirror* e *vault-vault*.

Un'implementazione a cascata di mirror consiste in una catena di relazioni in cui un volume di origine viene mirrorato su un volume secondario e il volume secondario viene mirrorato su un volume terzo. Se il volume secondario non è più disponibile, è possibile sincronizzare la relazione tra il volume primario e il volume terzo senza eseguire un nuovo trasferimento di riferimento.

A partire da ONTAP 9.6, le relazioni sincrone di SnapMirror sono supportate in una distribuzione a cascata con mirror. Solo i volumi primari e secondari possono trovarsi in una relazione sincrona di SnapMirror. La relazione tra i volumi secondari e i volumi terziari deve essere asincrona.



Un'implementazione a cascata del vault mirror consiste in una catena di relazioni in cui un volume di origine viene mirrorato su un volume secondario e il volume secondario viene vault su un volume terzo.



Sono supportate anche le implementazioni Vault-Mirror e, a partire da ONTAP 9.2, Vault-Vault Cascade:

- Un'implementazione a cascata del vault-mirror consiste in una catena di relazioni in cui un volume di origine viene vault su un volume secondario e il volume secondario viene mirrorato su un volume terzo.
- (A partire da ONTAP 9.2) Una distribuzione a cascata di vault è costituita da una catena di relazioni in cui un volume di origine viene vault su un volume secondario e il volume secondario viene vault su un volume terzo.

#### Ulteriori letture

- [Ripristino della protezione in una configurazione fan-out con SM-BC](#)

## Licenze SnapMirror

### Panoramica sulle licenze di SnapMirror

A partire da ONTAP 9.3, le licenze sono state semplificate per la replica tra istanze di ONTAP. Nelle versioni di ONTAP 9, la licenza SnapMirror supporta le relazioni di vault e mirror. Puoi utilizzare una licenza SnapMirror per supportare la replica ONTAP per casi d'utilizzo di backup e disaster recovery.

Prima della release di ONTAP 9.3, era necessaria una licenza SnapVault separata per configurare le relazioni *vault* tra le istanze di ONTAP, in cui l'istanza DP poteva mantenere un numero più elevato di copie Snapshot per supportare i casi d'utilizzo del backup con tempi di conservazione più lunghi, inoltre, era necessaria una licenza SnapMirror per configurare relazioni *mirror* tra istanze di ONTAP, in cui ciascuna istanza di ONTAP conservava lo stesso numero di copie Snapshot (ovvero un'immagine *mirror*) per supportare i casi d'utilizzo di disaster recovery al fine di rendere possibili i failover dei cluster. Le licenze SnapMirror e SnapVault continuano a essere utilizzate e supportate per le release di ONTAP 8.x e 9.x.

Mentre le licenze SnapVault continuano a funzionare e sono supportate per entrambe le release di ONTAP 8.x e 9.x, la licenza SnapMirror può essere utilizzata al posto di una licenza SnapVault e può essere utilizzata sia per le configurazioni mirror che per quelle del vault.

Per la replica asincrona di ONTAP, a partire da ONTAP 9.3 viene utilizzato un singolo motore di replica unificato per configurare i criteri XDP (Extended Data Protection Mode), in cui la licenza SnapMirror può essere configurata per un criterio mirror, un criterio di vault o un criterio di vault mirror. È necessaria una licenza SnapMirror sia per i cluster di origine che per quelli di destinazione. Se è già installata una licenza SnapVault, non è necessaria alcuna licenza SnapMirror. La licenza perpetua asincrona SnapMirror è inclusa nella suite software ONTAP One installata sui nuovi sistemi AFF e FAS.

I limiti di configurazione per la protezione dei dati vengono determinati in base a diversi fattori, tra cui la

versione di ONTAP, la piattaforma hardware e le licenze installate. Per ulteriori informazioni, vedere ["Hardware Universe"](#).

### Licenza SnapMirror Synchronous

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror. Per creare una relazione sincrona con SnapMirror sono necessarie le seguenti licenze:

- La licenza SnapMirror Synchronous è richiesta sia sul cluster di origine che sul cluster di destinazione.

La licenza SnapMirror Synchronous è parte di ["Suite di licenze ONTAP One"](#).

Se il sistema è stato acquistato prima di giugno 2019 con un pacchetto Premium o Flash, è possibile scaricare una chiave master NetApp per ottenere la licenza SnapMirror Synchronous richiesta dal sito di supporto NetApp: ["Chiavi di licenza master"](#).

- La licenza SnapMirror è richiesta sia sul cluster di origine che sul cluster di destinazione.

### Licenza SnapMirror Cloud

A partire da ONTAP 9.8, la licenza di SnapMirror Cloud offre la replica asincrona delle copie Snapshot dalle istanze di ONTAP agli endpoint dello storage a oggetti. Le destinazioni di replica possono essere configurate utilizzando archivi di oggetti on-premise e servizi di storage a oggetti cloud pubblico compatibili con S3 e S3. Le relazioni cloud di SnapMirror sono supportate dai sistemi ONTAP alle destinazioni di storage a oggetti pre-qualificate.

SnapMirror Cloud non è disponibile come licenza standalone. È necessaria una sola licenza per cluster ONTAP. Oltre a una licenza SnapMirror Cloud, è necessaria anche la licenza SnapMirror asincrona.

Per creare una relazione SnapMirror Cloud sono necessarie le seguenti licenze:

- Sia una licenza SnapMirror che una licenza SnapMirror Cloud per la replica direttamente nell'endpoint dell'archivio di oggetti.
- Quando si configura un flusso di lavoro di replica multi-policy (ad esempio, da disco a disco a cloud), è necessaria una licenza SnapMirror su tutte le istanze di ONTAP, mentre la licenza SnapMirror Cloud è richiesta solo per il cluster di origine che esegue la replica direttamente sull'endpoint dello storage a oggetti.

A partire da ONTAP 9.9.1, è possibile ["Utilizza System Manager per la replica SnapMirror Cloud"](#).

Un elenco delle applicazioni di terze parti autorizzate di SnapMirror Cloud è pubblicato sul sito Web di NetApp.

### Licenza ottimizzata per la protezione dei dati

Le licenze DPO (Data Protection Optimized) non vengono più vendute e il DPO non è supportato sulle piattaforme correnti; tuttavia, se si dispone di una licenza DPO installata su una piattaforma supportata, NetApp continua a fornire supporto fino alla fine della disponibilità di tale piattaforma.

DPO non è incluso nel pacchetto di licenze di ONTAP One e non è possibile eseguire l'aggiornamento al pacchetto di licenze di ONTAP One se la licenza DPO è installata su un sistema.

Per informazioni sulle piattaforme supportate, vedere ["Hardware Universe"](#).



## Installare le licenze di SnapMirror Cloud

È possibile orchestrare le relazioni con SnapMirror Cloud utilizzando applicazioni di backup di terze parti prequalificate. A partire da ONTAP 9.9.1, puoi anche utilizzare System Manager per orchestrare la replica cloud di SnapMirror. Le licenze di capacità di SnapMirror e SnapMirror Cloud sono necessarie quando si utilizza System Manager per orchestrare ONTAP on-premise ai backup di storage a oggetti. Devi anche richiedere e installare la licenza SnapMirror Cloud API.

### A proposito di questa attività

Le licenze di SnapMirror Cloud e S3 SnapMirror sono licenze cluster, non di nodi, quindi *non* vengono fornite con il bundle della licenza di ONTAP One. Queste licenze sono incluse nel pacchetto di compatibilità ONTAP One separato. Per abilitare SnapMirror Cloud, devi richiedere questo bundle.

Inoltre, l'orchestrazione di System Manager dei backup SnapMirror Cloud nello storage a oggetti richiede una chiave SnapMirror Cloud API. Si tratta di una licenza API a singola istanza estesa a tutto il cluster, che non richiede l'installazione su ogni nodo del cluster.

### Fasi

Devi richiedere e scaricare il bundle di compatibilità di ONTAP ONE e la licenza API di SnapMirror Cloud, quindi installarli utilizzando System Manager.

1. Individuare e registrare l'UUID del cluster per il cluster che si desidera concedere in licenza.

L'UUID del cluster è necessario quando invii la richiesta di ordinare il bundle di compatibilità di ONTAP One per il tuo cluster.

2. Contatta il tuo team di vendita NetApp e richiedi il pacchetto compatibilità ONTAP One.
3. Richiedere la licenza SnapMirror Cloud API seguendo le istruzioni fornite sul sito di supporto NetApp.

["Richiedere la chiave di licenza API di SnapMirror Cloud"](#)

4. Una volta ricevuti e scaricati i file di licenza, utilizzare Gestione sistema per caricare nel cluster la compatibilità cloud NLF di ONTAP e l'API cloud di SnapMirror NLF:
  - a. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
  - b. Nella finestra **Impostazioni**, fare clic su **licenze**.
  - c. Nella finestra **licenze**, fare clic su **+ Add**.
  - d. Nella finestra di dialogo **Aggiungi licenza**, fare clic su **Sfoglia** per selezionare l'NLF scaricato, quindi fare clic su **Aggiungi** per caricare il file nel cluster.

### Informazioni correlate

["Eseguire il backup dei dati nel cloud utilizzando SnapMirror"](#)

["Ricerca licenze software NetApp"](#)

## Miglioramenti delle funzionalità dei sistemi DPO

A partire da ONTAP 9.6, il numero massimo di volumi FlexVol supportati aumenta quando viene installata la licenza DP\_Optimized (DPO). A partire da ONTAP 9.4, i sistemi con licenza DPO supportano il backoff di SnapMirror, la deduplica in background tra volumi,

## l'utilizzo di blocchi Snapshot come donatori e la compattazione.

A partire da ONTAP 9.6, il numero massimo di volumi FlexVol supportati sui sistemi secondari o di protezione dei dati è aumentato, consentendo di scalare fino a 2,500 volumi FlexVol per nodo o fino a 5,000 in modalità di failover. L'aumento dei volumi FlexVol viene abilitato con "[Licenza DP\\_Optimized \(DPO\)](#)". R "[Licenza SnapMirror](#)" è comunque necessario sia sui nodi di origine che su quelli di destinazione.

A partire da ONTAP 9.4, ai sistemi DPO sono stati apportati i seguenti miglioramenti:

- Backoff di SnapMirror: Nei sistemi DPO, al traffico di replica viene assegnata la stessa priorità dei carichi di lavoro client.

Il backoff di SnapMirror è disattivato per impostazione predefinita nei sistemi DPO.

- Deduplica del volume in background e deduplica del cross-volume in background: La deduplica del volume in background e la deduplica del cross-volume in background sono abilitate nei sistemi DPO.

È possibile eseguire `storage aggregate efficiency cross-volume-dedupe start -aggregate aggregate_name -scan-old-data true` per deduplicare i dati esistenti. La Best practice consiste nell'eseguire il comando durante le ore di lavoro fuori dalle ore di punta per ridurre l'impatto sulle performance.

- Maggiori risparmi utilizzando i blocchi Snapshot come donatori: I blocchi di dati che non sono disponibili nel file system attivo ma sono intrappolati nelle copie Snapshot vengono utilizzati come donatori per la deduplica dei volumi.

I nuovi dati possono essere deduplicati con i dati intrappolati nelle copie Snapshot, condividendo efficacemente anche i blocchi Snapshot. L'aumento dello spazio dei donatori offre maggiori risparmi, soprattutto quando il volume dispone di un elevato numero di copie Snapshot.

- Compaction (compattazione): La compattazione dei dati è attivata per impostazione predefinita sui volumi DPO.

## Gestire la replica del volume SnapMirror

### Workflow di replica di SnapMirror

SnapMirror offre tre tipi di relazione di protezione dei dati: Disaster recovery SnapMirror, archivio (precedentemente noto come SnapVault) e replica unificata. È possibile seguire lo stesso flusso di lavoro di base per configurare ogni tipo di relazione.

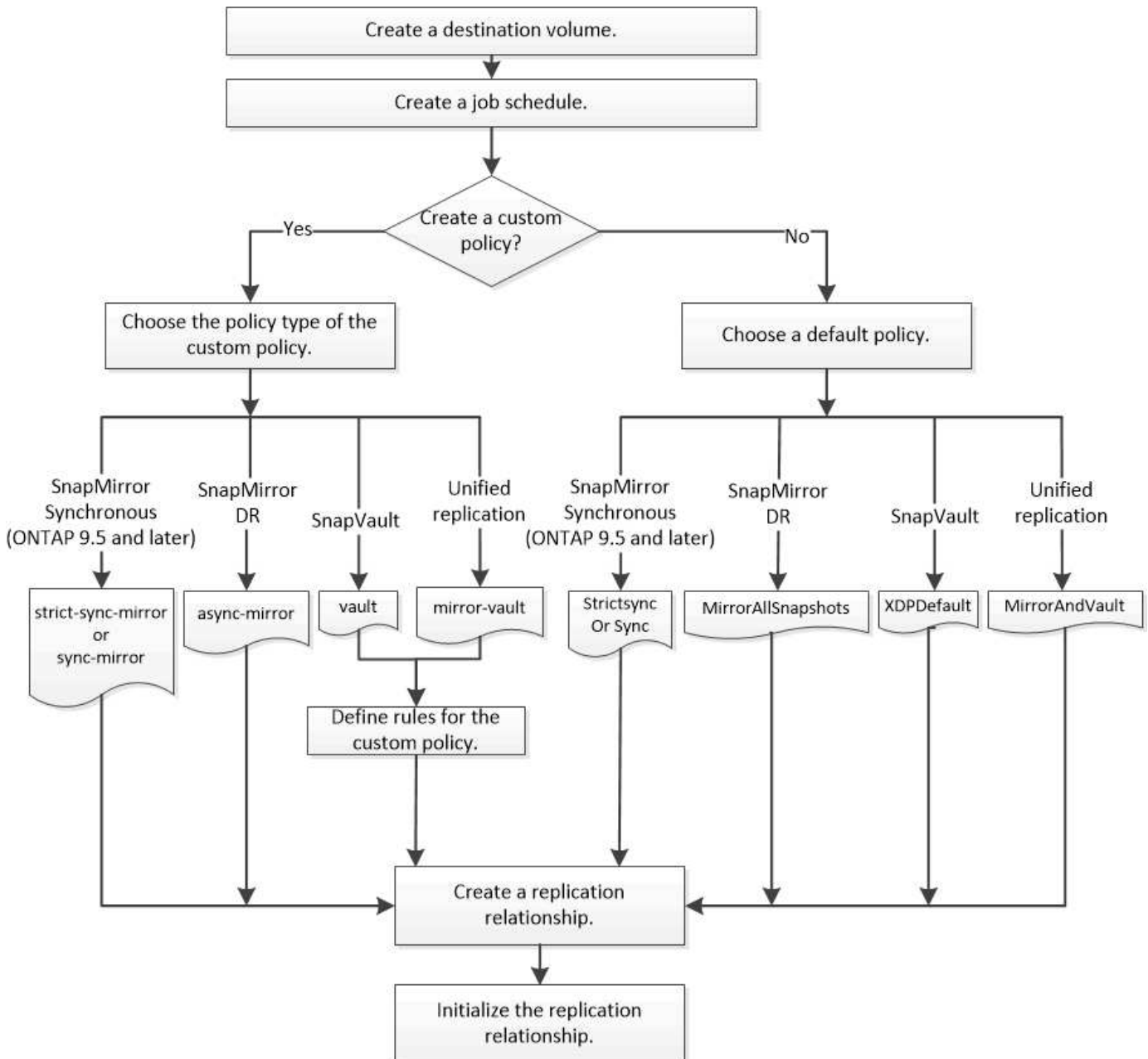
A partire dalla disponibilità generale in ONTAP 9.9.1, la business continuity di SnapMirror (SM-BC) offre un obiettivo di tempo di ripristino zero (RTO zero) o un failover delle applicazioni trasparente (TAF) per consentire il failover automatico delle applicazioni business-critical negli ambienti SAN. SM-BC è supportato in configurazioni con due cluster AFF o due cluster ASA (All-Flash SAN Array).

["Documentazione NetApp: SnapMirror Business Continuity"](#)

Per ogni tipo di relazione di protezione dei dati di SnapMirror, il flusso di lavoro è lo stesso: Creare un volume di destinazione, creare una pianificazione dei processi, specificare una policy, creare e inizializzare la relazione.

A partire da ONTAP 9.3, è possibile utilizzare `snapmirror protect` comando per configurare una relazione

di protezione dei dati in un singolo passaggio. Anche se si utilizza `snapmirror protect`, è necessario comprendere ogni fase del flusso di lavoro.



## Configurare una relazione di replica in un'unica fase

A partire da ONTAP 9.3, è possibile utilizzare `snapmirror protect` comando per configurare una relazione di protezione dei dati in un singolo passaggio. Specificare un elenco di volumi da replicare, una SVM sul cluster di destinazione, una pianificazione dei processi e un criterio SnapMirror. `snapmirror protect` fa il resto.

### Di cosa hai bisogno

- I cluster di origine e di destinazione e le SVM devono essere peering.

["Peering di cluster e SVM"](#)

- La lingua del volume di destinazione deve essere la stessa del volume di origine.

### A proposito di questa attività

Il `snapmirror protect` Il comando sceglie un aggregato associato alla SVM specificata. Se nessun aggregato è associato alla SVM, sceglie tra tutti gli aggregati del cluster. La scelta dell'aggregato si basa sulla quantità di spazio libero e sul numero di volumi sull'aggregato.

Il `snapmirror protect` il comando esegue quindi le seguenti operazioni:

- Crea un volume di destinazione con un tipo e una quantità di spazio riservato appropriati per ciascun volume nell'elenco di volumi da replicare.
- Configura una relazione di replica appropriata per il criterio specificato.
- Inizializza la relazione.

Il nome del volume di destinazione è del modulo `source_volume_name_dst`. In caso di conflitto con un nome esistente, il comando aggiunge un numero al nome del volume. È possibile specificare un prefisso e/o un suffisso nelle opzioni dei comandi. Il suffisso sostituisce quello fornito dal sistema `dst` suffisso.

In ONTAP 9.3 e versioni precedenti, un volume di destinazione può contenere fino a 251 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume di destinazione può contenere fino a 1019 copie Snapshot.



L'inizializzazione può richiedere molto tempo. `snapmirror protect` non attende il completamento dell'inizializzazione prima del completamento del lavoro. Per questo motivo, è necessario utilizzare `snapmirror show` invece di `job show` comando per determinare quando l'inizializzazione è completa.

A partire da ONTAP 9.5, è possibile creare relazioni sincroni SnapMirror utilizzando `snapmirror protect` comando.

### Fase

1. Creare e inizializzare una relazione di replica in un'unica fase:

È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

```
snapmirror protect -path-list <SVM:volume> -destination-vserver
<destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
<true|false> -destination-volume-prefix <prefix> -destination-volume
-suffix <suffix>
```



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Il `-auto-initialize` l'opzione predefinita è "true".

Nell'esempio seguente viene creata e inizializzata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy:

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB  
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule  
replication_daily
```



Se preferisci, puoi utilizzare una policy personalizzata. Per ulteriori informazioni, vedere ["Creazione di un criterio di replica personalizzato"](#).

Nell'esempio seguente viene creata e inizializzata una relazione SnapVault utilizzando l'impostazione predefinita `XDPEndpoint` policy:

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB  
-destination-vserver svm_backup -policy XDPEndpoint -schedule  
replication_daily
```

Nell'esempio seguente viene creata e inizializzata una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` policy:

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB  
-destination-vserver svm_backup -policy MirrorAndVault
```

Nell'esempio seguente viene creata e inizializzata una relazione sincrona SnapMirror utilizzando l'impostazione predefinita `Sync` policy:

```
cluster_dst:> snapmirror protect -path-list svm1:volA, svm1:volB  
-destination-vserver svm_sync -policy Sync
```



Per SnapVault e le policy di replica unificate, potrebbe essere utile definire una pianificazione per la creazione di una copia dell'ultima copia Snapshot trasferita sulla destinazione. Per ulteriori informazioni, vedere ["Definizione di una pianificazione per la creazione di una copia locale sulla destinazione"](#).

## Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina `man`.

## Configurare una relazione di replica un passaggio alla volta

### Creare un volume di destinazione

È possibile utilizzare `volume create` sulla destinazione per creare un volume di destinazione. Le dimensioni del volume di destinazione devono essere uguali o superiori a quelle del volume di origine.

## Fase

1. Creare un volume di destinazione:

```
volume create -vserver SVM -volume volume -aggregate aggregate -type DP -size size
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene creato un volume di destinazione da 2 GB denominato `volA_dst`:

```
cluster_dst::> volume create -vserver SVM_backup -volume volA_dst  
-aggregate node01_aggr -type DP -size 2GB
```

## Creare una pianificazione del processo di replica

È possibile utilizzare `job schedule cron create` per creare una pianificazione del processo di replica. La pianificazione del processo determina quando SnapMirror aggiorna automaticamente la relazione di protezione dei dati a cui viene assegnata la pianificazione.

### A proposito di questa attività

Quando si crea una relazione di protezione dei dati, viene assegnata una pianificazione dei processi. Se non si assegna una pianificazione del lavoro, è necessario aggiornare la relazione manualmente.

## Fase

1. Creare una pianificazione del processo:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

A partire da ONTAP 9.10.1, è possibile includere il server virtuale per la pianificazione del processo:

```
job schedule cron create -name job_name -vserver Vserver_name -month month  
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```



La pianificazione minima supportata (RPO) per i volumi FlexVol in un volume SnapMirror è di 5 minuti. La pianificazione minima supportata (RPO) per i volumi FlexGroup in un volume SnapMirror è di 30 minuti.

Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` il sabato alle 3:00:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

## Personalizzare un criterio di replica

### Creare un criterio di replica personalizzato

È possibile creare un criterio di replica personalizzato se il criterio predefinito per una relazione non è adatto. È possibile, ad esempio, comprimere i dati in un trasferimento di rete o modificare il numero di tentativi eseguiti da SnapMirror per trasferire le copie Snapshot.

È possibile utilizzare un criterio predefinito o personalizzato quando si crea una relazione di replica. Per un archivio personalizzato (in precedenza SnapVault) o una policy di replica unificata, è necessario definire una o più *regole* che determinano quali copie Snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento. È inoltre possibile definire una pianificazione per la creazione di copie Snapshot locali sulla destinazione.

Il *tipo di policy* del criterio di replica determina il tipo di relazione che supporta. La tabella seguente mostra i tipi di policy disponibili.

| Tipo di policy                      | Tipo di relazione                                                                 |
|-------------------------------------|-----------------------------------------------------------------------------------|
| mirror asincrono                    | Dr. SnapMirror                                                                    |
| vault                               | SnapVault                                                                         |
| vault mirror                        | Replica unificata                                                                 |
| mirror di sincronizzazione rigoroso | SnapMirror Synchronous in modalità StrictSync (supportato a partire da ONTAP 9.5) |
| sync-mirror                         | SnapMirror Synchronous in modalità Sync (supportato a partire da ONTAP 9.5)       |



Quando si crea un criterio di replica personalizzato, è consigliabile modellare il criterio dopo un criterio predefinito.

### Fase

#### 1. Creare un criterio di replica personalizzato:

```
snapmirror policy create -vserver SVM -policy policy -type async-  
mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror -comment comment  
-tries transfer_tries -transfer-priority low|normal -is-network-compression  
-enabled true|false
```

Per la sintassi completa dei comandi, vedere la pagina man.

A partire da ONTAP 9.5, è possibile specificare la pianificazione per la creazione di una pianificazione di copia Snapshot comune per le relazioni sincroni di SnapMirror utilizzando `-common-snapshot` `-schedule` parametro. Per impostazione predefinita, il programma di copia Snapshot comune per le relazioni sincrone di SnapMirror è di un'ora. È possibile specificare un valore compreso tra 30 minuti e due ore per la pianificazione della copia Snapshot per le relazioni sincroni di SnapMirror.

Nell'esempio seguente viene creato un criterio di replica personalizzato per il DR SnapMirror che consente la compressione di rete per i trasferimenti di dati:

```
cluster_dst::> snapmirror policy create -vserver svml -policy
DR_compressed -type async-mirror -comment "DR with network compression
enabled" -is-network-compression-enabled true
```

Nell'esempio seguente viene creato un criterio di replica personalizzato per SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svml -policy
my_snapvault -type vault
```

Nell'esempio seguente viene creata una policy di replica personalizzata per la replica unificata:

```
cluster_dst::> snapmirror policy create -vserver svml -policy my_unified
-type mirror-vault
```

Nell'esempio seguente viene creato un criterio di replica personalizzato per la relazione sincrona di SnapMirror in modalità StrictSync:

```
cluster_dst::> snapmirror policy create -vserver svml -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

## Al termine

Per i tipi di policy "vault" e "mirror-vault", è necessario definire le regole che determinano quali copie Snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento.

Utilizzare `snapmirror policy show` Per verificare che il criterio SnapMirror sia stato creato. Per la sintassi completa dei comandi, vedere la pagina man.

## Definire una regola per un criterio

Per le policy personalizzate con il tipo di policy "vault" o "mirror-vault", è necessario definire almeno una regola che determina quali copie Snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento. È inoltre possibile definire le regole per i criteri di default con il tipo di policy "vault" o "mirror-vault".

## A proposito di questa attività

Ogni policy con il tipo di policy "vault" o "mirror-vault" deve avere una regola che specifica quali copie Snapshot replicare. La regola "bimestrale", ad esempio, indica che devono essere replicate solo le copie Snapshot assegnate all'etichetta SnapMirror "bimestrale". Specificare l'etichetta SnapMirror quando si configura il criterio Snapshot sull'origine.

Ogni tipo di policy è associato a una o più regole definite dal sistema. Queste regole vengono assegnate



automaticamente a un criterio quando si specifica il relativo tipo di criterio. La tabella seguente mostra le regole definite dal sistema.

| Regola definita dal sistema | Utilizzato nei tipi di policy                | Risultato                                                                                                                                                          |
|-----------------------------|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sm_created                  | async-mirror, mirror-vault, Sync, StrictSync | Una copia Snapshot creata da SnapMirror viene trasferita all'inizializzazione e all'aggiornamento.                                                                 |
| all_source_snapshot         | mirror asincrono                             | Le nuove copie Snapshot sull'origine vengono trasferite all'inizializzazione e all'aggiornamento.                                                                  |
| ogni giorno                 | vault, vault mirror                          | Le nuove copie Snapshot sull'origine con l'etichetta SnapMirror "daily" vengono trasferite all'inizializzazione e all'aggiornamento.                               |
| settimanale                 | vault, vault mirror                          | Le nuove copie Snapshot sull'origine con l'etichetta SnapMirror "settimanale" vengono trasferite all'inizializzazione e all'aggiornamento.                         |
| mensile                     | vault mirror                                 | Le nuove copie Snapshot sull'origine con l'etichetta SnapMirror "mOnhly" vengono trasferite all'inizializzazione e all'aggiornamento.                              |
| coerente con l'applicazione | Sync, StrictSync                             | Le copie Snapshot con l'etichetta SnapMirror "app_coerente" sull'origine vengono replicate in modo sincrono sulla destinazione. Supportato a partire da ONTAP 9.7. |

Ad eccezione del tipo di policy "async-mirror", è possibile specificare regole aggiuntive in base alle esigenze, per i criteri predefiniti o personalizzati. Ad esempio:

- Per impostazione predefinita `MirrorAndVault` Policy, è possibile creare una regola chiamata "bimestrale" per associare le copie Snapshot sull'origine con l'etichetta "bimestrale" SnapMirror.
- Per una policy personalizzata con il tipo di policy "mirror-vault", è possibile creare una regola chiamata "bisettimanale" per far corrispondere le copie Snapshot sull'origine con l'etichetta "bisettimanale" SnapMirror.

## Fase

1. Definire una regola per un criterio:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror  
-label snapmirror-label -keep retention_count
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror bi-monthly al valore predefinito MirrorAndVault policy:

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy  
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror bi-weekly al personalizzato my\_snapvault policy:

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy  
my_snapvault -snapmirror-label bi-weekly -keep 26
```

Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror app\_consistent al personalizzato Sync policy:

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy Sync  
-snapmirror-label app_consistent -keep 1
```

È quindi possibile replicare le copie Snapshot dal cluster di origine che corrispondono a questa etichetta SnapMirror:

```
cluster_src:> snapshot create -vserver vs1 -volume voll -snapshot  
snapshot1 -snapmirror-label app_consistent
```

### Definire una pianificazione per la creazione di una copia locale sulla destinazione

Per le relazioni di replica unificate e SnapVault, è possibile proteggersi dalla possibilità che una copia Snapshot aggiornata venga danneggiata creando una copia dell'ultima copia Snapshot trasferita sulla destinazione. Questa "copia locale" viene conservata indipendentemente dalle regole di conservazione sull'origine, in modo che anche se l'istantanea originariamente trasferita da SnapMirror non è più disponibile sull'origine, una copia di essa sarà disponibile sulla destinazione.

#### A proposito di questa attività

Specificare la pianificazione per la creazione di una copia locale in `-schedule` opzione di `snapmirror policy add-rule` comando.

#### Fase

## 1. Definire una pianificazione per la creazione di una copia locale sulla destinazione:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror  
-label snapmirror-label -schedule schedule
```

Per la sintassi completa dei comandi, vedere la pagina [man](#). Per un esempio su come creare una pianificazione del lavoro, vedere ["Creazione di una pianificazione del processo di replica"](#).

Nell'esempio seguente viene aggiunto un programma per la creazione di una copia locale al valore predefinito MirrorAndVault policy:

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy  
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

Nell'esempio riportato di seguito viene aggiunto un programma per la creazione di una copia locale nel personalizzato my\_unified policy:

```
cluster_dst:> snapmirror policy add-rule -vserver svml -policy  
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

## Creare una relazione di replica

La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene definita *relazione di protezione dei dati*. È possibile utilizzare `snapmirror create` Per creare relazioni di protezione dei dati di replica unificata, SnapVault o DR SnapMirror.

### Di cosa hai bisogno

- I cluster di origine e di destinazione e le SVM devono essere peering.

["Peering di cluster e SVM"](#)

- La lingua del volume di destinazione deve essere la stessa del volume di origine.

### A proposito di questa attività

Fino a ONTAP 9.3, SnapMirror invocato in modalità DP e SnapMirror richiamato in modalità XDP utilizzavano diversi motori di replica, con diversi approcci alla dipendenza dalla versione:

- SnapMirror invocato in modalità DP utilizzava un motore di replica *dipendente dalla versione* in cui la versione di ONTAP doveva essere la stessa sullo storage primario e secondario:

```
cluster_dst:> snapmirror create -type DP -source-path ... -destination  
-path ...
```

- SnapMirror invocato in modalità XDP utilizzava un motore di replica *version-Flexible* che supportava diverse versioni di ONTAP sullo storage primario e secondario:

```
cluster_dst::> snapmirror create -type XDP -source-path ...  
-destination-path ...
```

Con i miglioramenti delle performance, i benefici significativi di SnapMirror flessibile per la versione superano il leggero vantaggio nel throughput di replica ottenuto con la modalità dipendente dalla versione. Per questo motivo, a partire da ONTAP 9.3, la modalità XDP è stata impostata come nuova impostazione predefinita e tutte le invocazioni della modalità DP sulla riga di comando o in script nuovi o esistenti vengono automaticamente convertite in modalità XDP.

Le relazioni esistenti non vengono influenzate. Se una relazione è già di tipo DP, continuerà ad essere di tipo DP. La tabella seguente mostra il comportamento che ci si può aspettare.

| Se si specifica... | Il tipo è... | Il criterio predefinito (se non si specifica un criterio) è... |
|--------------------|--------------|----------------------------------------------------------------|
| DP                 | XDP          | MirrorAllSnapshot (DR SnapMirror)                              |
| Niente             | XDP          | MirrorAllSnapshot (DR SnapMirror)                              |
| XDP                | XDP          | XDPDefault (SnapVault)                                         |

Vedere anche gli esempi della procedura riportata di seguito.

Le uniche eccezioni alla conversione sono le seguenti:

- Le relazioni di protezione dei dati SVM continuano a essere impostate per impostazione predefinita sulla modalità DP.

Specificare XDP esplicitamente per ottenere la modalità XDP predefinita `MirrorAllSnapshots` policy.

- Le relazioni di protezione dei dati con condivisione del carico continuano a essere impostate per impostazione predefinita sulla modalità DP.
- Le relazioni di protezione dei dati di SnapLock continuano a essere impostate per impostazione predefinita sulla modalità DP.
- Le invocazioni esplicite di DP continuano a essere predefinite in modalità DP se si imposta la seguente opzione a livello di cluster:

```
options replication.create_data_protection_rels.enable on
```

Questa opzione viene ignorata se non si richiama esplicitamente DP.

In ONTAP 9.3 e versioni precedenti, un volume di destinazione può contenere fino a 251 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume di destinazione può contenere fino a 1019 copie Snapshot.

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror.

## Fase

1. Dal cluster di destinazione, creare una relazione di replica:

È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
```

Per la sintassi completa dei comandi, vedere la pagina man.



Il `schedule` Il parametro non è applicabile quando si creano relazioni sincroni di SnapMirror.

Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorLatest` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy  
MirrorLatest
```

Nell'esempio seguente viene creata una relazione SnapVault utilizzando l'impostazione predefinita `XDPDefault` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy  
XDPDefault
```

Nell'esempio seguente viene creata una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` policy:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination-path  
svm_backup:volA_dst -type XDP -schedule my_daily -policy MirrorAndVault
```

Nell'esempio riportato di seguito viene creata una relazione di replica unificata utilizzando il metodo personalizzato `my_unified` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy  
my_unified
```

Nell'esempio seguente viene creata una relazione sincrona SnapMirror utilizzando l'impostazione predefinita `Sync` policy:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -policy Sync
```

Nell'esempio seguente viene creata una relazione sincrona SnapMirror utilizzando l'impostazione predefinita `StrictSync` policy:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

Nell'esempio seguente viene creata una relazione di DR di SnapMirror. Con il tipo di DP convertito automaticamente in XDP e senza alcun criterio specificato, il criterio viene automaticamente impostato su `MirrorAllSnapshots` policy:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type DP -schedule my_daily
```

Nell'esempio seguente viene creata una relazione di DR di SnapMirror. Se non viene specificato alcun tipo o criterio, il criterio viene impostato automaticamente su `MirrorAllSnapshots` policy:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -schedule my_daily
```

Nell'esempio seguente viene creata una relazione di DR di SnapMirror. Se non è stato specificato alcun criterio, il criterio viene impostato automaticamente su `XDPEndefault` policy:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

Nell'esempio seguente viene creata una relazione SnapMirror Synchronous con il criterio predefinito `SnapCenterSync`:

```
cluster_dst:> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```



Il criterio predefinito `SnapCenterSync` è di tipo `Sync`. Questo criterio replica qualsiasi copia Snapshot creata con `snapmirror-label` di "app\_coerente".

## Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

## Informazioni correlate

- ["Creazione ed eliminazione di volumi di test del failover SnapMirror"](#).

## Altri modi per farlo in ONTAP

| Per eseguire queste attività con...                                           | Guarda questo contenuto...                                       |
|-------------------------------------------------------------------------------|------------------------------------------------------------------|
| System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive) | <a href="#">"Configurare mirror e vault"</a>                     |
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)      | <a href="#">"Panoramica del backup del volume con SnapVault"</a> |

## Inizializzare una relazione di replica

Per tutti i tipi di relazione, l'inizializzazione esegue un *trasferimento baseline*: Esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione. In caso contrario, il contenuto del trasferimento dipende dalla policy.

### Di cosa hai bisogno

I cluster di origine e di destinazione e le SVM devono essere peering.

["Peering di cluster e SVM"](#)

### A proposito di questa attività

L'inizializzazione può richiedere molto tempo. Si consiglia di eseguire il trasferimento di riferimento in ore non di punta.

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror.

### Fase

1. Inizializzare una relazione di replica:

```
snapmirror initialize -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio riportato di seguito viene inizializzata la relazione tra il volume di origine volA acceso svm1 e il volume di destinazione volA\_dst acceso svm\_backup:

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

## Esempio: Configurare una cascata di vault

Un esempio mostra in termini concreti come è possibile configurare le relazioni di replica una fase alla volta. È possibile utilizzare la distribuzione a cascata del vault configurata nell'esempio per conservare più di 251 copie Snapshot etichettate "my-weekly".

### Di cosa hai bisogno

- I cluster di origine e di destinazione e le SVM devono essere peering.
- È necessario eseguire ONTAP 9.2 o versione successiva. Le Cascade del vault non sono supportate nelle versioni precedenti di ONTAP.

### A proposito di questa attività

L'esempio presuppone quanto segue:

- Le copie Snapshot sono state configurate sul cluster di origine con le etichette SnapMirror "my-daily", "my-weekly" e "my-monthly".
- Sono stati configurati volumi di destinazione denominati "Vola" nei cluster di destinazione secondari e terziari.
- Sono state configurate le pianificazioni dei processi di replica denominate "my\_snapvault" sui cluster di destinazione secondari e terziari.

L'esempio mostra come creare relazioni di replica in base a due criteri personalizzati:

- Il criterio "snapvault\_secondary" conserva 7 copie Snapshot giornaliere, 52 settimanali e 180 mensili sul cluster di destinazione secondario.
- La "snapvault\_terzo policy" conserva 250 copie Snapshot settimanali sul cluster di destinazione terzo.

### Fasi

1. Sul cluster di destinazione secondario, creare il criterio "snapvault\_secondary":

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary  
-type vault -comment "Policy on secondary for vault to vault cascade" -vserver  
svm_secondary
```

2. Nel cluster di destinazione secondario, definire la regola "y-daily `m`" per la policy:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary  
-snapmirror-label my-daily -keep 7 -vserver svm_secondary
```

3. Nel cluster di destinazione secondario, definire la regola "my-weekly" per il criterio:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary  
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. Nel cluster di destinazione secondario, definire la regola "my-monthly" per il criterio:

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary  
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. Sul cluster di destinazione secondario, verificare la policy:



```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```

```

                Vserver: svm_secondary
SnapMirror Policy Name: snapvault_secondary
SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                Tries Limit: 8
                Transfer Priority: normal
Ignore accesstime Enabled: false
                Transfer Restartability: always
Network Compression Enabled: false
                Create Snapshot: false
                Comment: Policy on secondary for vault to vault
cascade
    Total Number of Rules: 3
                Total Keep: 239
                Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
                my-daily                    7    false    0 -
-
                my-weekly                   52    false    0 -
-
                my-monthly                  180    false    0 -
-
```

6. Sul cluster di destinazione secondario, creare la relazione con il cluster di origine:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. Nel cluster di destinazione secondario, inizializzare la relazione con il cluster di origine:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. Nel cluster di destinazione terzo, creare il criterio “snapvault\_terzo”:

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. Nel cluster di destinazione terzo, definire la regola “my-weekly” per la policy:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. Nel cluster di destinazione terzo, verificare la policy:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```

                Vserver: svm_tertiary
SnapMirror Policy Name: snapvault_tertiary
SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                Tries Limit: 8
                Transfer Priority: normal
Ignore accesstime Enabled: false
                Transfer Restartability: always
Network Compression Enabled: false
                Create Snapshot: false
                Comment: Policy on tertiary for vault to vault
cascade
                Total Number of Rules: 1
                        Total Keep: 250
                                Rules: SnapMirror Label      Keep  Preserve Warn
Schedule Prefix
-----
-----
                                my-weekly      250   false      0  -
-
```

11. Nel cluster di destinazione terzo, creare la relazione con il cluster secondario:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. Nel cluster di destinazione terzo, inizializzare la relazione con il cluster secondario:

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

## Convertire una relazione di tipo DP esistente in XDP

Se si esegue l'aggiornamento a ONTAP 9.12.1 o versioni successive, è necessario convertire le relazioni di tipo DP in XDP prima di eseguire l'aggiornamento. ONTAP 9.12.1 e versioni successive non supportano le relazioni di tipo DP. È possibile convertire facilmente una relazione di tipo DP esistente in XDP per sfruttare SnapMirror flessibile in versione.

### A proposito di questa attività

- SnapMirror non converte automaticamente le relazioni di tipo DP esistenti in XDP. Per convertire la relazione, è necessario interrompere ed eliminare la relazione esistente, creare una nuova relazione XDP

e risincronizzare la relazione. Per informazioni generali, vedere ["XDP sostituisce DP come impostazione predefinita di SnapMirror"](#).

- Durante la pianificazione della conversione, è necessario tenere presente che la preparazione in background e la fase di data warehousing di una relazione SnapMirror XDP possono richiedere molto tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.



Dopo aver convertito un tipo di relazione SnapMirror da DP a XDP, le impostazioni relative allo spazio, come la dimensione automatica e la garanzia dello spazio, non vengono più replicate nella destinazione.

## Fasi

1. Dal cluster di destinazione, assicurarsi che la relazione SnapMirror sia di tipo DP, che lo stato del mirror sia SnapMirrored, che lo stato della relazione sia inattivo e che la relazione sia integra:

```
snapmirror show -destination-path <SVM:volume>
```

L'esempio seguente mostra l'output di `snapmirror show` comando:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```



Potrebbe essere utile conservare una copia di `snapmirror show` output dei comandi per tenere traccia delle impostazioni delle relazioni esistenti.

2. Dai volumi di origine e di destinazione, assicurarsi che entrambi i volumi dispongano di una copia Snapshot comune:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Nell'esempio riportato di seguito viene illustrato il `volume snapshot show` output per i volumi di origine e di destinazione:

```
cluster_src:> volume snapshot show -vserver svml -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
svml volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.
```

```
cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Per garantire che gli aggiornamenti pianificati non vengano eseguiti durante la conversione, interrompere la relazione DP-type esistente:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path  
<SVM:volume>
```

Per la sintassi completa dei comandi, vedere ["pagina man"](#).



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio seguente viene meno la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

#### 4. Interrompere la relazione di tipo DP esistente:

```
snapmirror break -destination-path <SVM:volume>
```

Per la sintassi completa dei comandi, vedere ["pagina man"](#).



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio seguente viene spezzata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

#### 5. Se l'eliminazione automatica delle copie Snapshot è attivata sul volume di destinazione, disattivarla:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_  
-enabled false
```

Nell'esempio seguente viene disattivata l'eliminazione automatica della copia Snapshot sul volume di destinazione `volA_dst`:

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup  
-volume volA_dst -enabled false
```

#### 6. Eliminare la relazione DP-type esistente:

```
snapmirror delete -destination-path <SVM:volume>
```

Per la sintassi completa dei comandi, vedere ["pagina man"](#).



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio riportato di seguito viene eliminata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

#### 7. Rilasciare la relazione di disaster recovery della SVM di origine sull'origine:

```
snapmirror release -destination-path <SVM:volume> -relationship-info  
-only true
```

L'esempio seguente rilascia la relazione di disaster recovery della SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst  
-relationship-info-only true
```

#### 8. È possibile utilizzare l'output conservato da `snapmirror show` Comando per creare la nuova relazione XDP-type:

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type XDP -schedule <schedule> -policy <policy>
```

La nuova relazione deve utilizzare lo stesso volume di origine e di destinazione. Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

L'esempio seguente crea una relazione di disaster recovery SnapMirror tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup` utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination  
-path svm_backup:volA_dst  
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

## 9. Risincronizzare i volumi di origine e di destinazione:

```
snapmirror resync -source-path <SVM:volume> -destination-path  
<SVM:volume>
```

Per migliorare il tempo di risincronizzazione, è possibile utilizzare `-quick-resync` tuttavia, è importante tenere presente che i risparmi in termini di efficienza dello storage possono andare persi. Per la sintassi completa dei comandi, vedere la pagina man: ["Comando di risync di SnapMirror"](#).



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

## 10. Se l'eliminazione automatica delle copie Snapshot è stata disattivata, riattivarla:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>  
-enabled true
```

### Al termine

1. Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror.
2. Quando il volume di destinazione SnapMirror XDP inizia ad aggiornare le copie Snapshot come definito dalla policy SnapMirror, utilizzare l'output di `snapmirror list-destinations` Dal cluster di origine per visualizzare la nuova relazione SnapMirror XDP.

## Convertire il tipo di relazione SnapMirror

A partire da ONTAP 9.5, SnapMirror Synchronous è supportato. È possibile convertire una relazione SnapMirror asincrona in una relazione SnapMirror Synchronous o viceversa senza eseguire un trasferimento di riferimento.

### A proposito di questa attività

Non è possibile convertire una relazione SnapMirror asincrona in una relazione SnapMirror Synchronous o viceversa modificando il criterio SnapMirror

### Fasi

- **Conversione di una relazione SnapMirror asincrona in una relazione SnapMirror Synchronous**
  - a. Dal cluster di destinazione, eliminare la relazione SnapMirror asincrona:



```
snapmirror delete -destination-path SVM:volume
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- b. Dal cluster di origine, rilasciare la relazione SnapMirror senza eliminare le comuni copie Snapshot:

```
snapmirror release -relationship-info-only true -destination-path  
dest_SVM:dest_volume
```

```
cluster1::>snapmirror release -relationship-info-only true  
-destination-path vs1_dr:vol1
```

- c. Dal cluster di destinazione, creare una relazione sincrona SnapMirror:

```
snapmirror create -source-path src_SVM:src_volume -destination-path  
dest_SVM:dest_volume -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path  
vs1_dr:vol1 -policy sync
```

- d. Risincronizzare la relazione sincrona di SnapMirror:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

• **Conversione di una relazione SnapMirror Synchronous in una relazione SnapMirror asincrona**

- a. Dal cluster di destinazione, interrompere la relazione sincrona di SnapMirror esistente:

```
snapmirror quiesce -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

- b. Dal cluster di destinazione, eliminare la relazione SnapMirror asincrona:

```
snapmirror delete -destination-path SVM:volume
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

- c. Dal cluster di origine, rilasciare la relazione SnapMirror senza eliminare le comuni copie Snapshot:

```
snapmirror release -relationship-info-only true -destination-path
```

*dest\_SVM:dest\_volume*

```
cluster1::>snapmirror release -relationship-info-only true  
-destination-path vs1_dr:vol1
```

- d. Dal cluster di destinazione, creare una relazione SnapMirror asincrona:

```
snapmirror create -source-path src_SVM:src_volume -destination-path  
dest_SVM:dest_volume -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path  
vs1_dr:vol1 -policy sync
```

- e. Risincronizzare la relazione sincrona di SnapMirror:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

## Convertire la modalità di una relazione sincrona SnapMirror

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror. È possibile convertire la modalità di una relazione sincrona SnapMirror da StrictSync a Sync o viceversa.

### A proposito di questa attività

Non è possibile modificare il criterio di una relazione sincrona di SnapMirror per convertirne la modalità.

### Fasi

1. Dal cluster di destinazione, interrompere la relazione sincrona di SnapMirror esistente:

```
snapmirror quiesce -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. Dal cluster di destinazione, eliminare la relazione sincrona SnapMirror esistente:

```
snapmirror delete -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. Dal cluster di origine, rilasciare la relazione SnapMirror senza eliminare le comuni copie Snapshot:

```
snapmirror release -relationship-info-only true -destination-path  
dest_SVM:dest_volume
```

```
cluster1::> snapmirror release -relationship-info-only true -destination  
-path vs1_dr:vol1
```

4. Dal cluster di destinazione, creare una relazione sincrona di SnapMirror specificando la modalità in cui si desidera convertire la relazione sincrona di SnapMirror:

```
snapmirror create -source-path vs1:vol1 -destination-path dest_SVM:dest_volume  
-policy Sync|StrictSync
```

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination-path  
vs1_dr:vol1 -policy Sync
```

5. Dal cluster di destinazione, risincronizzare la relazione SnapMirror:

```
snapmirror resync -destination-path dest_SVM:dest_volume
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

## Creazione ed eliminazione di volumi di test del failover SnapMirror

A partire da ONTAP 9.14.1, puoi utilizzare System Manager per creare un clone del volume per verificare il failover e il disaster recovery di SnapMirror, senza interrompere la relazione di SnapMirror attiva. Al termine del test, è possibile cancellare i dati associati ed eliminare il volume del test.

### Creazione di un volume di test del failover SnapMirror


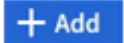
#### A proposito di questa attività

- È possibile eseguire test di failover su relazioni SnapMirror sincrone e asincrone.
- Viene creato un clone del volume per eseguire il test di disaster recovery.
- Il volume clone viene creato sulla stessa macchina virtuale di storage della destinazione SnapMirror.
- Puoi utilizzare relazioni di SnapMirror di FlexVol e FlexGroup.
- Se esiste già un clone di test per la relazione selezionata, non è possibile creare un altro clone per tale relazione.
- Le relazioni del vault di SnapLock non sono supportate.

#### Prima di iniziare

- Devi essere un amministratore del cluster.
- La licenza SnapMirror deve essere installata sul cluster di origine e destinazione.


#### Fasi

1. Nel cluster di destinazione, selezionare **protezione > Relazioni**.
2. Selezionare  Accanto all'origine della relazione e scegliere **Test failover**.
3. Nella finestra **Test failover**, selezionare **Test failover**.
4. Selezionare **Storage > Volumes** (archiviazione > volumi\*) e verificare che il volume di failover di prova sia elencato.
5. Selezionare **Storage > Share** (archiviazione > Condividi).
6. Fare clic su  E scegliere **Condividi**.
7. Nella finestra **Aggiungi condivisione**, digitare un nome per la condivisione nel campo **Nome condivisione**.
8. Nel campo **cartella**, selezionare **Sfoggia**, selezionare il volume del clone di test e **Salva**.
9. Nella parte inferiore della finestra **Aggiungi condivisione**, scegliere **Salva**.
10. Aprire la condivisione sul client e verificare che il volume di prova disponga di capacità di lettura e scrittura.

### Pulire i dati di failover ed eliminare il volume di test

Una volta completato il test di failover, è possibile cancellare tutti i dati associati al volume di test ed eliminarlo.

#### Fasi

1. Nel cluster di destinazione, selezionare **protezione > Relazioni**.
2. Selezionare  Accanto all'origine della relazione e scegliere **Clean Up Test failover**.
3. Nella finestra **Clean Up Test failover**, selezionare **Clean Up**.
4. Selezionare **archiviazione > volumi** e verificare che il volume di prova sia stato eliminato.

## Fornire i dati da un volume di destinazione DR SnapMirror

### Rendere il volume di destinazione scrivibile

È necessario rendere il volume di destinazione scrivibile prima di poter inviare i dati dal volume ai client. È possibile utilizzare `snapmirror quiesce` per arrestare i trasferimenti pianificati verso la destinazione, il `snapmirror abort` per interrompere i trasferimenti in corso e il `snapmirror break` per rendere la destinazione scrivibile.

#### A proposito di questa attività

È necessario eseguire questa attività dalla SVM di destinazione o dal cluster di destinazione.

#### Fasi

1. Interrompere i trasferimenti pianificati verso la destinazione:

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ...
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente vengono interrotti i trasferimenti pianificati tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst:> snapmirror quiesce -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

## 2. Interrompere i trasferimenti in corso verso la destinazione:

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ...
```

Per la sintassi completa dei comandi, vedere la pagina man.



Questo passaggio non è necessario per le relazioni sincroni di SnapMirror (supportate a partire da ONTAP 9.5).

Nell'esempio seguente vengono interrotti i trasferimenti in corso tra il volume di origine volA acceso svm1 e il volume di destinazione volA\_dst acceso svm\_backup:

```
cluster_dst:> snapmirror abort -source-path svm1:volA -destination-path  
svm_backup:volA_dst
```

## 3. Interrompere la relazione di disaster recovery di SnapMirror:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ...
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene spezzata la relazione tra il volume di origine volA acceso svm1 e il volume di destinazione volA\_dst acceso svm\_backup:

```
cluster_dst:> snapmirror break -source-path svm1:volA -destination-path  
svm_backup:volA_dst
```

### Altri modi per farlo in ONTAP

| Per eseguire queste attività con...                                           | Guarda questo contenuto...                                      |
|-------------------------------------------------------------------------------|-----------------------------------------------------------------|
| System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive) | <a href="#">"Fornire i dati da una destinazione SnapMirror"</a> |
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)      | <a href="#">"Panoramica sul disaster recovery dei volumi"</a>   |

### Configurare il volume di destinazione per l'accesso ai dati

Una volta reso scrivibile il volume di destinazione, è necessario configurare il volume per l'accesso ai dati. I client NAS, il sottosistema NVMe e gli host SAN possono accedere ai dati dal volume di destinazione fino alla riattivazione del volume di origine.

## Ambiente NAS:

1. Montare il volume NAS nello spazio dei nomi utilizzando lo stesso percorso di giunzione in cui è stato montato il volume di origine nella SVM di origine.
2. Applicare gli ACL appropriati alle condivisioni SMB del volume di destinazione.
3. Assegnare i criteri di esportazione NFS al volume di destinazione.
4. Applicare le regole di quota al volume di destinazione.
5. Reindirizzare i client al volume di destinazione.
6. Rimontare le condivisioni NFS e SMB sui client.

## Ambiente SAN:

1. Mappare le LUN nel volume al gruppo iniziatore appropriato.
2. Per iSCSI, creare sessioni iSCSI dagli iniziatori host SAN alle LIF SAN.
3. Sul client SAN, eseguire una nuova scansione dello storage per rilevare i LUN connessi.

Per informazioni sull'ambiente NVMe, vedere ["Amministrazione SAN"](#).

## Riattivare il volume di origine originale

È possibile ristabilire la relazione di protezione dei dati originale tra i volumi di origine e di destinazione quando non è più necessario fornire dati dalla destinazione.

### A proposito di questa attività

- La procedura riportata di seguito presuppone che la linea di base nel volume di origine originale sia intatta. Se la linea di base non è intatta, è necessario creare e inizializzare la relazione tra il volume da cui si stanno fornendo i dati e il volume di origine originale prima di eseguire la procedura.
- La preparazione in background e la fase di data warehousing di una relazione SnapMirror XDP possono richiedere molto tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.

### Fasi

1. Invertire la relazione di protezione dei dati originale:

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine. Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta. Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

Nell'esempio seguente viene invertita la relazione tra il volume di origine originale, `volA` acceso `svm1` e il volume da cui vengono forniti i dati, `volA_dst` acceso `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

2. Quando si è pronti a ristabilire l'accesso ai dati all'origine originale, interrompere l'accesso al volume di destinazione originale. Un modo per farlo è arrestare la SVM di destinazione originale:

```
vserver stop -vserver SVM
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di destinazione originale o dal cluster di destinazione originale. Questo comando interrompe l'accesso dell'utente all'intera SVM di destinazione originale. È possibile interrompere l'accesso al volume di destinazione originale utilizzando altri metodi.

Nell'esempio seguente viene interrotta la SVM di destinazione originale:

```
cluster_dst::> vserver stop svm_backup
```

3. Aggiornare la relazione inversa:

```
snapmirror update -source-path SVM:volume -destination-path SVM:volume
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine.

Nell'esempio riportato di seguito viene aggiornata la relazione tra il volume da cui si stanno fornendo i dati, `volA_dst acceso svm_backup` e il volume di origine originale, ``volA acceso svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

4. Dalla SVM di origine originale o dal cluster di origine originale, interrompere i trasferimenti pianificati per la relazione invertita:

```
snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine.

Nell'esempio seguente vengono interrotti i trasferimenti pianificati tra il volume di destinazione originale, `volA_dst acceso svm_backup` e il volume di origine originale, ``volA acceso svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

5. Quando l'aggiornamento finale è completo e la relazione indica "Quiesced" per lo stato della relazione, eseguire il seguente comando dalla SVM di origine o dal cluster di origine originale per interrompere la relazione invertita:

```
snapmirror break -source-path SVM:volume -destination-path SVM:volume
```

Per la sintassi completa dei comandi, vedere la pagina man.



Eseguire questo comando dalla SVM di origine o dal cluster di origine.

L'esempio seguente interrompe la relazione tra il volume di destinazione originale, `volA_dst` acceso `svm_backup` e il volume di origine originale, `volA` acceso `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

6. Dalla SVM di origine originale o dal cluster di origine originale, eliminare la relazione di protezione dei dati invertita:

```
snapmirror delete -source-path SVM:volume -destination-path SVM:volume
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine.

Nell'esempio seguente viene eliminata la relazione inversa tra il volume di origine originale, `volA` acceso `svm1` e il volume da cui vengono forniti i dati, `volA_dst` acceso `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

7. Rilasciare la relazione invertita dalla SVM di destinazione originale o dal cluster di destinazione originale.

```
snapmirror release -source-path SVM:volume -destination-path SVM:volume
```



È necessario eseguire questo comando dalla SVM di destinazione originale o dal cluster di destinazione originale.

Nell'esempio seguente viene rilasciata la relazione inversa tra il volume di destinazione originale, `volA_dst` acceso `svm_backup` e il volume di origine originale, `volA` acceso `svm1`:



```
cluster_dst:> snapmirror release -source-path svm_backup:volA_dst  
-destination-path svm1:volA
```

8. Ristabilire la relazione di protezione dei dati originale dalla destinazione originale:

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene ristabilita la relazione tra il volume di origine originale, volA acceso svm1 e il volume di destinazione originale, volA\_dst acceso svm\_backup:

```
cluster_dst:> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

9. Se necessario, avviare la SVM di destinazione originale:

```
vserver start -vserver SVM
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene avviata la SVM di destinazione originale:

```
cluster_dst:> vserver start svm_backup
```

### Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

## Ripristinare i file da un volume di destinazione SnapMirror

### Ripristinare un singolo file, LUN o spazio dei nomi NVMe da una destinazione SnapMirror

È possibile ripristinare un singolo file, LUN, un set di file o LUN da una copia Snapshot o uno spazio dei nomi NVMe da un volume di destinazione SnapMirror. A partire da ONTAP 9.7, è anche possibile ripristinare gli spazi dei nomi NVMe da una destinazione sincrona SnapMirror. È possibile ripristinare i file nel volume di origine originale o in un volume diverso.

### Di cosa hai bisogno

Per ripristinare un file o un LUN da una destinazione sincrona SnapMirror (supportata a partire da ONTAP 9.5), è necessario prima eliminare e rilasciare la relazione.

### A proposito di questa attività

Il volume su cui si ripristinano file o LUN (il volume di destinazione) deve essere un volume di lettura/scrittura:

- SnapMirror esegue un *ripristino incrementale* se i volumi di origine e di destinazione dispongono di una copia Snapshot comune (come in genere avviene quando si esegue il ripristino nel volume di origine originale).
- In caso contrario, SnapMirror esegue un *ripristino baseline*, in cui la copia Snapshot specificata e tutti i blocchi di dati a cui fa riferimento vengono trasferiti al volume di destinazione.

## Fasi

1. Elencare le copie Snapshot nel volume di destinazione:

```
volume snapshot show -vserver SVM -volume volume
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio riportato di seguito vengono illustrate le copie Snapshot di vserversB:secondary1 destinazione:

```
cluster_dst::> volume snapshot show -vserver vserversB -volume secondary1
```

| Vserver   | Volume     | Snapshot               | State | Size  | Total% |
|-----------|------------|------------------------|-------|-------|--------|
| Used%     | -----      | -----                  | ----- | ----- | -----  |
| -----     | -----      | -----                  | ----- | ----- | -----  |
| vserversB | secondary1 | hourly.2013-01-25_0005 | valid | 224KB | 0%     |
| 0%        |            | daily.2013-01-25_0010  | valid | 92KB  | 0%     |
| 0%        |            | hourly.2013-01-25_0105 | valid | 228KB | 0%     |
| 0%        |            | hourly.2013-01-25_0205 | valid | 236KB | 0%     |
| 0%        |            | hourly.2013-01-25_0305 | valid | 244KB | 0%     |
| 0%        |            | hourly.2013-01-25_0405 | valid | 244KB | 0%     |
| 0%        |            | hourly.2013-01-25_0505 | valid | 244KB | 0%     |

7 entries were displayed.

2. Ripristinare un singolo file o LUN o un set di file o LUN da una copia Snapshot in un volume di destinazione SnapMirror:

```
snapmirror restore -source-path SVM:volume|cluster://SVM/volume, ...
-destination-path SVM:volume|cluster://SVM/volume, ... -source-snapshot snapshot
-file-list source_file_path,@destination_file_path
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Il seguente comando ripristina i file `file1` e `file2` Dalla copia Snapshot `daily.2013-01-25_0010` nel volume di destinazione originale `secondary1`, nella stessa posizione nel file system attivo del volume di origine originale `primary1`:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Il seguente comando ripristina i file `file1` e `file2` Dalla copia Snapshot `daily.2013-01-25_0010` nel volume di destinazione originale `secondary1`, in una posizione diversa nel file system attivo del volume di origine originale `primary1`.

Il percorso del file di destinazione inizia con il simbolo `@` seguito dal percorso del file dalla directory principale del volume di origine originale. In questo esempio, `file1` viene ripristinato a `/dir1/file1.new` e il `file2` viene ripristinato a `/dir2.new/file2` acceso `primary1`:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Il seguente comando ripristina i file `file1` e `file3` Dalla copia Snapshot `daily.2013-01-25_0010` nel volume di destinazione originale `secondary1`, in posizioni diverse nel file system attivo del volume di origine originale `primary1` e ripristina `file2` da `snap1` nella stessa posizione nel file system attivo di `primary1`.

In questo esempio, il file `file1` viene ripristinato a `/dir1/file1.new` e `file3` viene ripristinato a `/dir3.new/file3`:

```
cluster_dst:> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3
```

```
[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

## Ripristinare il contenuto di un volume da una destinazione SnapMirror

È possibile ripristinare il contenuto di un intero volume da una copia Snapshot in un volume di destinazione SnapMirror. È possibile ripristinare il contenuto del volume nel volume di origine originale o in un volume diverso.

### A proposito di questa attività

Il volume di destinazione per l'operazione di ripristino deve essere uno dei seguenti:

- Un volume di lettura/scrittura, nel qual caso SnapMirror esegue un *ripristino incrementale*, a condizione che i volumi di origine e di destinazione dispongano di una copia Snapshot comune (come accade generalmente quando si esegue il ripristino nel volume di origine originale).



Il comando non riesce se non esiste una copia Snapshot comune. Non è possibile ripristinare il contenuto di un volume su un volume vuoto in lettura/scrittura.

- Un volume di protezione dei dati vuoto, nel qual caso SnapMirror esegue un *ripristino baseline*, in cui la copia Snapshot specificata e tutti i blocchi di dati a cui fa riferimento vengono trasferiti al volume di origine.

Il ripristino del contenuto di un volume è un'operazione che comporta interruzioni. Il traffico SMB non deve essere in esecuzione sul volume primario SnapVault quando è in esecuzione un'operazione di ripristino.

Se la compressione del volume di destinazione per l'operazione di ripristino è attivata e la compressione del volume di origine non è attivata, disattivare la compressione sul volume di destinazione. Al termine dell'operazione di ripristino, è necessario riattivare la compressione.

Tutte le regole di quota definite per il volume di destinazione vengono disattivate prima di eseguire il ripristino. È possibile utilizzare `volume quota modify` comando per riattivare le regole di quota al termine dell'operazione di ripristino.

### Fasi

1. Elencare le copie Snapshot nel volume di destinazione:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio riportato di seguito vengono illustrate le copie Snapshot di `vserverB:secondary1` destinazione:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1
```

| Vserver<br>Used% | Volume     | Snapshot               | State | Size  | Total% |
|------------------|------------|------------------------|-------|-------|--------|
| -----<br>-----   | -----      | -----                  | ----- | ----- | -----  |
| vserverB<br>0%   | secondary1 | hourly.2013-01-25_0005 | valid | 224KB | 0%     |
| 0%               |            | daily.2013-01-25_0010  | valid | 92KB  | 0%     |
| 0%               |            | hourly.2013-01-25_0105 | valid | 228KB | 0%     |
| 0%               |            | hourly.2013-01-25_0205 | valid | 236KB | 0%     |
| 0%               |            | hourly.2013-01-25_0305 | valid | 244KB | 0%     |
| 0%               |            | hourly.2013-01-25_0405 | valid | 244KB | 0%     |
| 0%               |            | hourly.2013-01-25_0505 | valid | 244KB | 0%     |

7 entries were displayed.

## 2. Ripristinare il contenuto di un volume da una copia Snapshot in un volume di destinazione SnapMirror:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot  
<snapshot>
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di origine originale o dal cluster di origine.

Il seguente comando ripristina il contenuto del volume di origine originale primary1 Dalla copia Snapshot daily.2013-01-25\_0010 nel volume di destinazione originale secondary1:

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1  
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-  
25_0010
```

Warning: All data newer than Snapshot copy daily.2013-01-25\_0010 on  
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source  
vserverB:secondary1 for the snapshot daily.2013-01-25\_0010.

3. Rimontare il volume ripristinato e riavviare tutte le applicazioni che utilizzano il volume.

#### Altri modi per farlo in ONTAP

| Per eseguire queste attività con...                                           | Guarda questo contenuto...                                                |
|-------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| System Manager riprogettato (disponibile con ONTAP 9.7 e versioni successive) | <a href="#">"Ripristinare un volume da una copia Snapshot precedente"</a> |
| System Manager Classic (disponibile con ONTAP 9.7 e versioni precedenti)      | <a href="#">"Panoramica del ripristino del volume con SnapVault"</a>      |

## Aggiornare manualmente una relazione di replica

Potrebbe essere necessario aggiornare manualmente una relazione di replica se un aggiornamento non riesce a causa dello spostamento del volume di origine.

#### A proposito di questa attività

SnapMirror interrompe i trasferimenti da un volume di origine spostato fino a quando non si aggiorna manualmente la relazione di replica.

A partire da ONTAP 9.5, sono supportate le relazioni sincroni di SnapMirror. Sebbene i volumi di origine e di destinazione siano sempre sincronizzati in queste relazioni, la vista dal cluster secondario viene sincronizzata con il principale solo su base oraria. Se si desidera visualizzare i dati point-in-time nella destinazione, eseguire un aggiornamento manuale eseguendo il `snapmirror update` comando.

#### Fase

1. Aggiornare manualmente una relazione di replica:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ...
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

Nell'esempio seguente viene aggiornata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_src:> snapmirror update -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

## Risincronizzare una relazione di replica

È necessario risincronizzare una relazione di replica dopo che si rende scrivibile un volume di destinazione, dopo che un aggiornamento non riesce perché non esiste una copia Snapshot comune sui volumi di origine e di destinazione o se si desidera modificare il criterio di replica per la relazione.

### A proposito di questa attività

- Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.
- La risincronizzazione dei volumi che fanno parte di una configurazione fan-out o a cascata può richiedere più tempo. Non è raro che la relazione di SnapMirror riporti lo stato di "preparazione" per un periodo di tempo prolungato.

### Fase

1. Risincronizzare i volumi di origine e di destinazione:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ... -type DP|XDP -policy policy
```

Per la sintassi completa dei comandi, vedere la pagina `man`.



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst:> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

## Eliminare una relazione di replica di un volume

È possibile utilizzare `snapmirror delete` e `snapmirror release` comandi per eliminare una relazione di replica di un volume. È quindi possibile eliminare manualmente i volumi di destinazione non necessari.

### A proposito di questa attività

Il `snapmirror release` comando elimina tutte le copie Snapshot create da SnapMirror dall'origine. È

possibile utilizzare `-relationship-info-only` Opzione per conservare le copie Snapshot.

## Fasi

1. Interrompere la relazione di replica:

```
snapmirror quiesce -destination-path SVM:volume|cluster://SVM/volume
```

```
cluster_dst:> snapmirror quiesce -destination-path svm_backup:volA_dst
```

2. (Facoltativo) interrompere la relazione di replica se si desidera che il volume di destinazione sia un volume di lettura/scrittura. È possibile saltare questo passaggio se si intende eliminare il volume di destinazione o se non è necessario che il volume sia in lettura/scrittura:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ...
```

```
cluster_dst:> snapmirror break -source-path svm1:volA -destination-path  
svm_backup:volA_dst
```

3. Eliminare la relazione di replica:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ...
```

Per la sintassi completa dei comandi, vedere la pagina man.



Eseguire questo comando dal cluster di destinazione o dalla SVM di destinazione.

Nell'esempio riportato di seguito viene eliminata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup`:

```
cluster_dst:> snapmirror delete -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

4. Rilasciare le informazioni sulle relazioni di replica dalla SVM di origine:

```
snapmirror release -source-path SVM:volume|cluster://SVM/volume, ...  
-destination-path SVM:volume|cluster://SVM/volume, ...
```

Per la sintassi completa dei comandi, vedere la pagina man.



Eseguire questo comando dal cluster di origine o dalla SVM di origine.

Nell'esempio riportato di seguito vengono rilasciate informazioni per la relazione di replica specificata dalla SVM di origine `svm1`:



```
cluster_src::> snapmirror release -source-path svm1:volA -destination  
-path svm_backup:volA_dst
```

## Gestire l'efficienza dello storage

SnapMirror preserva l'efficienza dello storage sui volumi di origine e di destinazione, con un'eccezione, quando la compressione dei dati post-elaborazione è attivata sulla destinazione. In tal caso, tutta l'efficienza dello storage viene persa sulla destinazione. Per risolvere questo problema, è necessario disattivare la compressione post-elaborazione sulla destinazione, aggiornare manualmente la relazione e riattivare l'efficienza dello storage.

### Di cosa hai bisogno

- I cluster di origine e di destinazione e le SVM devono essere peering.

#### "Peering di cluster e SVM"

- È necessario disattivare la compressione post-elaborazione sulla destinazione.

### A proposito di questa attività

È possibile utilizzare `volume efficiency show` comando per determinare se l'efficienza è attivata su un volume. Per ulteriori informazioni, consulta le pagine man.

È possibile verificare se SnapMirror mantiene l'efficienza dello storage visualizzando i registri di controllo di SnapMirror e individuando la descrizione del trasferimento. Se viene visualizzata la descrizione del trasferimento `transfer_desc=Logical Transfer`, SnapMirror non mantiene l'efficienza dello storage. Se viene visualizzata la descrizione del trasferimento `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror sta mantenendo l'efficienza dello storage. Ad esempio:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-  
b665-11e5-a626-00a09860c273 Operation-Uid=39fbcf48-550a-4282-a906-  
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>  
destination=<destpath> status=Success bytes_transferred=117080571  
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized  
Directory Mode
```

### Trasferimento logico con storage

A partire da ONTAP 9.3, l'aggiornamento manuale non è più necessario per riattivare l'efficienza dello storage. Se SnapMirror rileva che la compressione post-processo è stata disattivata, riattiva automaticamente l'efficienza dello storage al successivo aggiornamento pianificato. Sia l'origine che la destinazione devono eseguire ONTAP 9.3.

A partire da ONTAP 9.3, i sistemi AFF gestiscono le impostazioni di efficienza dello storage in modo diverso dai sistemi FAS dopo che un volume di destinazione è reso scrivibile:

- Dopo aver impostato un volume di destinazione scrivibile utilizzando `snapmirror break` il criterio di

caching sul volume viene automaticamente impostato su “auto” (impostazione predefinita).



Questo comportamento è applicabile solo ai volumi FlexVol e non ai volumi FlexGroup.

- Alla risincronizzazione, il criterio di caching viene automaticamente impostato su “none” e deduplica e compressione inline vengono automaticamente disabilitate, indipendentemente dalle impostazioni originali. È necessario modificare le impostazioni manualmente in base alle necessità.



Gli aggiornamenti manuali con l'efficienza dello storage abilitata possono richiedere molto tempo. Potrebbe essere necessario eseguire l'operazione in ore non di punta.

## Fase

1. Aggiornare una relazione di replica e riattivare l'efficienza dello storage:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ... -enable-storage-efficiency true
```

Per la sintassi completa dei comandi, vedere la pagina man.



È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione. Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

Nell'esempio seguente viene aggiornata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA_dst` acceso `svm_backup` e riattiva l'efficienza dello storage:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination  
-path svm_backup:volA_dst -enable-storage-efficiency true
```

## Utilizzare la funzione di limitazione globale di SnapMirror

La funzione di limitazione globale della rete è disponibile per tutti i trasferimenti SnapMirror e SnapVault a livello di nodo.

### A proposito di questa attività

La limitazione globale di SnapMirror limita la larghezza di banda utilizzata dai trasferimenti SnapMirror e SnapVault in entrata e/o in uscita. La restrizione viene applicata a livello di cluster su tutti i nodi del cluster.

Ad esempio, se l'acceleratore in uscita è impostato su 100 Mbps, per ogni nodo del cluster la larghezza di banda in uscita sarà impostata su 100 Mbps. Se la funzione di limitazione globale è disattivata, viene disattivata su tutti i nodi.

Sebbene le velocità di trasferimento dei dati siano spesso espresse in bit per secondo (bps), i valori di accelerazione devono essere immessi in kilobyte per secondo (kbps).



In ONTAP 9.9.1 e versioni precedenti, l'acceleratore non ha alcun effetto su `volume move` trasferimenti o trasferimenti mirror di condivisione del carico. A partire da ONTAP 9.10.0, è possibile specificare un'opzione per limitare le operazioni di spostamento di un volume. Per ulteriori informazioni, vedere ["Come ridurre lo spostamento del volume in ONTAP 9.10 e versioni successive."](#)

La funzione Global Throttling funziona con la funzione di accelerazione per relazione per i trasferimenti SnapMirror e SnapVault. La regolazione per relazione viene applicata fino a quando la larghezza di banda combinata dei trasferimenti per relazione non supera il valore della valvola a farfalla globale, dopodiché viene applicata la valvola a farfalla globale. Un valore di accelerazione 0 implica che la limitazione globale è disattivata.



La limitazione globale di SnapMirror non ha alcun effetto sulle relazioni sincrone di SnapMirror quando sono in-Sync. Tuttavia, l'accelerazione influisce sulle relazioni sincrone di SnapMirror quando eseguono una fase di trasferimento asincrona, ad esempio un'operazione di inizializzazione o dopo un evento out of Sync. Per questo motivo, si sconsiglia di attivare la limitazione globale con le relazioni sincroni di SnapMirror.

## Fasi

1. Attivare la limitazione globale:

```
options -option-name replication.throttle.enable on|off
```

Nell'esempio seguente viene illustrato come attivare la funzione di limitazione globale di SnapMirror  
`cluster_dst:`

```
cluster_dst::> options -option-name replication.throttle.enable on
```

2. Specificare la larghezza di banda totale massima utilizzata dai trasferimenti in entrata sul cluster di destinazione:

```
options -option-name replication.throttle.incoming.max_kbs KBps
```

La larghezza di banda dell'acceleratore minima consigliata è di 4 kbps e la massima è di 2 Tbps. Il valore predefinito per questa opzione è `unlimited`, il che significa che non esiste alcun limite alla larghezza di banda totale utilizzata.

L'esempio seguente mostra come impostare la larghezza di banda massima totale utilizzata dai trasferimenti in entrata su 100 Mbps:

```
cluster_dst::> options -option-name  
replication.throttle.incoming.max_kbs 12500
```



100 Mbps = 12500 kbps

3. Specificare la larghezza di banda totale massima utilizzata dai trasferimenti in uscita sul cluster di origine:

```
options -option-name replication.throttle.outgoing.max_kbs KBps
```

La larghezza di banda dell'acceleratore minima consigliata è di 4 kbps e la massima è di 2 Tbps. Il valore predefinito per questa opzione è `unlimited`, il che significa che non esiste alcun limite alla larghezza di banda totale utilizzata. I valori dei parametri sono espressi in kbps.

L'esempio seguente mostra come impostare la larghezza di banda massima totale utilizzata dai trasferimenti in uscita su 100 Mbps:

```
cluster_src::> options -option-name  
replication.throttle.outgoing.max_kbs 12500
```

## Gestire la replica di SnapMirror SVM

### Informazioni sulla replica di SnapMirror SVM

È possibile utilizzare SnapMirror per creare una relazione di protezione dei dati tra le SVM. In questo tipo di relazione di protezione dei dati, viene replicata tutta o parte della configurazione di SVM, dalle esportazioni NFS e dalle condivisioni SMB a RBAC, nonché i dati nei volumi di proprietà di SVM.

#### Tipi di relazione supportati

È possibile replicare solo le SVM che servono i dati. Sono supportati i seguenti tipi di relazione per la protezione dei dati:

- *SnapMirror DR*, in cui la destinazione contiene in genere solo le copie Snapshot attualmente presenti nell'origine.

A partire da ONTAP 9.9.1, questo comportamento cambia quando si utilizza il criterio del vault mirror. A partire da ONTAP 9.9.1, è possibile creare diverse policy Snapshot sull'origine e sulla destinazione e le copie Snapshot sulla destinazione non vengono sovrascritte dalle copie Snapshot sull'origine:

- Non vengono sovrascritti dall'origine alla destinazione durante le normali operazioni pianificate, gli aggiornamenti e la risincronizzazione
- Non vengono cancellati durante le operazioni di interruzione.
- Non vengono cancellati durante le operazioni flip-resync.  
Quando si configura una relazione di emergenza SVM utilizzando il criterio mirror-vault utilizzando ONTAP 9.9.1 e versioni successive, il criterio si comporta come segue:
  - I criteri di copia Snapshot definiti dall'utente all'origine non vengono copiati nella destinazione.
  - I criteri di copia Snapshot definiti dal sistema non vengono copiati nella destinazione.
  - L'associazione dei volumi con le policy Snapshot definite dall'utente e dal sistema non viene copiata nella destinazione. + SVM.
- A partire da ONTAP 9.2, *SnapMirror Unified Replication*, in cui la destinazione è configurata sia per il DR che per la conservazione a lungo termine.

I dettagli su questi tipi di relazione sono disponibili qui: ["Informazioni sulla replica dei volumi SnapMirror"](#).

Il *tipo di policy* del criterio di replica determina il tipo di relazione che supporta. La tabella seguente mostra i tipi di policy disponibili.

|                  |                   |
|------------------|-------------------|
| Tipo di policy   | Tipo di relazione |
| mirror asincrono | Dr. SnapMirror    |
| vault mirror     | Replica unificata |

## XDP sostituisce DP come replica SVM predefinita in ONTAP 9.4

A partire da ONTAP 9.4, le relazioni di protezione dei dati SVM passano per impostazione predefinita alla modalità XDP. Le relazioni di protezione dei dati SVM continuano a essere impostate per impostazione predefinita sulla modalità DP in ONTAP 9.3 e versioni precedenti.

Le relazioni esistenti non vengono influenzate dal nuovo valore predefinito. Se una relazione è già di tipo DP, continuerà ad essere di tipo DP. La tabella seguente mostra il comportamento che ci si può aspettare.

| Se si specifica... | Il tipo è... | Il criterio predefinito (se non si specifica un criterio) è... |
|--------------------|--------------|----------------------------------------------------------------|
| DP                 | XDP          | MirrorAllSnapshot (DR SnapMirror)                              |
| Niente             | XDP          | MirrorAllSnapshot (DR SnapMirror)                              |
| XDP                | XDP          | MirrorAndVault (replica unificata)                             |

I dettagli sulle modifiche di default sono disponibili qui: ["XDP sostituisce DP come impostazione predefinita di SnapMirror"](#).



L'indipendenza dalla versione non è supportata per la replica SVM. In una configurazione di disaster recovery delle SVM, la SVM di destinazione deve trovarsi su un cluster dotato della stessa versione di ONTAP del cluster SVM di origine per supportare le operazioni di failover e failback.

## "Versioni ONTAP compatibili per le relazioni SnapMirror"

### Come vengono replicate le configurazioni SVM

Il contenuto di una relazione di replica SVM è determinato dall'interazione dei seguenti campi:

- Il `-identity-preserve true` opzione di `snapmirror create` Il comando replica l'intera configurazione SVM.  
  
Il `-identity-preserve false` L'opzione replica solo i volumi e le configurazioni di autenticazione e autorizzazione della SVM, nonché le impostazioni del protocollo e del servizio nomi elencate nella ["Configurazioni replicate nelle relazioni di disaster recovery delle SVM"](#).
- Il `-discard-configs network` opzione di `snapmirror policy create` Il comando esclude le LIF e le relative impostazioni di rete dalla replica SVM, da utilizzare nei casi in cui le SVM di origine e di destinazione si trovano in sottoreti diverse.
- Il `-vserver-dr-protection unprotected` opzione di `volume modify` Il comando esclude il volume specificato dalla replica SVM.

In caso contrario, la replica SVM è quasi identica alla replica del volume. È possibile utilizzare virtualmente lo stesso flusso di lavoro per la replica SVM utilizzato per la replica dei volumi.

## Dettagli del supporto

La seguente tabella mostra i dettagli del supporto per la replica SVM di SnapMirror.

| Risorsa o funzione                    | Dettagli del supporto                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tipi di implementazione               | <ul style="list-style-type: none"><li>• Da origine singola a destinazione singola</li><li>• A partire da ONTAP 9.4, fan-out. È possibile eseguire la fan-out solo su due destinazioni.</li></ul> <p>Per impostazione predefinita, è consentita una sola relazione effettiva -Identity-Preserve per SVM di origine.</p> |
| Tipi di relazione                     | <ul style="list-style-type: none"><li>• Disaster recovery SnapMirror</li><li>• A partire da ONTAP 9.2, la replica unificata di SnapMirror</li></ul>                                                                                                                                                                    |
| Ambito della replica                  | Solo intercluster. Non è possibile replicare le SVM nello stesso cluster.                                                                                                                                                                                                                                              |
| Protezione ransomware autonoma        | <ul style="list-style-type: none"><li>• Supportato a partire da ONTAP 9.12.1. Per ulteriori informazioni, vedere "<a href="#">Protezione ransomware autonoma</a>"</li></ul>                                                                                                                                            |
| Supporto asincrono gruppi di coerenza | A partire da ONTAP 9.14.1, sono supportate massimo 32 relazioni di disaster recovery SVM in presenza di gruppi di coerenza. Vedere " <a href="#">Proteggere un gruppo di coerenza</a> " e " <a href="#">Limiti del gruppo di coerenza</a> " per ulteriori informazioni.                                                |
| FabricPool                            | A partire da ONTAP 9.6, la replica SVM di SnapMirror è supportata con FabricPools.                                                                                                                                                                                                                                     |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MetroCluster       | <p>A partire da ONTAP 9.11.1, entrambi i lati di una relazione di disaster recovery SVM all'interno di una configurazione MetroCluster possono fungere da origine per ulteriori configurazioni di disaster recovery SVM.</p> <p>A partire da ONTAP 9.5, la replica SVM di SnapMirror è supportata nelle configurazioni MetroCluster.</p> <ul style="list-style-type: none"> <li>• Nelle release precedenti a ONTAP 9,10.X, una configurazione MetroCluster non può essere la destinazione di una relazione di disaster recovery della SVM.</li> <li>• In ONTAP 9.10.1 e versioni successive, una configurazione MetroCluster può essere la destinazione di una relazione di disaster recovery della SVM solo ai fini della migrazione e deve soddisfare tutti i requisiti necessari descritti in <a href="#">"TR-4966: Migrazione di una SVM in una soluzione MetroCluster"</a>.</li> <li>• Solo una SVM attiva all'interno di una configurazione MetroCluster può essere l'origine di una relazione di disaster recovery SVM.</li> </ul> <p>Un'origine può essere una SVM di origine della sincronizzazione prima dello switchover o una SVM di destinazione della sincronizzazione dopo lo switchover.</p> <ul style="list-style-type: none"> <li>• Quando una configurazione MetroCluster si trova in uno stato stabile, la SVM di destinazione della sincronizzazione MetroCluster non può essere l'origine di una relazione di disaster recovery SVM, poiché i volumi non sono online.</li> <li>• Quando la SVM sync-source è l'origine di una relazione di disaster recovery della SVM, le informazioni della relazione di disaster recovery della SVM di origine vengono replicate al partner MetroCluster.</li> <li>• Durante i processi di switchover e switchback, è possibile che si verifichi un errore nella replica alla destinazione di disaster recovery della SVM.</li> </ul> <p>Tuttavia, al termine del processo di switchover o switchback, gli aggiornamenti pianificati del disaster recovery della SVM successivo avranno esito positivo.</p> |
| Gruppo di coerenza | <p>Supportato a partire da ONTAP 9.14.1. Per ulteriori informazioni, vedere <a href="#">Proteggere un gruppo di coerenza</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP S3                    | Non supportato con disaster recovery SVM.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| SnapMirror sincrono         | Non supportato con disaster recovery SVM.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Indipendenza dalla versione | Non supportato.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Crittografia dei volumi     | <ul style="list-style-type: none"> <li>• I volumi crittografati sull'origine vengono crittografati sulla destinazione.</li> <li>• I server Onboard Key Manager o KMIP devono essere configurati sulla destinazione.</li> <li>• Le nuove chiavi di crittografia vengono generate alla destinazione.</li> <li>• Se la destinazione non contiene un nodo che supporta la crittografia .volume, la replica ha esito positivo, ma i volumi di destinazione non vengono crittografati.</li> </ul> |

### Configurazioni replicate nelle relazioni di disaster recovery delle SVM

La seguente tabella mostra l'interazione di `snapmirror create -identity-preserve` e il `snapmirror policy create -discard-configs network` opzione:

| Configurazione replicata    |          | <b>-identity-preserve true</b>                                      |                                                                   | <b>-identity-preserve false</b> |
|-----------------------------|----------|---------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------|
|                             |          | <b>Policy senza<br/>-discard<br/>-configs<br/>network impostato</b> | <b>Policy con<br/>-discard<br/>-configs<br/>network impostato</b> |                                 |
| Rete                        | LIF NAS  | Sì                                                                  | No                                                                | No                              |
| Configurazione Kerberos LIF | Sì       | No                                                                  | No                                                                | LIF SAN                         |
| No                          | No       | No                                                                  | Policy firewall                                                   | Sì                              |
| Sì                          | No       | Politiche di servizio                                               | Sì                                                                | Sì                              |
| No                          | Percorsi | Sì                                                                  | No                                                                | No                              |
| Dominio di broadcast        | No       | No                                                                  | No                                                                | Subnet                          |
| No                          | No       | No                                                                  | IPSpace                                                           | No                              |
| No                          | No       | PMI                                                                 | Server SMB                                                        | Sì                              |



|                          |                                    |                               |                                           |                                                                          |
|--------------------------|------------------------------------|-------------------------------|-------------------------------------------|--------------------------------------------------------------------------|
| Sì                       | No                                 | Gruppi locali e utenti locali | Sì                                        | Sì                                                                       |
| Sì                       | Privilegio                         | Sì                            | Sì                                        | Sì                                                                       |
| Copia shadow             | Sì                                 | Sì                            | Sì                                        | BranchCache                                                              |
| Sì                       | Sì                                 | Sì                            | Opzioni del server                        | Sì                                                                       |
| Sì                       | Sì                                 | Sicurezza del server          | Sì                                        | Sì                                                                       |
| No                       | Home directory, condividere        | Sì                            | Sì                                        | Sì                                                                       |
| Link simbolico           | Sì                                 | Sì                            | Sì                                        | Policy Fpolicy, policy FSecurity e FSecurity NTFS                        |
| Sì                       | Sì                                 | Sì                            | Mappatura dei nomi e mappatura dei gruppi | Sì                                                                       |
| Sì                       | Sì                                 | Informazioni di audit         | Sì                                        | Sì                                                                       |
| Sì                       | NFS                                | Policy di esportazione        | Sì                                        | Sì                                                                       |
| No                       | Regole dei criteri di esportazione | Sì                            | Sì                                        | No                                                                       |
| Server NFS               | Sì                                 | Sì                            | No                                        | RBAC                                                                     |
| Certificati di sicurezza | Sì                                 | Sì                            | No                                        | Configurazione dell'utente, della chiave pubblica, del ruolo e del ruolo |
| Sì                       | Sì                                 | Sì                            | SSL                                       | Sì                                                                       |
| Sì                       | No                                 | Servizi di nome               | Host DNS e DNS                            | Sì                                                                       |
| Sì                       | No                                 | Utente UNIX e gruppo UNIX     | Sì                                        | Sì                                                                       |

|                      |                                                                     |                    |                                                                                                                      |                                               |
|----------------------|---------------------------------------------------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Sì                   | Aree di autenticazione Kerberos e blocchi di chiavi Kerberos        | Sì                 | Sì                                                                                                                   | No                                            |
| Client LDAP e LDAP   | Sì                                                                  | Sì                 | No                                                                                                                   | Netgroup                                      |
| Sì                   | Sì                                                                  | No                 | NIS                                                                                                                  | Sì                                            |
| Sì                   | No                                                                  | Accesso web e web  | Sì                                                                                                                   | Sì                                            |
| No                   | Volume                                                              | Oggetto            | Sì                                                                                                                   | Sì                                            |
| Sì                   | Copie Snapshot, policy Snapshot e policy di eliminazione automatica | Sì                 | Sì                                                                                                                   | Sì                                            |
| Policy di efficienza | Sì                                                                  | Sì                 | Sì                                                                                                                   | Policy di quota e regola dei criteri di quota |
| Sì                   | Sì                                                                  | Sì                 | Coda di recovery                                                                                                     | Sì                                            |
| Sì                   | Sì                                                                  | Volume root        | Namespace                                                                                                            | Sì                                            |
| Sì                   | Sì                                                                  | Dati dell'utente   | No                                                                                                                   | No                                            |
| No                   | Qtree                                                               | No                 | No                                                                                                                   | No                                            |
| Quote                | No                                                                  | No                 | No                                                                                                                   | QoS a livello di file                         |
| No                   | No                                                                  | No                 | Attributi: stato del volume root, garanzia di spazio, dimensione, dimensionamento automatico e numero totale di file | No                                            |
| No                   | No                                                                  | QoS dello storage  | Gruppo di criteri QoS                                                                                                | Sì                                            |
| Sì                   | Sì                                                                  | Fibre Channel (FC) | No                                                                                                                   | No                                            |
| No                   | ISCSI                                                               | No                 | No                                                                                                                   | No                                            |

|         |         |      |                 |         |
|---------|---------|------|-----------------|---------|
| LUN     | Oggetto | Sì   | Sì              | Sì      |
| igroups | No      | No   | No              | portset |
| No      | No      | No   | Numeri di serie | No      |
| No      | No      | SNMP | utenti v3       | Sì      |

### Limiti storage per il disaster recovery delle SVM

Nella tabella seguente viene indicato il numero massimo consigliato di volumi e relazioni di disaster recovery delle SVM supportate per ogni oggetto storage. Devi essere consapevole che i limiti sono spesso dipendenti dalla piattaforma. Fare riferimento a. ["Hardware Universe"](#) per conoscere i limiti della configurazione specifica.

| Oggetto di storage | Limite                              |
|--------------------|-------------------------------------|
| SVM                | 300 volumi flessibili               |
| Coppia HA          | 1,000 volumi flessibili             |
| Cluster            | 128 relazioni di disastro delle SVM |

## Replicare le configurazioni SVM

### Workflow di replica di SnapMirror SVM

La replica di SnapMirror SVM implica la creazione della SVM di destinazione, la creazione di una pianificazione dei processi di replica e la creazione e l'inizializzazione di una relazione SnapMirror.

È necessario determinare il flusso di lavoro di replica più adatto alle proprie esigenze:

- ["Replica di un'intera configurazione SVM"](#)
- ["Escludere le LIF e le relative impostazioni di rete dalla replica SVM"](#)
- ["Escludi rete, name service e altre impostazioni dalla configurazione della SVM"](#)

### Criteri per l'inserimento dei volumi nelle SVM di destinazione

Durante la replica dei volumi dalla SVM di origine alla SVM di destinazione, è importante conoscere i criteri per la selezione degli aggregati.

Gli aggregati vengono selezionati in base ai seguenti criteri:

- I volumi vengono sempre posizionati su aggregati non root.
- Gli aggregati non root vengono selezionati in base allo spazio libero disponibile e al numero di volumi già ospitati nell'aggregato.

Gli aggregati con più spazio libero e meno volumi hanno la priorità. Viene selezionato l'aggregato con la priorità più alta.

- I volumi di origine sugli aggregati FabricPool vengono collocati su aggregati FabricPool sulla destinazione con la stessa policy di tiering.
- Se un volume sulla SVM di origine si trova su un aggregato di Flash Pool, il volume viene collocato su un aggregato di Flash Pool sulla SVM di destinazione, se tale aggregato esiste e dispone di spazio libero sufficiente.
- Se il `-space-guarantee` l'opzione del volume replicato è impostata su `volume`, vengono presi in considerazione solo gli aggregati con spazio libero maggiore della dimensione del volume.
- Le dimensioni del volume aumentano automaticamente sulla SVM di destinazione durante la replica, in base alle dimensioni del volume di origine.

Se si desidera riservare in anticipo le dimensioni sulla SVM di destinazione, è necessario ridimensionare il volume. Le dimensioni del volume non si riducono automaticamente sulla SVM di destinazione in base alla SVM di origine.

Se si desidera spostare un volume da un aggregato all'altro, è possibile utilizzare `volume move` Sulla SVM di destinazione.

## Replica di un'intera configurazione SVM

È possibile utilizzare `-identity-preserve true` opzione di `snapmirror create` Per replicare un'intera configurazione SVM.

### Prima di iniziare

I cluster di origine e di destinazione e le SVM devono essere peering. Per ulteriori informazioni, vedere ["Creare una relazione peer del cluster"](#) e ["Creare una relazione peer tra cluster SVM"](#).

Per la sintassi completa dei comandi, vedere la pagina man.

### A proposito di questa attività

Questo flusso di lavoro presuppone che si stia già utilizzando un criterio predefinito o un criterio di replica personalizzato.

A partire da ONTAP 9.9.1, quando si utilizza la policy del vault mirror, è possibile creare policy Snapshot diverse sulla SVM di origine e di destinazione e le copie Snapshot sulla destinazione non vengono sovrascritte dalle copie Snapshot sull'origine. Per ulteriori informazioni, vedere ["Informazioni sulla replica di SnapMirror SVM"](#).

### Fasi

1. Creare una SVM di destinazione:

```
vserver create -vserver SVM_name -subtype dp-destination
```

Il nome SVM deve essere univoco nei cluster di origine e di destinazione.

Nell'esempio seguente viene creata una SVM di destinazione denominata `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. Dal cluster di destinazione, creare una relazione peer SVM utilizzando `vserver peer create` comando.

Per ulteriori informazioni, vedere ["Creare una relazione peer tra cluster SVM"](#).

3. Creare una pianificazione del processo di replica:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare all per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.



La pianificazione minima supportata (RPO) per i volumi FlexVol in una relazione SnapMirror SVM è di 15 minuti. La pianificazione minima supportata (RPO) per i volumi FlexGroup in una relazione SnapMirror SVM è di 30 minuti.

Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` il sabato alle 3:00:

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

4. Dalla SVM di destinazione o dal cluster di destinazione, creare una relazione di replica:

```
snapmirror create -source-path SVM_name: -destination-path SVM_name: -type
DP|XDP -schedule schedule -policy policy -identity-preserve true
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni.

Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve true
```

Nell'esempio seguente viene creata una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` policy:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

Supponendo di aver creato un criterio personalizzato con il tipo di criterio `async-mirror`, Nell'esempio seguente viene creata una relazione di DR di SnapMirror:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity  
-preserve true
```

Supponendo di aver creato un criterio personalizzato con il tipo di criterio `mirror-vault`, nell'esempio seguente viene creata una relazione di replica unificata:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity  
-preserve true
```

#### 5. Arrestare la SVM di destinazione:

```
vserver stop
```

*SVM name*

Nell'esempio seguente viene interrotta una SVM di destinazione denominata `dvs1`:

```
cluster_dst::> vserver stop -vserver dvs1
```

#### 6. Dalla SVM di destinazione o dal cluster di destinazione, inizializzare la relazione di replica SVM: +

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

Nell'esempio seguente viene inizializzata la relazione tra la SVM di origine, `svm1` e la SVM di destinazione, `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination  
-path svm_backup:
```

### Escludere le LIF e le relative impostazioni di rete dalla replica SVM

Se le SVM di origine e di destinazione si trovano in sottoreti diverse, è possibile utilizzare `-discard-configs network` opzione di `snapmirror policy create` Comando per escludere le LIF e le relative impostazioni di rete dalla replica SVM.

#### Di cosa hai bisogno

I cluster di origine e di destinazione e le SVM devono essere peering.

Per ulteriori informazioni, vedere ["Creare una relazione peer del cluster"](#) e ["Creare una relazione peer tra cluster SVM"](#).

#### A proposito di questa attività

Il `-identity-preserve` opzione di `snapmirror create` il comando deve essere impostato su `true` Quando si crea la relazione di replica SVM.

Per la sintassi completa dei comandi, vedere la pagina `man`.

## Fasi

1. Creare una SVM di destinazione:

```
vserver create -vserver SVM -subtype dp-destination
```

Il nome SVM deve essere univoco nei cluster di origine e di destinazione.

Nell'esempio seguente viene creata una SVM di destinazione denominata `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. Dal cluster di destinazione, creare una relazione peer SVM utilizzando `vserver peer create` comando.

Per ulteriori informazioni, vedere ["Creare una relazione peer tra cluster SVM"](#).

3. Creare una pianificazione del processo:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.



La pianificazione minima supportata (RPO) per i volumi FlexVol in una relazione SnapMirror SVM è di 15 minuti. La pianificazione minima supportata (RPO) per i volumi FlexGroup in una relazione SnapMirror SVM è di 30 minuti.

Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` Il sabato alle 3:00:

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek  
"Saturday" -hour 3 -minute 0
```

4. Creare un criterio di replica personalizzato:

```
snapmirror policy create -vserver SVM -policy policy -type async-  
mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer  
-priority low|normal -is-network-compression-enabled true|false -discard  
-configs network
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene creato un criterio di replica personalizzato per il DR SnapMirror che esclude le LIF:

```
cluster_dst:> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

Nell'esempio seguente viene creata una policy di replica personalizzata per la replica unificata che esclude le LIF:

```
cluster_dst:> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

5. Dalla SVM di destinazione o dal cluster di destinazione, eseguire il seguente comando per creare una relazione di replica:

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve true|false
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere gli esempi riportati di seguito.

Nell'esempio seguente viene creata una relazione di DR di SnapMirror che esclude i LIF:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy DR_exclude_LIFs
-identity-preserve true
```

Nell'esempio seguente viene creata una relazione di replica unificata di SnapMirror che esclude le LIF:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy unified_exclude_LIFs
-identity-preserve true
```

6. Arrestare la SVM di destinazione:

```
vserver stop
```

*SVM name*

Nell'esempio seguente viene interrotta una SVM di destinazione denominata dvs1:

```
cluster_dst:> vserver stop -vserver dvs1
```

7. Dalla SVM di destinazione o dal cluster di destinazione, inizializzare una relazione di replica:

```
snapmirror initialize -source-path SVM: -destination-path SVM:
```



Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene inizializzata la relazione tra l'origine, `svm1` e la destinazione, `svm_backup`:

```
cluster_dst:> snapmirror initialize -source-path svm1: -destination  
-path svm_backup:
```

### Al termine

È necessario configurare la rete e i protocolli sulla SVM di destinazione per l'accesso ai dati in caso di disastro.

### Escludere la rete, il servizio nomi e altre impostazioni dalla replica SVM

È possibile utilizzare `-identity-preserve false` opzione di `snapmirror create` Per replicare solo i volumi e le configurazioni di sicurezza di una SVM. Vengono mantenute anche alcune impostazioni del protocollo e del servizio nomi.

### A proposito di questa attività

Per un elenco delle impostazioni preservate del protocollo e del servizio nomi, vedere ["Configurazioni replicate nelle relazioni di DR SVM"](#).

Per la sintassi completa dei comandi, vedere la pagina man.

### Prima di iniziare

I cluster di origine e di destinazione e le SVM devono essere peering.

Per ulteriori informazioni, vedere ["Creare una relazione peer del cluster"](#) e ["Creare una relazione peer tra cluster SVM"](#).

### Fasi

1. Creare una SVM di destinazione:

```
vserver create -vserver SVM -subtype dp-destination
```

Il nome SVM deve essere univoco nei cluster di origine e di destinazione.

Nell'esempio seguente viene creata una SVM di destinazione denominata `svm_backup`:

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. Dal cluster di destinazione, creare una relazione peer SVM utilizzando `vserver peer create` comando.

Per ulteriori informazioni, vedere ["Creare una relazione peer tra cluster SVM"](#).

3. Creare una pianificazione del processo di replica:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week  
-day day_of_month -hour hour -minute minute
```

Per `-month`, `-dayofweek`, e. `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.



La pianificazione minima supportata (RPO) per i volumi FlexVol in una relazione SnapMirror SVM è di 15 minuti. La pianificazione minima supportata (RPO) per i volumi FlexGroup in una relazione SnapMirror SVM è di 30 minuti.

Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` il sabato alle 3:00:

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

4. Creare una relazione di replica che escluda le impostazioni di rete, name service e altre impostazioni di configurazione:

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve false
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e. `-destination-path` opzioni. Vedere gli esempi riportati di seguito. È necessario eseguire questo comando dalla SVM di destinazione o dal cluster di destinazione.

Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita `MirrorAllSnapshots` policy. La relazione esclude la rete, il servizio nomi e altre impostazioni di configurazione dalla replica SVM:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

Nell'esempio seguente viene creata una relazione di replica unificata utilizzando l'impostazione predefinita `MirrorAndVault` policy. La relazione esclude le impostazioni di rete, name service e altre impostazioni di configurazione:

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

Supponendo di aver creato un criterio personalizzato con il tipo di criterio `async-mirror`, Nell'esempio seguente viene creata una relazione di DR di SnapMirror. La relazione esclude la rete, il servizio nomi e altre impostazioni di configurazione dalla replica SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity  
-preserve false
```

Supponendo di aver creato un criterio personalizzato con il tipo di criterio `mirror-vault`, nell'esempio seguente viene creata una relazione di replica unificata. La relazione esclude la rete, il servizio nomi e altre impostazioni di configurazione dalla replica SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path  
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity  
-preserve false
```

#### 5. Arrestare la SVM di destinazione:

```
vserver stop
```

*SVM name*

Nell'esempio seguente viene interrotta una SVM di destinazione denominata `dvs1`:

```
destination_cluster::> vserver stop -vserver dvs1
```

#### 6. Se si utilizza SMB, è necessario configurare anche un server SMB.

Vedere ["Solo SMB: Creazione di un server SMB"](#).

#### 7. Dalla SVM di destinazione o dal cluster di destinazione, inizializzare la relazione di replica SVM:

```
snapmirror initialize -source-path SVM_name: -destination-path SVM_name:
```

#### Al termine

È necessario configurare la rete e i protocolli sulla SVM di destinazione per l'accesso ai dati in caso di disastro.

#### Specificare gli aggregati da utilizzare per le relazioni di DR SVM

Dopo aver creato una SVM per il disaster recovery, è possibile utilizzare `aggr-list` opzione con `vserver modify` Comando per limitare gli aggregati utilizzati per ospitare i volumi di destinazione DR SVM.

#### Fase

##### 1. Creare una SVM di destinazione:

```
vserver create -vserver SVM -subtype dp-destination
```

##### 2. Modificare l'elenco di server SVM per il disaster recovery per limitare gli aggregati utilizzati per ospitare il volume SVM per il disaster recovery:

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

## Solo SMB: Creare un server SMB

Se la SVM di origine dispone di una configurazione SMB e si è scelto di impostarla `identity-preserve a. false`, È necessario creare un server SMB per la SVM di destinazione. Il server SMB è necessario per alcune configurazioni SMB, come ad esempio le condivisioni durante l'inizializzazione della relazione SnapMirror.

### Fasi

1. Avviare la SVM di destinazione utilizzando `vserver start` comando.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

2. Verificare che la SVM di destinazione si trovi in `running` lo stato e il sottotipo sono `dp-destination` utilizzando `vserver show` comando.

```
destination_cluster::> vserver show
```

|           |       |                | Admin   | Operational | Root   |       |
|-----------|-------|----------------|---------|-------------|--------|-------|
| Vserver   | Type  | Subtype        | State   | State       | Volume |       |
| Aggregate |       |                |         |             |        |       |
| -----     | ----- | -----          | -----   | -----       | -----  | ----- |
| dvs1      | data  | dp-destination | running | running     | -      | -     |

3. Creare una LIF utilizzando `network interface create` comando.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101 -address 192.0.2.128 -netmask 255.255.255.128
```

4. Creare un percorso utilizzando `network route create` comando.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

### "Gestione della rete"

5. Configurare il DNS utilizzando `vserver services dns create` comando.

```
destination_cluster::>vserver services dns create -domains  
mydomain.example.com -vserver  
dvs1 -name-servers 192.0.2.128 -state enabled
```

6. Aggiungere il domain controller preferito utilizzando `vserver cifs domain preferred-dc add` comando.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1  
-preferred-dc  
192.0.2.128 -domain mydomain.example.com
```

7. Creare il server SMB utilizzando `vserver cifs create` comando.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain  
mydomain.example.com  
-cifs-server CIFS1
```

8. Arrestare la SVM di destinazione utilizzando `vserver stop` comando.

```
destination_cluster::> vserver stop -vserver dvs1  
[Job 46] Job succeeded: DONE
```

## Escludere i volumi dalla replica SVM

Per impostazione predefinita, tutti i volumi di dati RW della SVM di origine vengono replicati. Se non si desidera proteggere tutti i volumi sulla SVM di origine, è possibile utilizzare `-vserver-dr-protection unprotected` opzione di `volume modify` Comando per escludere i volumi dalla replica SVM.

### Fasi

1. Escludere un volume dalla replica SVM:

```
volume modify -vserver SVM -volume volume -vserver-dr-protection unprotected
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

Il seguente esempio esclude il volume `volA_src` Dalla replica SVM:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr  
-protection unprotected
```

Se in seguito si desidera includere un volume nella replica SVM precedentemente esclusa, eseguire il

seguinte comando:

```
volume modify -vserver SVM -volume volume -vserver-dr-protection protected
```

Il seguente esempio include il volume volA\_src Nella replica SVM:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr  
-protection protected
```

2. Creare e inizializzare la relazione di replica SVM come descritto in ["Replica di un'intera configurazione SVM"](#).

## Fornire i dati da una destinazione DR SVM

### Workflow di disaster recovery SVM

Per eseguire il ripristino da un disastro e fornire i dati dalla SVM di destinazione, è necessario attivare la SVM di destinazione. L'attivazione della SVM di destinazione comporta l'interruzione dei trasferimenti pianificati di SnapMirror, l'interruzione dei trasferimenti in corso di SnapMirror, l'interruzione della relazione di replica, l'interruzione della SVM di origine e l'avvio della SVM di destinazione.



#### Rendere scrivibili i volumi di destinazione SVM

È necessario rendere scrivibili i volumi di destinazione SVM prima di poter fornire i dati ai client. La procedura è in gran parte identica alla procedura per la replica del volume, con un'eccezione. Se si imposta `-identity-preserve true` Una volta creata la relazione di replica SVM, è necessario arrestare la SVM di origine prima di attivare la SVM di destinazione.

#### A proposito di questa attività

Per la sintassi completa dei comandi, vedere la pagina man.



In uno scenario di disaster recovery, non è possibile eseguire un aggiornamento di SnapMirror dalla SVM di origine alla SVM di destinazione del disaster recovery perché la SVM di origine e i relativi dati non saranno accessibili e poiché gli aggiornamenti dall'ultima risincronizzazione potrebbero essere danneggiati o danneggiati.

## Fasi

1. Dalla SVM di destinazione o dal cluster di destinazione, interrompere i trasferimenti pianificati verso la destinazione:

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente vengono interrotti i trasferimenti pianificati tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination-path  
svm_backup:
```

2. Dalla SVM di destinazione o dal cluster di destinazione, interrompere i trasferimenti in corso alla destinazione:

```
snapmirror abort -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

L'esempio seguente interrompe i trasferimenti in corso tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path  
svm_backup:
```

3. Dalla SVM di destinazione o dal cluster di destinazione, interrompere la relazione di replica:

```
snapmirror break -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene spezzata la relazione tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:



```
cluster_dst:> snapmirror break -source-path svm1: -destination-path  
svm_backup:
```

4. Se si imposta `-identity-preserve true` Una volta creata la relazione di replica SVM, interrompere la SVM di origine:

```
vserver stop -vserver SVM
```

Nell'esempio seguente viene interrotta la SVM di origine `svm1`:

```
cluster_src:> vserver stop svm1
```

5. Avviare la SVM di destinazione:

```
vserver start -vserver SVM
```

Nell'esempio seguente viene avviata la SVM di destinazione `svm_backup`:

```
cluster_dst:> vserver start svm_backup
```

### Al termine

Configurare i volumi di destinazione SVM per l'accesso ai dati, come descritto in ["Configurazione del volume di destinazione per l'accesso ai dati"](#).

## Riattivare l'SVM di origine

### Workflow di riattivazione SVM di origine

Se la SVM di origine esiste dopo un disastro, è possibile riattivarla e proteggerla ricreando la relazione di disaster recovery di SVM.



### Riattivare l'SVM di origine originale

È possibile ristabilire la relazione di protezione dei dati originale tra la SVM di origine e di destinazione quando non è più necessario fornire dati dalla destinazione. La procedura è in gran parte identica alla procedura per la replica del volume, con un'eccezione. È necessario arrestare la SVM di destinazione prima di riattivare la SVM di origine.

#### Prima di iniziare

Se si sono aumentate le dimensioni del volume di destinazione durante la distribuzione dei dati da esso, prima di riattivare il volume di origine, è necessario aumentare manualmente la dimensione massima automatica sul volume di origine per garantire che possa crescere in modo sufficiente.

#### "Quando un volume di destinazione cresce automaticamente"

#### A proposito di questa attività

A partire da ONTAP 9.11.1, è possibile ridurre il tempo di risincronizzazione durante una prova di disaster recovery utilizzando `-quick-resync true` opzione di `snapmirror resync`. Durante l'esecuzione di una risincronizzazione inversa di una relazione DR SVM. Una rapida risincronizzazione può ridurre il tempo necessario per tornare alla produzione ignorando le operazioni di ricostruzione e ripristino del data warehouse.



La risincronizzazione rapida non preserva l'efficienza dello storage dei volumi di destinazione. L'attivazione della risincronizzazione rapida potrebbe aumentare lo spazio del volume utilizzato dai volumi di destinazione.

Questa procedura presuppone che la linea di base nel volume di origine originale sia intatta. Se la linea di

base non è intatta, è necessario creare e inizializzare la relazione tra il volume da cui si stanno fornendo i dati e il volume di origine originale prima di eseguire la procedura.

Per la sintassi completa dei comandi, vedere la pagina man.

## Fasi

1. Dalla SVM di origine originale o dal cluster di origine, creare una relazione DR SVM inversa utilizzando la stessa configurazione, policy e impostazioni di conservazione delle identità della relazione DR SVM originale:

```
snapmirror create -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene creata una relazione tra la SVM da cui vengono forniti i dati, `svm_backup` e la SVM di origine originale, `svm1`:

```
cluster_src:> snapmirror create -source-path svm_backup: -destination-path svm1:
```

2. Dalla SVM di origine originale o dal cluster di origine, eseguire il seguente comando per invertire la relazione di protezione dei dati:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.



Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

Nell'esempio seguente viene invertita la relazione tra la SVM di origine originale, `svm1` e la SVM da cui vengono forniti i dati, `svm_backup`:

```
cluster_src:> snapmirror resync -source-path svm_backup: -destination-path svm1:
```

Esempio di utilizzo dell'opzione `-quick-resync`:

```
cluster_src:> snapmirror resync -source-path svm_backup: -destination-path svm1: -quick-resync true
```

3. Quando si è pronti a ristabilire l'accesso ai dati alla SVM di origine, arrestare la SVM di destinazione originale per disconnettere tutti i client attualmente connessi alla SVM di destinazione originale.

```
vserver stop -vserver SVM
```

Nell'esempio riportato di seguito viene interrotta la SVM di destinazione originale che attualmente fornisce i dati:

```
cluster_dst:> vserver stop svm_backup
```

4. Verificare che la SVM di destinazione originale si trovi nello stato arrestato utilizzando `vserver show` comando.

```
cluster_dst:> vserver show
```

| Vserver    | Type  | Subtype | Admin State | Operational State | Root Volume |
|------------|-------|---------|-------------|-------------------|-------------|
| Aggregate  |       |         |             |                   |             |
| -----      | ----- | -----   | -----       | -----             | -----       |
| svm_backup | data  | default | stopped     | stopped           | rv          |
| aggr1      |       |         |             |                   |             |

5. Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per eseguire l'aggiornamento finale della relazione inversa e trasferire tutte le modifiche dalla SVM di destinazione originale alla SVM di origine:

```
snapmirror update -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio riportato di seguito viene aggiornata la relazione tra la SVM di destinazione originale da cui vengono forniti i dati, `svm_backup` e la SVM di origine originale, `svm1`:

```
cluster_src:> snapmirror update -source-path svm_backup: -destination-path svm1:
```

6. Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per interrompere i trasferimenti pianificati per la relazione inversa:

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente vengono interrotti i trasferimenti pianificati tra la SVM da cui si stanno fornendo i

dati, svm\_backup`E la SVM originale, `svm1:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination  
-path svm1:
```

7. Quando l'aggiornamento finale è completo e la relazione indica "Quiesced" per lo stato della relazione, eseguire il seguente comando dalla SVM di origine o dal cluster di origine originale per interrompere la relazione invertita:

```
snapmirror break -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene spezzata la relazione tra la SVM di destinazione originale da cui si stavano servendo i dati, svm\_backup`E la SVM di origine originale, `svm1:

```
cluster_src::> snapmirror break -source-path svm_backup: -destination  
-path svm1:
```

8. Se la SVM di origine originale è stata precedentemente arrestata, dal cluster di origine, avviare la SVM di origine originale:

```
vserver start -vserver SVM
```

Nell'esempio seguente viene avviata la SVM di origine originale:

```
cluster_src::> vserver start svm1
```

9. Dalla SVM di destinazione originale o dal cluster di destinazione originale, ristabilire la relazione di protezione dei dati originale:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene ristabilita la relazione tra la SVM di origine originale, svm1`E la SVM di destinazione originale, `svm\_backup:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path  
svm_backup:
```

10. Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per eliminare la relazione di protezione dei dati invertita:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene eliminata la relazione inversa tra la SVM di destinazione originale, `svm_backup` e la SVM di origine originale, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination  
-path svm1:
```

11. Dalla SVM di destinazione originale o dal cluster di destinazione originale, rilasciare la relazione di protezione dei dati invertita:

```
snapmirror release -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene rilasciata la relazione inversa tra SVM di destinazione originale, `svm_backup` e SVM di origine, `svm1`

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination  
-path svm1:
```

## Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina `man`.

## Riattivare la SVM di origine originale (solo volumi FlexGroup)

È possibile ristabilire la relazione di protezione dei dati originale tra la SVM di origine e di destinazione quando non è più necessario fornire dati dalla destinazione. Per riattivare la SVM di origine originale quando si utilizzano volumi FlexGroup, è necessario eseguire alcuni passaggi aggiuntivi, tra cui l'eliminazione della relazione DR SVM originale e il rilascio della relazione originale prima di annullare la relazione. È inoltre necessario rilasciare la relazione invertita e ricreare la relazione originale prima di interrompere i trasferimenti pianificati.

## Fasi

1. Dalla SVM di destinazione originale o dal cluster di destinazione originale, eliminare la relazione DR SVM originale:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene eliminata la relazione originale tra SVM di origine, `svm1` e SVM di destinazione originale, `svm_backup`:

```
cluster_dst:> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

2. Dalla SVM di origine originale o dal cluster di origine originale, rilasciare la relazione originale mantenendo intatte le copie Snapshot:

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
-only true
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene rilasciata la relazione originale tra SVM di origine, `svm1` e SVM di destinazione originale, `svm_backup`.

```
cluster_src:> snapmirror release -source-path svm1: -destination-path
svm_backup: -relationship-info-only true
```

3. Dalla SVM di origine originale o dal cluster di origine, creare una relazione DR SVM inversa utilizzando la stessa configurazione, policy e impostazioni di conservazione delle identità della relazione DR SVM originale:

```
snapmirror create -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene creata una relazione tra la SVM da cui vengono forniti i dati, `svm_backup` e la SVM di origine originale, `svm1`:

```
cluster_src:> snapmirror create -source-path svm_backup: -destination
-path svm1:
```

4. Dalla SVM di origine originale o dal cluster di origine, eseguire il seguente comando per invertire la relazione di protezione dei dati:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.



Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

Nell'esempio seguente viene invertita la relazione tra la SVM di origine originale, `svm1` e la SVM da cui vengono forniti i dati, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

- Quando si è pronti a ristabilire l'accesso ai dati alla SVM di origine, arrestare la SVM di destinazione originale per disconnettere tutti i client attualmente connessi alla SVM di destinazione originale.

```
vserver stop -vserver SVM
```

Nell'esempio riportato di seguito viene interrotta la SVM di destinazione originale che attualmente fornisce i dati:

```
cluster_dst::> vserver stop svm_backup
```

- Verificare che la SVM di destinazione originale si trovi nello stato arrestato utilizzando `vserver show` comando.

```
cluster_dst::> vserver show
```

| Vserver    | Type  | Subtype | Admin State | Operational State | Root Volume |
|------------|-------|---------|-------------|-------------------|-------------|
| Aggregate  |       |         |             |                   |             |
| -----      | ----- | -----   | -----       | -----             | -----       |
| svm_backup | data  | default | stopped     | stopped           | rv          |
| aggr1      |       |         |             |                   |             |

- Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per eseguire l'aggiornamento finale della relazione inversa e trasferire tutte le modifiche dalla SVM di destinazione originale alla SVM di origine:

```
snapmirror update -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.



Nell'esempio riportato di seguito viene aggiornata la relazione tra la SVM di destinazione originale da cui vengono forniti i dati, `svm_backup` e la SVM di origine originale, `svm1`:

```
cluster_src:> snapmirror update -source-path svm_backup: -destination-path svm1:
```

8. Dalla SVM di origine originale o dal cluster di origine originale, eseguire il seguente comando per interrompere i trasferimenti pianificati per la relazione inversa:

```
snapmirror quiesce -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente vengono interrotti i trasferimenti pianificati tra la SVM da cui si stanno fornendo i dati, `svm_backup` e la SVM originale, `svm1`:

```
cluster_src:> snapmirror quiesce -source-path svm_backup: -destination-path svm1:
```

9. Quando l'aggiornamento finale è completo e la relazione indica "Quiesced" per lo stato della relazione, eseguire il seguente comando dalla SVM di origine o dal cluster di origine originale per interrompere la relazione invertita:

```
snapmirror break -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene spezzata la relazione tra la SVM di destinazione originale da cui si stavano servendo i dati, `svm_backup` e la SVM di origine originale, `svm1`:

```
cluster_src:> snapmirror break -source-path svm_backup: -destination-path svm1:
```

10. Se la SVM di origine originale è stata precedentemente arrestata, dal cluster di origine, avviare la SVM di origine originale:

```
vserver start -vserver SVM
```

Nell'esempio seguente viene avviata la SVM di origine originale:

```
cluster_src:> vserver start svm1
```

11. Dalla SVM di origine originale o dal cluster di origine, eliminare la relazione DR SVM inversa:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene eliminata la relazione inversa tra SVM di destinazione originale, `svm_backup` e SVM di origine, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination  
-path svm1:
```

12. Dalla SVM di destinazione originale o dal cluster di destinazione originale, rilasciare la relazione invertita mantenendo intatte le copie Snapshot:

```
snapmirror release -source-path SVM: -destination-path SVM: -relationship-info  
-only true
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene rilasciata la relazione inversa tra SVM di destinazione originale, `svm_backup` e SVM di origine, `svm1`:

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination  
-path svm1: -relationship-info-only true
```

13. Dalla SVM di destinazione originale o dal cluster di destinazione originale, ricreare la relazione originale. Utilizzare le stesse impostazioni di configurazione, policy e conservazione delle identità della relazione DR SVM originale:

```
snapmirror create -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene creata una relazione tra la SVM di origine originale, `svm1` e la SVM di destinazione originale, `svm_backup`:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path  
svm_backup:
```

14. Dalla SVM di destinazione originale o dal cluster di destinazione originale, ristabilire la relazione di protezione dei dati originale:

```
snapmirror resync -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene ristabilita la relazione tra la SVM di origine originale, `svm1` e la SVM di destinazione originale, `svm_backup`:

```
cluster_dst:> snapmirror resync -source-path svm1: -destination-path  
svm_backup:
```

## Convertire le relazioni di replica dei volumi in una relazione di replica SVM

È possibile convertire le relazioni di replica tra i volumi in una relazione di replica tra le macchine virtuali di storage (SVM) che possiedono i volumi, a condizione che ciascun volume sull'origine (eccetto il volume root) venga replicato, inoltre, ciascun volume di origine (incluso il volume root) ha lo stesso nome del volume di destinazione.

### A proposito di questa attività

Utilizzare `volume rename` Quando la relazione SnapMirror è inattiva per rinominare i volumi di destinazione, se necessario.

### Fasi

1. Dalla SVM di destinazione o dal cluster di destinazione, eseguire il seguente comando per risincronizzare i volumi di origine e di destinazione:

```
snapmirror resync -source-path SVM:volume -destination-path SVM:volume -type  
DP|XDP -policy policy
```

Per la sintassi completa dei comandi, vedere la pagina `man`.



Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine `volA` acceso `svm1` e il volume di destinazione `volA` acceso `svm_backup`:

```
cluster_dst:> snapmirror resync -source-path svm1:volA -destination  
-path svm_backup:volA
```

2. Creare una relazione di replica SVM tra le SVM di origine e di destinazione, come descritto in ["Replica delle configurazioni SVM"](#).

È necessario utilizzare `-identity-preserve true` opzione di `snapmirror create` quando si crea la relazione di replica.

3. Arrestare la SVM di destinazione:

```
vserver stop -vserver SVM
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene interrotta la SVM di destinazione `svm_backup`:

```
cluster_dst:> vserver stop svm_backup
```

4. Dalla SVM di destinazione o dal cluster di destinazione, eseguire il seguente comando per risincronizzare le SVM di origine e di destinazione:

```
snapmirror resync -source-path SVM: -destination-path SVM: -type DP|XDP  
-policy policy
```

Per la sintassi completa dei comandi, vedere la pagina man.



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

Nell'esempio seguente viene risincronizzata la relazione tra la SVM di origine `svm1` e la SVM di destinazione `svm_backup`:

```
cluster_dst:> snapmirror resync -source-path svm1: -destination-path  
svm_backup:
```

## Eliminare una relazione di replica SVM

È possibile utilizzare `snapmirror delete` e `snapmirror release` Comandi per eliminare una relazione di replica SVM. È quindi possibile eliminare manualmente i volumi di destinazione non necessari.

### A proposito di questa attività

Il `snapmirror release` Il comando elimina tutte le copie Snapshot create da SnapMirror dall'origine. È possibile utilizzare `-relationship-info-only` Opzione per conservare le copie Snapshot.

Per la sintassi completa dei comandi, vedere la pagina man.

### Fasi

1. Eseguire il seguente comando dalla SVM di destinazione o dal cluster di destinazione per interrompere la relazione di replica:

```
snapmirror break -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene spezzata la relazione tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

```
cluster_dst:> snapmirror break -source-path svm1: -destination-path  
svm_backup:
```

2. Eseguire il seguente comando dalla SVM di destinazione o dal cluster di destinazione per eliminare la relazione di replica:

```
snapmirror delete -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio seguente viene eliminata la relazione tra la SVM di origine `svm1` E la SVM di destinazione `svm_backup`:

```
cluster_dst:> snapmirror delete -source-path svm1: -destination-path  
svm_backup:
```

3. Eseguire il seguente comando dal cluster di origine o dalla SVM di origine per rilasciare le informazioni sulle relazioni di replica dalla SVM di origine:

```
snapmirror release -source-path SVM: -destination-path SVM:
```



Inserire i due punti (:) dopo il nome SVM in `-source-path` e `-destination-path` opzioni. Vedere l'esempio riportato di seguito.

Nell'esempio riportato di seguito vengono rilasciate informazioni per la relazione di replica specificata dalla SVM di origine `svm1`:

```
cluster_src:> snapmirror release -source-path svm1: -destination-path  
svm_backup:
```

## Gestire la replica del volume root di SnapMirror

### Panoramica sulla gestione della replica del volume root di SnapMirror

Ogni SVM in un ambiente NAS ha uno spazio dei nomi unico. Il *volume root di SVM*, contenente il sistema operativo e le relative informazioni, è il punto di ingresso della gerarchia dello spazio dei nomi. Per garantire che i dati rimangano accessibili ai client in caso di interruzione o failover di un nodo, è necessario creare una copia mirror di condivisione del carico del volume root SVM.

Lo scopo principale dei mirror di condivisione del carico per i volumi root SVM non è più la condivisione del carico, ma il loro scopo è il disaster recovery.

- Se il volume root non è temporaneamente disponibile, il mirror di load-sharing fornisce automaticamente l'accesso in sola lettura ai dati del volume root.
- Se il volume root non è disponibile in modo permanente, è possibile promuovere uno dei volumi di load sharing per fornire l'accesso in scrittura ai dati del volume root.

## Creare e inizializzare relazioni mirror di condivisione del carico

È necessario creare un mirror di condivisione del carico (LSM) per ogni volume root SVM che serve i dati NAS nel cluster. Per i cluster che consistono di due o più coppie ha, è consigliabile considerare mirror di condivisione del carico dei root volumi SVM per garantire l'accessibilità del namespace ai client in caso affermativo. Si guastano entrambi i nodi di una coppia ha. I mirror per la condivisione del carico non sono adatti per i cluster costituiti da una singola coppia ha.

### A proposito di questa attività

Se si crea un LSM sullo stesso nodo e il nodo non è disponibile, si dispone di un singolo punto di errore e non si dispone di una seconda copia per garantire che i dati rimangano accessibili ai client. Tuttavia, quando si crea il LSM su un nodo diverso da quello contenente il volume root o su una coppia ha diversa, i dati rimangono accessibili in caso di interruzione.

Ad esempio, in un cluster a quattro nodi con un volume root su tre nodi:

- Per il volume root sul nodo ha 1 1, creare il LSM sul nodo ha 2 1 o il nodo ha 2 2.
- Per il volume root sul nodo ha 1 2, creare il LSM sul nodo ha 2 1 o il nodo ha 2 2.
- Per il volume root sul nodo ha 2 1, creare il LSM sul nodo ha 1 1 o il nodo ha 1 2.

### Fasi

#### 1. Creare un volume di destinazione per LSM:

È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

Le dimensioni del volume di destinazione devono essere uguali o superiori a quelle del volume root.

Si consiglia di assegnare un nome al volume root e a quello di destinazione con suffissi, ad esempio `_root` e `_m1`.

Per la sintassi completa dei comandi, vedere la pagina `man`.

Nell'esempio seguente viene creato un volume mirror per la condivisione del carico per il volume root `svm1_root` poll `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate  
aggr_1 -size 1gb -state online -type DP
```

2. "Creare una pianificazione dei processi di replica".

3. Creare una relazione mirror di condivisione del carico tra il volume root SVM e il volume di destinazione per LSM:

È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

```
snapmirror create -source-path <SVM:volume> -destination-path  
<SVM:volume> -type LS -schedule <schedule>
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene creata una relazione mirror di condivisione del carico tra il volume root svm1\_root e il volume mirror per la condivisione del carico svm1\_m1:

```
cluster_src::> snapmirror create -source-path svm1:svm1_root  
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

L'attributo type del mirror di condivisione del carico cambia da DP a LS.

4. Inizializzare il mirror di condivisione del carico:

È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

L'inizializzazione può richiedere molto tempo. Si consiglia di eseguire il trasferimento di riferimento in ore non di punta.

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio riportato di seguito viene inizializzato il mirror di load sharing per il volume root svm1\_root:

```
cluster_src:> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

## Aggiornare una relazione mirror di condivisione del carico

Le relazioni del mirror di condivisione del carico (LSM) vengono aggiornate automaticamente per i volumi root SVM dopo che un volume nella SVM è stato montato o

dismontato e durante `volume create` operazioni che includono l'opzione `junction-path`. È possibile aggiornare manualmente una relazione LSM se si desidera che venga aggiornata prima del successivo aggiornamento pianificato.

Le relazioni mirror per la condivisione del carico si aggiornano automaticamente nei seguenti casi:

- È il momento di un aggiornamento pianificato
- Viene eseguita un'operazione di montaggio o disinstallazione su un volume nel volume root SVM
- R `volume create` viene emesso un comando che include `junction-path` opzione

## Fase

1. Aggiornare manualmente una relazione mirror di condivisione del carico:

È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

```
snapmirror update-ls-set -source-path <SVM:volume>
```

Nell'esempio riportato di seguito viene aggiornata la relazione del mirror di condivisione del carico per il volume root `svm1_root`:

```
cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
```

## Promuovere un mirror per la condivisione del carico

Se un volume root non è disponibile in modo permanente, è possibile promuovere il volume LOAD-sharing mirror (LSM) per fornire l'accesso in scrittura ai dati del volume root.

### Di cosa hai bisogno

Per questa attività, è necessario utilizzare i comandi avanzati del livello di privilegio.

## Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Promuovere un volume LSM:

È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

```
snapmirror promote -destination-path <SVM:volume>
```



Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente promuove il volume `svm1_m2` Come nuovo volume root SVM:

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
cluster_src://svm1/svm1_root and replace it with
cluster_src://svm1/svm1_m2. Because the volume is offline,
it is not possible to determine whether this promote will
affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

Invio `y`. ONTAP trasforma il volume LSM in un volume di lettura/scrittura ed elimina il volume root originale, se accessibile.



Il volume root promosso potrebbe non disporre di tutti i dati presenti nel volume root originale se l'ultimo aggiornamento non si è verificato di recente.

3. Torna al livello di privilegio admin:

```
set -privilege admin
```

4. Rinominare il volume promosso seguendo la convenzione di denominazione utilizzata per il volume root:

È necessario sostituire le variabili tra parentesi angolari con i valori richiesti prima di eseguire questo comando.

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

Nell'esempio riportato di seguito viene rinomina il volume promosso `svm1_m2` con il nome `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Proteggere il volume root rinominato, come descritto nei passaggi da 3 a 4 in ["Creazione e inizializzazione delle relazioni mirror di load sharing"](#).

## Dettagli tecnici di SnapMirror

### USA la corrispondenza del modello del nome del percorso

È possibile utilizzare la corrispondenza dei modelli per specificare i percorsi di origine e destinazione in `snapmirror` comandi.

`snapmirror` i comandi utilizzano nomi di percorso completi nel seguente formato: `vserver:volume`. È possibile abbreviare il nome del percorso senza inserire il nome SVM. In questo caso, il `snapmirror` Il comando presuppone il contesto SVM locale dell'utente.

Supponendo che SVM sia chiamato “vserver1” e che il volume sia chiamato “vol1”, il nome del percorso completo è `vserver1:vol1`.

È possibile utilizzare l'asterisco (\*) nei percorsi come carattere jolly per selezionare i nomi dei percorsi completi corrispondenti. Nella tabella seguente sono riportati alcuni esempi di utilizzo del carattere jolly per selezionare un intervallo di volumi.

|                    |                                                                                                    |
|--------------------|----------------------------------------------------------------------------------------------------|
| <code>*</code>     | Corrisponde a tutti i percorsi.                                                                    |
| <code>vs*</code>   | Consente di confrontare tutti gli SVM e i volumi con i nomi SVM che iniziano con <code>vs</code> . |
| <code>:*src</code> | Consente di confrontare tutti gli SVM con i nomi dei volumi che contengono <code>src</code> testo. |
| <code>:vol</code>  | Consente di confrontare tutti gli SVM con i nomi dei volumi che iniziano con <code>vol</code> .    |

```
vs1::> snapmirror show -destination-path *:*dest*
```

```
Progress
Source          Destination  Mirror          Relationship  Total
Last
Path            Type  Path            State          Status          Progress
Healthy Updated
-----
vs1:sm_src2
DP    vs2:sm_dest1
Snapmirrored  Idle
true    -
```

## Utilizza query estese per agire su molte relazioni SnapMirror

È possibile utilizzare *query estese* per eseguire contemporaneamente operazioni SnapMirror su molte relazioni SnapMirror. Ad esempio, potrebbero essere presenti più relazioni SnapMirror non inizializzate che si desidera inizializzare utilizzando un solo comando.

### A proposito di questa attività

È possibile applicare query estese alle seguenti operazioni SnapMirror:

- Inizializzazione delle relazioni non inizializzate
- Ripresa delle relazioni in quiescenza
- Risincronizzazione delle relazioni interrotte
- Aggiornamento delle relazioni inattive
- Interruzione dei trasferimenti di dati di relazione

### Fase

1. Eseguire un'operazione SnapMirror su molte relazioni:

```
snapmirror command {-state state } *
```

Il comando seguente inizializza le relazioni SnapMirror che si trovano in un Uninitialized stato:

```
vs1::> snapmirror initialize {-state Uninitialized} *
```

## Garantire una copia Snapshot comune in un'implementazione del vault mirror

È possibile utilizzare `snapmirror snapshot-owner create` Per conservare una copia Snapshot etichettata sul secondario in una distribuzione con vault mirror. In questo modo si garantisce l'esistenza di una copia Snapshot comune per l'aggiornamento della relazione del vault.

### A proposito di questa attività

Se si utilizza una combinazione di fan-out del vault mirror o distribuzione a cascata, tenere presente che gli aggiornamenti non avranno esito positivo se non esiste una copia Snapshot comune sui volumi di origine e di destinazione.

Questo non è mai un problema per la relazione del mirror in una distribuzione fan-out o cascata del vault mirror, poiché SnapMirror crea sempre una copia Snapshot del volume di origine prima di eseguire l'aggiornamento.

Tuttavia, potrebbe trattarsi di un problema per la relazione del vault, poiché SnapMirror non crea una copia Snapshot del volume di origine quando aggiorna una relazione del vault. È necessario utilizzare `snapmirror snapshot-owner create` Per garantire la presenza di almeno una copia Snapshot comune sia sull'origine che sulla destinazione della relazione del vault.

### Fasi

1. Sul volume di origine, assegnare un proprietario alla copia Snapshot etichettata che si desidera conservare:

```
snapmirror snapshot-owner create -vserver SVM -volume volume -snapshot  
snapshot -owner owner
```

L'esempio seguente assegna ApplicationA in qualità di proprietario di snap1 Copia Snapshot:

```
clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1  
-snapshot snap1 -owner ApplicationA
```

2. Aggiornare la relazione mirror, come descritto in ["Aggiornamento manuale di una relazione di replica"](#).

In alternativa, è possibile attendere l'aggiornamento pianificato della relazione mirror.

3. Trasferire la copia Snapshot etichettata nella destinazione del vault:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume, ... -destination  
-path SVM:volume|cluster://SVM/volume, ... -source-snapshot snapshot
```

Per la sintassi completa dei comandi, vedere la pagina man.

#### **Nell'esempio riportato di seguito viene trasferito il snap1 Copia Snapshot**

```
clust1::> snapmirror update -vserver vs1 -volume vol1  
-source-snapshot snap1
```

La copia Snapshot etichettata viene mantenuta quando la relazione del vault viene aggiornata.

4. Sul volume di origine, rimuovere il proprietario dalla copia Snapshot etichettata:

```
snapmirror snapshot-owner delete -vserver SVM -volume volume -snapshot  
snapshot -owner owner
```

I seguenti esempi vengono rimossi ApplicationA in qualità di proprietario di snap1 Copia Snapshot:

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1  
-snapshot snap1 -owner ApplicationA
```

## **Versioni ONTAP compatibili per le relazioni SnapMirror**

Prima di creare una relazione di data Protection SnapMirror, i volumi di origine e destinazione devono eseguire versioni di ONTAP compatibili. Prima di eseguire l'aggiornamento di ONTAP, devi verificare che la tua versione attuale di ONTAP sia compatibile con la tua versione di ONTAP di destinazione per le relazioni SnapMirror.

### **Relazioni di replica unificate**

Per le relazioni SnapMirror di tipo "XDP", utilizzando release on-premise o Cloud Volumes ONTAP:

A partire da ONTAP 9.9.0:



- Le release ONTAP 9.x,0 sono release solo per cloud e supportano i sistemi Cloud Volumes ONTAP. L'asterisco (\*) dopo la versione della release indica una release solo cloud.
- Le release ONTAP 9.x,1 sono release generali e supportano sistemi Cloud Volumes ONTAP e on-premise.



L'interoperabilità è bidirezionale.

### Interoperabilità per ONTAP versione 9.3 e successive

| Versione di ONTAP ... | Interagisce con queste versioni precedenti di ONTAP... |         |        |         |        |         |        |         |        |         |       |        |     |     |     |     |     |     |
|-----------------------|--------------------------------------------------------|---------|--------|---------|--------|---------|--------|---------|--------|---------|-------|--------|-----|-----|-----|-----|-----|-----|
|                       | 9.14.1                                                 | 9.14.0* | 9.13.1 | 9.13.0* | 9.12.1 | 9.12.0* | 9.11.1 | 9.11.0* | 9.10.1 | 9.10.0* | 9.9.1 | 9.9.0* | 9.8 | 9.7 | 9.6 | 9.5 | 9.4 | 9.3 |
| 9.14.1                | Sì                                                     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì    | Sì     | No  | No  | No  | No  | No  | No  |
| 9.14.0*               | Sì                                                     | Sì      | Sì     | No      | Sì     | No      | Sì     | No      | Sì     | No      | Sì    | No     | Sì  | No  | No  | No  | No  | No  |
| 9.13.1                | Sì                                                     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì    | Sì     | Sì  | No  | No  | No  | No  | No  |
| 9.13.0*               | Sì                                                     | No      | Sì     | Sì      | Sì     | No      | Sì     | No      | Sì     | No      | Sì    | No     | Sì  | No  | No  | No  | No  | No  |
| 9.12.1                | Sì                                                     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì    | Sì     | Sì  | Sì  | No  | No  | No  | No  |
| 9.12.0*               | Sì                                                     | No      | Sì     | No      | Sì     | Sì      | Sì     | No      | Sì     | No      | Sì    | No     | Sì  | Sì  | No  | No  | No  | No  |
| 9.11.1                | Sì                                                     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì    | Sì     | Sì  | Sì  | Sì  | No  | No  | No  |
| 9.11.0*               | Sì                                                     | No      | Sì     | No      | Sì     | No      | Sì     | Sì      | Sì     | No      | Sì    | No     | Sì  | Sì  | Sì  | No  | No  | No  |
| 9.10.1                | Sì                                                     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì    | Sì     | Sì  | Sì  | Sì  | Sì  | No  | No  |
| 9.10.0*               | Sì                                                     | No      | Sì     | No      | Sì     | No      | Sì     | No      | Sì     | Sì      | Sì    | No     | Sì  | Sì  | Sì  | Sì  | No  | No  |
| 9.9.1                 | Sì                                                     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì    | Sì     | Sì  | Sì  | Sì  | Sì  | No  | No  |
| 9.9.0*                | Sì                                                     | No      | Sì     | No      | Sì     | No      | Sì     | No      | Sì     | No      | Sì    | Sì     | Sì  | Sì  | Sì  | Sì  | No  | No  |
| 9.8                   | No                                                     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì     | Sì      | Sì    | Sì     | Sì  | Sì  | Sì  | Sì  | No  | Sì  |

|     |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|-----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 9.7 | No | No | No | No | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | No | Sì |
| 9.6 | No | No | No | No | No | No | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | No | Sì |
| 9.5 | No | No | No | No | No | No | No | No | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì | Sì |
| 9.4 | No | No | No | No | No | No | No | No | No | No | No | No | No | No | No | Sì | Sì | Sì |
| 9.3 | No | No | No | No | No | No | No | No | No | No | No | No | Sì | Sì | Sì | Sì | Sì | Sì |

## Relazioni sincroni di SnapMirror



SnapMirror Synchronous non è supportato per le istanze cloud di ONTAP.

| Versione di ONTAP ... | Interagisce con queste versioni precedenti di ONTAP... |        |        |        |        |       |     |     |     |     |
|-----------------------|--------------------------------------------------------|--------|--------|--------|--------|-------|-----|-----|-----|-----|
|                       | 9.14.1                                                 | 9.13.1 | 9.12.1 | 9.11.1 | 9.10.1 | 9.9.1 | 9.8 | 9.7 | 9.6 | 9.5 |
| 9.14.1                | Sì                                                     | Sì     | Sì     | Sì     | Sì     | Sì    | Sì  | No  | No  | No  |
| 9.13.1                | Sì                                                     | Sì     | Sì     | Sì     | Sì     | Sì    | Sì  | Sì  | No  | No  |
| 9.12.1                | Sì                                                     | Sì     | Sì     | Sì     | Sì     | Sì    | Sì  | Sì  | No  | No  |
| 9.11.1                | Sì                                                     | Sì     | Sì     | Sì     | Sì     | Sì    | No  | No  | No  | No  |
| 9.10.1                | Sì                                                     | Sì     | Sì     | Sì     | Sì     | Sì    | Sì  | No  | No  | No  |
| 9.9.1                 | Sì                                                     | Sì     | Sì     | Sì     | Sì     | Sì    | Sì  | Sì  | No  | No  |
| 9.8                   | Sì                                                     | Sì     | Sì     | No     | Sì     | Sì    | Sì  | Sì  | Sì  | No  |
| 9.7                   | No                                                     | Sì     | Sì     | No     | No     | Sì    | Sì  | Sì  | Sì  | Sì  |
| 9.6                   | No                                                     | No     | No     | No     | No     | No    | Sì  | Sì  | Sì  | Sì  |
| 9.5                   | No                                                     | No     | No     | No     | No     | No    | No  | Sì  | Sì  | Sì  |

## Relazioni di disaster recovery di SnapMirror SVM

- Per i dati di disaster recovery SVM e la protezione SVM:

Il disaster recovery delle SVM è supportato solo tra cluster che eseguono la stessa versione di ONTAP.

**L'indipendenza dalla versione non è supportata per la replica SVM.**

- Per il disaster recovery SVM per la migrazione SVM:
  - La replica è supportata in una singola direzione da una versione precedente di ONTAP sull'origine alla stessa o versione successiva di ONTAP sulla destinazione.
- La versione di ONTAP nel cluster di destinazione non deve essere più recente di due versioni principali on-premise o due versioni principali di cloud più recenti, come mostrato nella tabella seguente.
  - La replica non è supportata per i casi di utilizzo a lungo termine della protezione dei dati.

L'asterisco (\*) dopo la versione della release indica una release solo cloud.

Per determinare il supporto, individuare la versione di origine nella colonna della tabella a sinistra, quindi

individuare la versione di destinazione nella riga superiore (DR/migrazione per le versioni simili e migrazione solo per le versioni più recenti).

| Origine | Destinazione  |               |               |               |               |               |               |               |               |               |            |            |            |            |         |        |         |        |
|---------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|------------|------------|------------|------------|---------|--------|---------|--------|
|         | 9.3           | 9.4           | 9.5           | 9.6           | 9.7           | 9.8           | 9.9.0*        | 9.9.1         | 9.10.0*       | 9.10.1        | 9.11.0*    | 9.11.1     | 9.12.0*    | 9.12.1     | 9.13.0* | 9.13.1 | 9.14.0* | 9.14.1 |
| 9.3     | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |               |               |               |               |               |            |            |            |            |         |        |         |        |
| 9.4     |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |               |               |               |               |            |            |            |            |         |        |         |        |
| 9.5     |               |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |               |               |               |            |            |            |            |         |        |         |        |
| 9.6     |               |               |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |               |               |            |            |            |            |         |        |         |        |
| 9.7     |               |               |               |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |               |            |            |            |            |         |        |         |        |
| 9.8     |               |               |               |               |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |            |            |            |            |         |        |         |        |
| 9.9.0*  |               |               |               |               |               |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione |            |            |            |         |        |         |        |
| 9.9.1   |               |               |               |               |               |               |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione | Migrazione |            |            |         |        |         |        |
| 9.10.0* |               |               |               |               |               |               |               |               | Dr/migrazione | Migrazione    | Migrazione | Migrazione | Migrazione |            |         |        |         |        |
| 9.10.1  |               |               |               |               |               |               |               |               |               | Dr/migrazione | Migrazione | Migrazione | Migrazione | Migrazione |         |        |         |        |

|         |  |  |  |  |  |  |  |  |  |               |               |               |               |               |               |               |               |
|---------|--|--|--|--|--|--|--|--|--|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| 9.11.0* |  |  |  |  |  |  |  |  |  | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |               |               |               |
| 9.11.1  |  |  |  |  |  |  |  |  |  |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |               |               |
| 9.12.0* |  |  |  |  |  |  |  |  |  |               |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |               |
| 9.12.1  |  |  |  |  |  |  |  |  |  |               |               |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    | Migrazione    |
| 9.13.0* |  |  |  |  |  |  |  |  |  |               |               |               |               | Dr/migrazione | Migrazione    | Migrazione    | Migrazione    |
| 9.13.1  |  |  |  |  |  |  |  |  |  |               |               |               |               |               | Dr/migrazione | Migrazione    | Migrazione    |
| 9.14.0* |  |  |  |  |  |  |  |  |  |               |               |               |               |               |               | Dr/migrazione | Migrazione    |
| 9.14.1  |  |  |  |  |  |  |  |  |  |               |               |               |               |               |               |               | Dr/migrazione |

## Relazioni di disaster recovery di SnapMirror

Per le relazioni SnapMirror di tipo “DP” e di tipo di policy “async-mirror”:



I mirror di tipo DP non possono essere inizializzati a partire da ONTAP 9.11.1 e sono completamente deprecati in ONTAP 9.12.1. Per ulteriori informazioni, vedere ["Deprecazione delle relazioni SnapMirror per la protezione dei dati"](#).



Nella tabella seguente, la colonna a sinistra indica la versione di ONTAP sul volume di origine, mentre la riga superiore indica le versioni di ONTAP disponibili sul volume di destinazione.

| Origine | Destinazione |        |       |     |     |     |     |     |     |     |     |    |
|---------|--------------|--------|-------|-----|-----|-----|-----|-----|-----|-----|-----|----|
|         | 9.11.1       | 9.10.1 | 9.9.1 | 9.8 | 9.7 | 9.6 | 9.5 | 9.4 | 9.3 | 9.2 | 9.1 | 9  |
| 9.11.1  | Sì           | No     | No    | No  | No  | No  | No  | No  | No  | No  | No  | No |



|        |    |    |    |    |    |    |    |    |    |    |    |    |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|
| 9.10.1 | Sì | Sì | No | No | No | No | No | No | No | No | No | No |
| 9.9.1  | Sì | Sì | Sì | No | No | No | No | No | No | No | No | No |
| 9.8    | No | Sì | Sì | Sì | No | No | No | No | No | No | No | No |
| 9.7    | No | No | Sì | Sì | Sì | No | No | No | No | No | No | No |
| 9.6    | No | No | No | Sì | Sì | Sì | No | No | No | No | No | No |
| 9.5    | No | No | No | No | Sì | Sì | Sì | No | No | No | No | No |
| 9.4    | No | No | No | No | No | Sì | Sì | Sì | No | No | No | No |
| 9.3    | No | No | No | No | No | No | Sì | Sì | Sì | No | No | No |
| 9.2    | No | No | No | No | No | No | No | Sì | Sì | Sì | No | No |
| 9.1    | No | No | No | No | No | No | No | No | Sì | Sì | Sì | No |
| 9      | No | No | No | No | No | No | No | No | No | Sì | Sì | Sì |



L'interoperabilità non è bidirezionale.

## Limitazioni di SnapMirror

Prima di creare una relazione di protezione dei dati, è necessario conoscere le limitazioni di base di SnapMirror.

- Un volume di destinazione può avere un solo volume di origine.



Un volume di origine può avere più volumi di destinazione. Il volume di destinazione può essere il volume di origine per qualsiasi tipo di relazione di replica di SnapMirror.

- A seconda del modello di array, è possibile utilizzare un massimo di otto o sedici volumi di destinazione da un singolo volume di origine. Vedere ["Hardware Universe"](#) per ulteriori informazioni sulla configurazione specifica.
- Non è possibile ripristinare i file sulla destinazione di una relazione di DR di SnapMirror.
- I volumi SnapVault di origine o di destinazione non possono essere a 32 bit.
- Il volume di origine per una relazione SnapVault non deve essere un volume FlexClone.



La relazione funzionerà, ma l'efficienza offerta dai volumi FlexClone non verrà preservata.

## Archiviazione e conformità con la tecnologia SnapLock

### Che cos'è SnapLock

SnapLock è una soluzione per la compliance dalle performance elevate per le organizzazioni che utilizzano lo storage WORM per conservare i file in forma non modificata a scopo normativo e di governance.

SnapLock aiuta a prevenire l'eliminazione, la modifica o la ridenominazione dei dati per soddisfare normative

come SEC 17a-4, HIPAA, FINRA, CFTC e GDPR. Con SnapLock, è possibile creare volumi speciali in cui i file possono essere memorizzati e impegnati in uno stato non cancellabile e non scrivibile per un determinato periodo di conservazione o a tempo indeterminato. SnapLock consente di eseguire questa conservazione a livello di file attraverso protocolli di file aperti standard come CIFS e NFS. I protocolli di file aperti supportati per SnapLock sono NFS (versioni 2, 3 e 4) e CIFS (SMB 1.0, 2.0 e 3.0).

Utilizzando SnapLock, è possibile assegnare file e copie Snapshot allo storage WORM e impostare periodi di conservazione per i dati protetti DA WORM. Lo storage WORM di SnapLock utilizza la tecnologia Snapshot di NetApp e può sfruttare la replica SnapMirror e i backup SnapVault come tecnologia di base per fornire la protezione del backup recovery per i dati. Scopri di più sullo storage WORM: ["Storage WORM conforme con NetApp SnapLock - TR-4526"](#).

È possibile utilizzare un'applicazione per il commit dei file in WORM su NFS o CIFS oppure utilizzare la funzione di autocommit di SnapLock per il commit automatico dei file IN WORM. È possibile utilizzare un *file .WORM\_appendibile* per conservare i dati scritti in modo incrementale, ad esempio le informazioni di log. Per ulteriori informazioni, vedere ["Utilizzare la modalità di aggiunta del volume per creare file .WORM appendibili"](#).

SnapLock supporta metodi di protezione dei dati che devono soddisfare la maggior parte dei requisiti di conformità:

- È possibile utilizzare SnapLock per SnapVault per proteggere WORM le copie Snapshot sullo storage secondario. Vedere ["Assegnare le copie Snapshot a WORM"](#).
- È possibile utilizzare SnapMirror per replicare i file WORM in un'altra posizione geografica per il disaster recovery. Vedere ["Mirrorare i file WORM"](#).

SnapLock è una funzionalità basata su licenza di NetApp ONTAP. Una singola licenza consente di utilizzare SnapLock in modalità di conformità rigorosa, per soddisfare mandati esterni come la norma SEC 17a-4 e una modalità aziendale più allentata, per soddisfare le normative interne per la protezione delle risorse digitali. Le licenze SnapLock fanno parte di ["ONTAP uno"](#) suite software.

SnapLock è supportato su tutti i sistemi AFF e FAS e su ONTAP Select. SnapLock non è una soluzione solo software, ma è una soluzione hardware e software integrata. Questa distinzione è importante per le rigide normative WORM come SEC 17a-4, che richiede una soluzione hardware e software integrata. Per ulteriori informazioni, fare riferimento a ["SEC interpretation: Archiviazione elettronica dei record dei broker-dealer"](#).

## Cosa puoi fare con SnapLock

Dopo aver configurato SnapLock, è possibile completare le seguenti attività:

- ["Esegui il commit dei file su WORM"](#)
- ["Assegnare copie Snapshot a WORM per lo storage secondario"](#)
- ["Mirroring dei file WORM per il disaster recovery"](#)
- ["Conservare i file WORM durante i contenziosi utilizzando la conservazione a fini legali"](#)
- ["Eliminare i file WORM utilizzando la funzione di eliminazione con privilegi"](#)
- ["Impostare il periodo di conservazione del file"](#)
- ["Spostare un volume SnapLock"](#)
- ["Bloccare una copia Snapshot per la protezione dagli attacchi ransomware"](#)
- ["Esaminare l'utilizzo di SnapLock con il registro di controllo"](#)
- ["Utilizzare le API di SnapLock"](#)

## Conformità SnapLock e modalità aziendali

La conformità SnapLock e le modalità aziendali differiscono principalmente per il livello di protezione dei file WORM in ciascuna modalità:

|                     |                       |                                                                                                                                 |
|---------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Modalità SnapLock   | Livello di protezione | Eliminazione del file WORM durante la conservazione                                                                             |
| Modalità compliance | A livello di file     | Impossibile eliminare                                                                                                           |
| Modalità Enterprise | A livello di disco    | Può essere eliminato dall'amministratore della compliance utilizzando una procedura controllata di "eliminazione con privilegi" |

Una volta trascorso il periodo di conservazione, l'utente è responsabile dell'eliminazione dei file non più necessari. Una volta che un file è stato salvato in WORM, sia in modalità Compliance che Enterprise, non può essere modificato, anche dopo che il periodo di conservazione è scaduto.

Non è possibile spostare un file WORM durante o dopo il periodo di conservazione. È possibile copiare un file WORM, ma la copia non conserverà le sue caratteristiche WORM.

La seguente tabella mostra le differenze nelle funzionalità supportate dalle modalità di conformità SnapLock e Enterprise:

| Funzionalità                                                                      | Conformità SnapLock | Azienda SnapLock                                                  |
|-----------------------------------------------------------------------------------|---------------------|-------------------------------------------------------------------|
| Abilitare ed eliminare i file utilizzando l'opzione di eliminazione con privilegi | No                  | Sì                                                                |
| Reinizializzare i dischi                                                          | No                  | Sì                                                                |
| Distruggere gli aggregati e i volumi SnapLock durante il periodo di conservazione | No                  | Sì, ad eccezione del volume del registro di controllo di SnapLock |
| Rinominare aggregati o volumi                                                     | No                  | Sì                                                                |
| Utilizzare dischi non NetApp                                                      | No                  | Sì (con <a href="#">"Virtualizzazione FlexArray"</a> )            |
| Utilizzare il volume SnapLock per la registrazione dell'audit                     | Sì                  | Sì, a partire da ONTAP 9.5                                        |

## Funzioni supportate e non supportate con SnapLock

La seguente tabella mostra le funzionalità supportate dalla modalità di conformità SnapLock, dalla modalità aziendale SnapLock o da entrambe:

| Funzione                                    | Supportato con conformità SnapLock                                                                    | Supportato con SnapLock Enterprise                                                                     |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Gruppi di coerenza                          | No                                                                                                    | No                                                                                                     |
| Volumi crittografati                        | Sì, a partire da ONTAP 9.2. Scopri di più <a href="#">Encryption e SnapLock</a> .                     | Sì, a partire da ONTAP 9.2. Scopri di più <a href="#">Encryption e SnapLock</a> .                      |
| FabricPools su aggregati SnapLock           | No                                                                                                    | Sì, a partire da ONTAP 9.8. Scopri di più <a href="#">FabricPool su aggregati aziendali SnapLock</a> . |
| Aggregati di Flash Pool                     | Sì, a partire da ONTAP 9.1.                                                                           | Sì, a partire da ONTAP 9.1.                                                                            |
| FlexClone                                   | È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock.                           | È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock.                            |
| Volumi FlexGroup                            | Sì, a partire da ONTAP 9.11.1. Scopri di più <a href="#">[flexgroup]</a> .                            | Sì, a partire da ONTAP 9.11.1. Scopri di più <a href="#">[flexgroup]</a> .                             |
| LUN                                         | No Scopri di più <a href="#">Supporto del LUN Con SnapLock</a> .                                      | No Scopri di più <a href="#">Supporto del LUN Con SnapLock</a> .                                       |
| Configurazioni MetroCluster                 | Sì, a partire da ONTAP 9.3. Scopri di più <a href="#">Supporto MetroCluster</a> .                     | Sì, a partire da ONTAP 9.3. Scopri di più <a href="#">Supporto MetroCluster</a> .                      |
| Verifica multi-admin (MAV)                  | Sì, a partire da ONTAP 9.13.1. Scopri di più <a href="#">Supporto MAV</a> .                           | Sì, a partire da ONTAP 9.13.1. Scopri di più <a href="#">Supporto MAV</a> .                            |
| SAN                                         | No                                                                                                    | No                                                                                                     |
| SnapRestore a file singolo                  | No                                                                                                    | Sì                                                                                                     |
| Continuità aziendale di SnapMirror          | No                                                                                                    | No                                                                                                     |
| SnapRestore                                 | No                                                                                                    | Sì                                                                                                     |
| SMTape                                      | No                                                                                                    | No                                                                                                     |
| SnapMirror sincrono                         | No                                                                                                    | No                                                                                                     |
| SSD                                         | Sì, a partire da ONTAP 9.1.                                                                           | Sì, a partire da ONTAP 9.1.                                                                            |
| Funzionalità per l'efficienza dello storage | Sì, a partire da ONTAP 9.9.1. Scopri di più <a href="#">supporto per l'efficienza dello storage</a> . | Sì, a partire da ONTAP 9.9.1. Scopri di più <a href="#">supporto per l'efficienza dello storage</a> .  |

## FabricPool su aggregati aziendali SnapLock

FabricPool sono supportati negli aggregati aziendali di SnapLock a partire da ONTAP 9.8. Tuttavia, il tuo account team deve aprire una richiesta di variazione del prodotto che documenta che sei consapevole del fatto che i dati FabricPool su più livelli di un cloud pubblico o privato non sono più protetti da SnapLock perché un amministratore del cloud può eliminare tali dati.



Tutti i dati che FabricPool esegue il Tier in un cloud pubblico o privato non sono più protetti da SnapLock perché tali dati possono essere cancellati da un amministratore del cloud.

## Volumi FlexGroup

SnapLock supporta i volumi FlexGroup a partire da ONTAP 9.11.1; tuttavia, le seguenti funzionalità non sono supportate:

- Conservazione a fini giudiziari
- Conservazione basata sugli eventi
- SnapLock per SnapVault (supportato a partire da ONTAP 9.12.1)

È inoltre necessario conoscere i seguenti comportamenti:

- Il clock di compliance del volume (VCC) di un volume FlexGroup è determinato dal VCC del costituente root. Tutti i componenti non root avranno il proprio VCC strettamente sincronizzato con il VCC root.
- Le proprietà di configurazione di SnapLock sono impostate solo su FlexGroup nel suo complesso. I singoli componenti non possono avere proprietà di configurazione diverse, come il tempo di conservazione predefinito e il periodo di autocommit.

## Supporto del LUN

Le LUN sono supportate nei volumi SnapLock solo in scenari in cui le copie Snapshot create su un volume non SnapLock vengono trasferite a un volume SnapLock per la protezione come parte della relazione del vault di SnapLock. I LUN non sono supportati nei volumi SnapLock in lettura/scrittura. Tuttavia, le copie Snapshot a prova di manomissione sono supportate sia sui volumi di origine di SnapMirror che sui volumi di destinazione che contengono LUN.

## Supporto MetroCluster

Il supporto SnapLock nelle configurazioni MetroCluster varia tra la modalità di conformità SnapLock e la modalità aziendale SnapLock.

### Conformità SnapLock

- A partire da ONTAP 9.3, la conformità SnapLock è supportata su aggregati MetroCluster senza mirror.
- A partire da ONTAP 9.3, la conformità SnapLock è supportata sugli aggregati mirrorati, ma solo se l'aggregato viene utilizzato per ospitare i volumi del registro di controllo SnapLock.
- Le configurazioni SnapLock specifiche di SVM possono essere replicate su siti primari e secondari utilizzando MetroCluster.

### Azienda SnapLock

- A partire da ONTAP 9, sono supportati gli aggregati aziendali di SnapLock.
- A partire da ONTAP 9.3, sono supportati gli aggregati aziendali SnapLock con eliminazione con privilegi.

- Le configurazioni SnapLock specifiche di SVM possono essere replicate in entrambi i siti utilizzando MetroCluster.

### Configurazioni MetroCluster e orologi per la compliance

Le configurazioni MetroCluster utilizzano due meccanismi di clock di compliance, il clock di compliance del volume (VCC) e il clock di compliance del sistema (SCC). VCC e SCC sono disponibili per tutte le configurazioni SnapLock. Quando si crea un nuovo volume su un nodo, il relativo VCC viene inizializzato con il valore corrente di SCC su quel nodo. Una volta creato il volume, il tempo di conservazione del volume e del file viene sempre monitorato con il VCC.

Quando un volume viene replicato in un altro sito, viene replicato anche il relativo VCC. Quando si verifica uno switchover del volume, ad esempio dal sito A al sito B, il VCC continua ad essere aggiornato sul sito B mentre il SCC sul sito A si arresta quando il sito A passa alla modalità offline.

Quando il sito A viene riportato in linea e viene eseguito il switchback del volume, il clock SCC del sito A viene riavviato mentre il VCC del volume continua ad essere aggiornato. Poiché il VCC viene costantemente aggiornato, indipendentemente dalle operazioni di switchover e switchback, i tempi di conservazione dei file non dipendono dai clock SCC e non si allungano.

### Supporto MAV (Multi-admin Ververifica)

A partire da ONTAP 9.13.1, un amministratore del cluster può abilitare esplicitamente la verifica multi-admin su un cluster per richiedere l'approvazione del quorum prima che vengano eseguite alcune operazioni SnapLock. Quando MAV è attivato, le proprietà del volume SnapLock come default-retention-time, minimum-retention-time, maximum-retention-time, volume-append-mode, autocommit-period e Privileged-delete richiedono l'approvazione del quorum. Scopri di più ["MAV"](#).

### Efficienza dello storage

A partire da ONTAP 9.9.1, SnapLock supporta funzionalità di efficienza dello storage, come la compattazione dei dati, la deduplica tra volumi e la compressione adattiva per volumi e aggregati SnapLock. Per ulteriori informazioni sull'efficienza dello storage, vedere ["Panoramica sulla gestione dello storage logico con la CLI"](#).

### Crittografia

ONTAP offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

**Disclaimer:** NetApp non può garantire che i file WORM protetti da SnapLock su dischi o volumi con crittografia automatica possano essere recuperati se la chiave di autenticazione viene persa o se il numero di tentativi di autenticazione non riusciti supera il limite specificato e il disco viene bloccato in modo permanente. È responsabilità dell'utente garantire la protezione dagli errori di autenticazione.



A partire da ONTAP 9.2, i volumi crittografati sono supportati negli aggregati SnapLock.

### Transizione 7-Mode

È possibile migrare i volumi SnapLock da 7-Mode a ONTAP utilizzando la funzione CBT (Copy-Based Transition) dello strumento di transizione 7-Mode. La modalità SnapLock del volume di destinazione, Compliance o Enterprise, deve corrispondere alla modalità SnapLock del volume di origine. Non è possibile utilizzare la transizione senza copia (CFT) per migrare i volumi SnapLock.

# Configurare SnapLock

## Configurare SnapLock

Prima di utilizzare SnapLock, è necessario configurare SnapLock completando varie attività, ad esempio ["Installare la licenza SnapLock"](#) Per ogni nodo che ospita un aggregato con un volume SnapLock, inizializzare l' ["Orologio di conformità"](#), Creare un aggregato SnapLock per i cluster che eseguono release ONTAP precedenti a ONTAP 9.10.1, ["Creare e montare un volume SnapLock"](#) e molto altro ancora.

## Inizializzare il Compliance Clock

SnapLock utilizza *Volume Compliance Clock* per evitare manomissioni che potrebbero alterare il periodo di conservazione dei file WORM. È necessario prima inizializzare il *system ComplianceClock* su ogni nodo che ospita un aggregato SnapLock.

A partire da ONTAP 9.14.1, è possibile inizializzare o reinizializzare il clock di conformità del sistema quando non ci sono volumi SnapLock o nessun volume con il blocco delle copie Snapshot attivato. La possibilità di reinizializzare consente agli amministratori di sistema di reimpostare l'orologio di conformità del sistema nei casi in cui potrebbe essere stato inizializzato in modo errato o di correggere la deriva dell'orologio sul sistema. In ONTAP 9.13.1 e nelle versioni precedenti, una volta inizializzato il Compliance Clock su un nodo, non è possibile inizializzarlo nuovamente.

### Prima di iniziare

Per reinizializzare il Compliance Clock:

- Tutti i nodi nel cluster devono essere in stato integro.
- Tutti i volumi devono essere online.
- La coda di ripristino non può contenere volumi.
- Non può essere presente alcun volume SnapLock.
- Non può essere presente alcun volume con il blocco della copia Snapshot abilitato.

Requisiti generali per l'inizializzazione dell'orologio di conformità:

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- ["La licenza SnapLock deve essere installata sul nodo"](#).

### A proposito di questa attività

L'ora del Compliance Clock del sistema viene ereditata dal *Volume Compliance Clock*, quest'ultimo dei quali controlla il periodo di conservazione dei file WORM sul volume. Il clock di conformità del volume viene inizializzato automaticamente quando si crea un nuovo volume SnapLock.



L'impostazione iniziale dell'orologio di conformità del sistema si basa sull'orologio di sistema hardware corrente. Per questo motivo, è necessario verificare che l'ora e il fuso orario del sistema siano corretti prima di inizializzare l'orologio di conformità del sistema su ciascun nodo. Una volta inizializzato il clock di conformità del sistema su un nodo, non è possibile inizializzarlo nuovamente quando sono presenti volumi SnapLock o volumi con blocco abilitato.

## Fasi

È possibile utilizzare la CLI di ONTAP per inizializzare l'orologio di conformità oppure, a partire da ONTAP 9.12.1, utilizzare Gestione sistema per inizializzare l'orologio di conformità.

### System Manager

1. Accedere a **Cluster > Panoramica**.
2. Nella sezione **nodi**, fare clic su **Inizializza clock di conformità SnapLock**.
3. Per visualizzare la colonna **Orologio conformità** e verificare che l'Orologio conformità sia inizializzato, nella sezione **Cluster > Panoramica > nodi**, fare clic su **Mostra/Nascondi** e selezionare **Orologio conformità SnapLock**.

### CLI

1. Inizializzare l'orologio di conformità del sistema:

```
snaplock compliance-clock initialize -node node_name
```

Il seguente comando inizializza il Compliance Clock del sistema su node1:

```
cluster1::> snaplock compliance-clock initialize -node node1
```

2. Quando richiesto, confermare che l'orologio di sistema è corretto e che si desidera inizializzare l'orologio di conformità:

```
Warning: You are about to initialize the secure ComplianceClock of
the node "node1" to the current value of the node's system clock.
This procedure can be performed only once on a given node, so you
should ensure that the system time is set correctly before
proceeding.
```

```
The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016
```

```
Do you want to continue? (y|n): y
```

3. Ripetere questa procedura per ogni nodo che ospita un aggregato SnapLock.

### Abilitare la risincronizzazione del clock di conformità per un sistema configurato con NTP

È possibile attivare la funzione di sincronizzazione dell'ora dell'orologio di conformità SnapLock quando è configurato un server NTP.

### Di cosa hai bisogno

- Questa funzione è disponibile solo al livello di privilegio avanzato.
- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- ["La licenza SnapLock deve essere installata sul nodo"](#).
- Questa funzione è disponibile solo per le piattaforme Cloud Volumes ONTAP, ONTAP Select e VSIM.



## A proposito di questa attività

Quando il daemon di clock sicuro SnapLock rileva un'inclinazione oltre la soglia, ONTAP utilizza l'ora di sistema per reimpostare sia il sistema che i blocchi di conformità del volume. Come soglia di disallineamento viene impostato un periodo di 24 ore. Ciò significa che l'orologio di conformità del sistema è sincronizzato con l'orologio di sistema solo se l'inclinazione è più vecchia di un giorno.

Il daemon dell'orologio sicuro SnapLock rileva un'inclinazione e modifica l'orologio di conformità all'ora del sistema. Qualsiasi tentativo di modifica dell'ora di sistema per forzare la sincronizzazione dell'orologio di conformità con l'ora di sistema non riesce, poiché l'orologio di conformità si sincronizza con l'ora di sistema solo se l'ora di sistema è sincronizzata con l'ora NTP.

## Fasi

1. Attivare la funzione sincronizzazione orologio conformità SnapLock quando è configurato un server NTP:

```
snaplock compliance-clock ntp
```

Il seguente comando abilita la funzione di sincronizzazione dell'ora dell'orologio di conformità del sistema:

```
cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
```

2. Quando richiesto, verificare che i server NTP configurati siano attendibili e che il canale di comunicazione sia sicuro per abilitare la funzione:
3. Verificare che la funzione sia attivata:

```
snaplock compliance-clock ntp show
```

Il seguente comando verifica che la funzione di sincronizzazione dell'ora del clock di conformità del sistema sia attivata:

```
cluster1::*> snaplock compliance-clock ntp show  
  
Enable clock sync to NTP system time: true
```

## Creare un aggregato SnapLock

Il volume viene utilizzato `-snaplock-type` Opzione per specificare un tipo di volume Compliance o Enterprise SnapLock. Per le release precedenti a ONTAP 9.10.1, è necessario creare un aggregato SnapLock separato. A partire da ONTAP 9.10.1, i volumi SnapLock e non SnapLock possono esistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1.

## Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Il SnapLock ["la licenza deve essere installata"](#) sul nodo. Questa licenza è inclusa in ["ONTAP uno"](#).
- ["È necessario inizializzare il Compliance Clock sul nodo"](#).
- Se i dischi sono stati partizionati come "root", "data1" e "data2", è necessario assicurarsi che siano

disponibili dischi di riserva.

### Considerazioni sull'upgrade

Quando si esegue l'aggiornamento a ONTAP 9.10.1, gli aggregati SnapLock e non SnapLock esistenti vengono aggiornati per supportare l'esistenza di volumi SnapLock e non SnapLock; tuttavia, gli attributi dei volumi SnapLock esistenti non vengono aggiornati automaticamente. Ad esempio, i campi di compaction dei dati, deduplica di volumi incrociati e deduplica di background di volumi incrociati rimangono invariati. I nuovi volumi SnapLock creati sugli aggregati esistenti hanno gli stessi valori predefiniti dei volumi non SnapLock e i valori predefiniti per i nuovi volumi e aggregati dipendono dalla piattaforma.

### Considerazioni sul revert

Se è necessario ripristinare una versione di ONTAP precedente alla 9.10.1, è necessario spostare tutti i volumi SnapLock Compliance, SnapLock Enterprise e SnapLock nei propri aggregati SnapLock.

### A proposito di questa attività

- Non è possibile creare aggregati di conformità per le LUN FlexArray, ma gli aggregati di conformità SnapLock sono supportati con le LUN FlexArray.
- Non è possibile creare aggregati di conformità con l'opzione SyncMirror.
- È possibile creare aggregati di conformità mirrorati in una configurazione MetroCluster solo se l'aggregato viene utilizzato per ospitare volumi di log di audit SnapLock.



In una configurazione MetroCluster, SnapLock Enterprise è supportato su aggregati mirrorati e senza mirror. La conformità SnapLock è supportata solo su aggregati senza mirror.

### Fasi

1. Creare un aggregato SnapLock:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>  
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

La pagina man del comando contiene un elenco completo di opzioni.

Il seguente comando crea un SnapLock Compliance aggregato con nome `aggr1` con tre dischi su `node1`:

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1  
-diskcount 3 -snaplock-type compliance
```

### Creare e montare volumi SnapLock

È necessario creare un volume SnapLock per i file o le copie Snapshot che si desidera assegnare allo stato WORM. A partire da ONTAP 9.10.1, qualsiasi volume creato, indipendentemente dal tipo di aggregato, viene creato per impostazione predefinita come volume non SnapLock. È necessario utilizzare `-snaplock-type` Opzione per creare esplicitamente un volume SnapLock specificando Compliance o Enterprise come tipo SnapLock. Per impostazione predefinita, il tipo di SnapLock è impostato su `non-`

snaplock.

### Prima di iniziare

- L'aggregato SnapLock deve essere online.
- Dovresti ["Verificare che sia installata una licenza SnapLock"](#). Se una licenza SnapLock non è installata sul nodo, è necessario ["installare"](#) it. Questa licenza è inclusa con ["ONTAP uno"](#). Prima di ONTAP One, la licenza SnapLock era inclusa nel pacchetto sicurezza e conformità. Il bundle Security and Compliance non è più offerto, ma è ancora valido. Sebbene non sia attualmente richiesto, i clienti esistenti possono scegliere di farlo ["Eseguire l'aggiornamento a ONTAP One"](#).
- ["È necessario inizializzare il Compliance Clock sul nodo"](#).

### A proposito di questa attività

Con le autorizzazioni SnapLock appropriate, è possibile distruggere o rinominare un volume Enterprise in qualsiasi momento. Non è possibile distruggere un volume Compliance fino allo scadere del periodo di conservazione. Non è mai possibile rinominare un volume Compliance.

È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock. Il volume clone sarà dello stesso tipo di SnapLock del volume padre.



I LUN non sono supportati nei volumi SnapLock. Le LUN sono supportate nei volumi SnapLock solo in scenari in cui le copie Snapshot create su un volume non SnapLock vengono trasferite a un volume SnapLock per la protezione come parte della relazione del vault di SnapLock. I LUN non sono supportati nei volumi SnapLock in lettura/scrittura. Tuttavia, le copie Snapshot a prova di manomissione sono supportate sia sui volumi di origine di SnapMirror che sui volumi di destinazione che contengono LUN.

Eseguire questa attività utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

## System Manager

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione sistema per creare un volume SnapLock.

### Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi) e fare clic su **Add** (Aggiungi).
2. Nella finestra **Add Volume** (Aggiungi volume), fare clic su **More Options** (altre opzioni).
3. Inserire le informazioni sul nuovo volume, inclusi il nome e le dimensioni del volume.
4. Selezionare **Enable SnapLock** (attiva conformità) e scegliere il tipo di SnapLock, Compliance (conformità) o Enterprise (Azienda).
5. Nella sezione **Auto-commit Files**, selezionare **Modified** e inserire il tempo in cui un file deve rimanere invariato prima che venga automaticamente salvato. Il valore minimo è di 5 minuti e il valore massimo è di 10 anni.
6. Nella sezione **conservazione dei dati**, selezionare il periodo di conservazione minimo e massimo.
7. Selezionare il periodo di conservazione predefinito.
8. Fare clic su **Save** (Salva).
9. Selezionare il nuovo volume nella pagina **Volumes** per verificare le impostazioni SnapLock.

### CLI

1. Creare un volume SnapLock:

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate  
<aggregate_name> -snaplock-type <compliance|enterprise>
```

Per un elenco completo delle opzioni, vedere la pagina man del comando. Le seguenti opzioni non sono disponibili per i volumi SnapLock: `-nvfail`, `-atime-update`, `-is-autobalance-eligible`, `-space-mgmt-try-first`, e `vmailn`.

Il seguente comando crea un SnapLock Compliance volume denominato `vol1` acceso `aggr1` acceso `vs1`:

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1  
-snaplock-type compliance
```

## Montare un volume SnapLock

È possibile montare un volume SnapLock su un percorso di giunzione nello spazio dei nomi SVM per l'accesso al client NAS.

### Di cosa hai bisogno

Il volume SnapLock deve essere online.

### A proposito di questa attività

- È possibile montare un volume SnapLock solo sotto la directory principale della SVM.

- Non è possibile montare un volume normale sotto un volume SnapLock.

## Fasi

1. Montare un volume SnapLock:

```
volume mount -vserver SVM_name -volume volume_name -junction-path path
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando consente di montare un volume SnapLock denominato `vol1` al percorso di giunzione `/sales` in `vs1` spazio dei nomi:

```
cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
```

## Impostare il tempo di conservazione

È possibile impostare il tempo di conservazione per un file in modo esplicito oppure utilizzare il periodo di conservazione predefinito per il volume per derivare il tempo di conservazione. A meno che non si definisca esplicitamente il tempo di conservazione, SnapLock utilizza il periodo di conservazione predefinito per calcolare il tempo di conservazione. È inoltre possibile impostare la conservazione dei file dopo un evento.

### Informazioni sul periodo di conservazione e sul tempo di conservazione

Il *periodo di conservazione* per un file WORM specifica il periodo di tempo in cui il file deve essere conservato dopo il commit allo stato WORM. Il *tempo di conservazione* per un file WORM è il tempo dopo il quale il file non deve più essere conservato. Un periodo di conservazione di 20 anni per un file impegnato nello stato WORM il 10 novembre 2020 alle 6:00, ad esempio, avrebbe un tempo di conservazione del 10 novembre 2040 alle 6:00.



A partire da ONTAP 9.10.1, è possibile impostare un periodo di conservazione fino al 26 ottobre 3058 e un periodo di conservazione fino a 100 anni. Quando estendi le date di conservazione, le policy precedenti vengono convertite automaticamente. In ONTAP 9.9.1 e versioni precedenti, a meno che il periodo di conservazione predefinito non sia impostato su infinito, il tempo di conservazione massimo supportato è gennaio 19 2071 (GMT).

### Considerazioni importanti sulla replica

Quando si stabilisce una relazione di SnapMirror con un volume di origine SnapLock utilizzando una data di conservazione successiva al 19 gennaio 2071 (GMT), il cluster di destinazione deve eseguire ONTAP 9.10.1 o versione successiva, altrimenti il trasferimento di SnapMirror avrà esito negativo.

### Considerazioni importanti sul revert

ONTAP impedisce di ripristinare un cluster da ONTAP 9.10.1 a una versione precedente di ONTAP quando sono presenti file con un periodo di conservazione successivo a "19 gennaio 2071 8:44:07".

## Comprensione dei periodi di conservazione

Un volume aziendale o di conformità SnapLock prevede quattro periodi di conservazione:

- Periodo minimo di conservazione ( $\min$ ), con un valore predefinito pari a 0
- Periodo di conservazione massimo ( $\max$ ), con un valore predefinito di 30 anni
- Periodo di conservazione predefinito, con un valore predefinito pari a  $\min$ . Sia per la modalità Compliance che per la modalità Enterprise a partire da ONTAP 9.10.1. Nelle versioni di ONTAP precedenti a ONTAP 9.10.1, il periodo di conservazione predefinito dipende dalla modalità:
  - Per la modalità Compliance, l'impostazione predefinita è uguale a  $\max$ .
  - Per la modalità Enterprise, il valore predefinito è uguale a  $\min$ .
- Periodo di conservazione non specificato.

A partire da ONTAP 9.8, è possibile impostare il periodo di conservazione dei file in un volume su `unspecified`, per consentire la conservazione del file fino a quando non si imposta un tempo di conservazione assoluto. È possibile impostare un file con tempo di conservazione assoluto su conservazione non specificata e su conservazione assoluta, a condizione che il nuovo tempo di conservazione assoluto sia successivo al tempo assoluto impostato in precedenza.

A partire da ONTAP 9.12.1, i file WORM con il periodo di conservazione impostato su `unspecified`. È garantito che un periodo di conservazione sia impostato sul periodo di conservazione minimo configurato per il volume SnapLock. Quando si modifica il periodo di conservazione del file da `unspecified` per un tempo di conservazione assoluto, il nuovo tempo di conservazione specificato deve essere maggiore del tempo di conservazione minimo già impostato nel file.

Pertanto, se non si imposta esplicitamente il tempo di conservazione prima di impostare un file in modalità Compliance allo stato WORM e non si modificano le impostazioni predefinite, il file verrà conservato per 30 anni. Allo stesso modo, se non si imposta esplicitamente il tempo di conservazione prima di eseguire il commit di un file in modalità Enterprise allo stato WORM e non si modificano le impostazioni predefinite, il file verrà conservato per 0 anni o, effettivamente, per niente.

### Impostare il periodo di conservazione predefinito

È possibile utilizzare `volume snaplock modify` Per impostare il periodo di conservazione predefinito per i file su un volume SnapLock.

### Di cosa hai bisogno

Il volume SnapLock deve essere online.

### A proposito di questa attività

La tabella seguente mostra i valori possibili per l'opzione periodo di conservazione predefinito:



Il periodo di conservazione predefinito deve essere maggiore o uguale al ( $\geq$ ) periodo di conservazione minimo e minore o uguale al ( $\leq$ ) periodo di conservazione massimo.

| Valore    | Unità   | Note |
|-----------|---------|------|
| 0 - 65535 | secondi |      |

| Valore          | Unità  | Note                                                                                      |
|-----------------|--------|-------------------------------------------------------------------------------------------|
| 0 - 24          | ore    |                                                                                           |
| 0 - 365         | giorni |                                                                                           |
| 0 - 12          | mesi   |                                                                                           |
| 0 - 100         | anni   | A partire da ONTAP 9.10.1. Per le release precedenti di ONTAP, il valore è 0 - 70.        |
| max             | -      | Utilizzare il periodo di conservazione massimo.                                           |
| min             | -      | Utilizzare il periodo di conservazione minimo.                                            |
| infinito        | -      | Conserva i file per sempre.                                                               |
| non specificato | -      | Conservare i file fino a quando non viene impostato un periodo di conservazione assoluto. |

I valori e gli intervalli dei periodi di conservazione massimo e minimo sono identici, ad eccezione di `max` e `min`, che non sono applicabili. Per ulteriori informazioni su questa attività, vedere ["Imposta la panoramica del tempo di conservazione"](#).

È possibile utilizzare `volume snaplock show` per visualizzare le impostazioni del periodo di conservazione per il volume. Per ulteriori informazioni, vedere la pagina man del comando.



Una volta che un file è stato impegnato nello stato WORM, è possibile estendere ma non ridurre il periodo di conservazione.

## Fasi

1. Impostare il periodo di conservazione predefinito per i file su un volume SnapLock:

```
volume snaplock modify -vserver SVM_name -volume volume_name -default  
-retention-period default_retention_period -minimum-retention-period  
min_retention_period -maximum-retention-period max_retention_period
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.



Gli esempi seguenti presuppongono che i periodi di conservazione minimo e massimo non siano stati modificati in precedenza.

Il comando seguente imposta il periodo di conservazione predefinito per un volume Compliance o Enterprise su 20 giorni:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period 20days
```

Il seguente comando imposta il periodo di conservazione predefinito per un volume Compliance su 70 anni:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum  
-retention-period 70years
```

Il seguente comando imposta il periodo di conservazione predefinito per un volume Enterprise su 10 anni:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period max -maximum-retention-period 10years
```

I seguenti comandi impostano il periodo di conservazione predefinito per un volume Enterprise su 10 giorni:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum  
-retention-period 10days  
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period min
```

Il comando seguente imposta il periodo di conservazione predefinito per un volume Compliance su infinito:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default  
-retention-period infinite -maximum-retention-period infinite
```

### Impostare il tempo di conservazione per un file in modo esplicito

È possibile impostare il tempo di conservazione di un file in modo esplicito modificando l'ultimo tempo di accesso. È possibile utilizzare qualsiasi comando o programma adatto su NFS o CIFS per modificare l'ultimo tempo di accesso.

#### A proposito di questa attività

Dopo che un file è stato eseguito il commit su WORM, è possibile estendere ma non ridurre il tempo di conservazione. Il tempo di conservazione viene memorizzato in `atime` per il file.



Non è possibile impostare esplicitamente il tempo di conservazione di un file su `infinite`. Tale valore è disponibile solo quando si utilizza il periodo di conservazione predefinito per calcolare il tempo di conservazione.

### Fasi

1. Utilizzare un comando o un programma adatto per modificare l'ultimo orario di accesso al file di cui si



desidera impostare il tempo di conservazione.

In una shell UNIX, utilizzare il seguente comando per impostare un tempo di conservazione del 21 novembre 2020 alle 6:00 su un file denominato `document.txt`:

```
touch -a -t 202011210600 document.txt
```



È possibile utilizzare qualsiasi comando o programma adatto per modificare l'ultimo orario di accesso in Windows.

### Impostare il periodo di conservazione del file dopo un evento

A partire da ONTAP 9.3, è possibile definire per quanto tempo un file viene conservato dopo un evento utilizzando la funzione di conservazione basata su eventi (EBR)\_ di SnapLock.

#### Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore di SnapLock.

["Creare un account amministratore di SnapLock"](#)

- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

#### A proposito di questa attività

Il *criterio di conservazione degli eventi* definisce il periodo di conservazione del file dopo il verificarsi dell'evento. Il criterio può essere applicato a un singolo file o a tutti i file di una directory.

- Se un file non è UN file WORM, viene impegnato nello stato WORM per il periodo di conservazione definito nella policy.
- Se un file è UN file WORM o un file WORM appendibile, il suo periodo di conservazione verrà esteso dal periodo di conservazione definito nella policy.

È possibile utilizzare un volume Compliance-mode o Enterprise-mode.



I criteri EBR non possono essere applicati ai file in stato di conservazione a scopo legale.

Per informazioni sull'utilizzo avanzato, vedere ["Storage WORM conforme con NetApp SnapLock"](#).

#### **utilizzo di EBR per estendere il periodo di conservazione dei file WORM già esistenti**

EBR è utile quando si desidera estendere il periodo di conservazione dei file WORM già esistenti. Ad esempio, la politica della tua azienda potrebbe essere quella di conservare i record W-4 del dipendente in forma non modificata per tre anni dopo che il dipendente ha modificato un'elezione di ritenuta. Un'altra policy aziendale potrebbe richiedere la conservazione dei record W-4 per cinque anni dopo la cessazione del dipendente.

In questa situazione, è possibile creare una policy EBR con un periodo di conservazione di cinque anni. Una volta terminato il dipendente (il "evento"), applicherai la policy EBR al record W-4 del dipendente, prolungandone il periodo di conservazione. In genere, questo sarà più semplice dell'estensione manuale del periodo di conservazione, in particolare quando si tratta di un numero elevato di file.

## Fasi

1. Creare un criterio EBR:

```
snaplock event-retention policy create -vserver SVM_name -name policy_name  
-retention-period retention_period
```

Il seguente comando crea il criterio EBR `employee_exit` acceso `vs1` con un periodo di conservazione di dieci anni:

```
cluster1::>snaplock event-retention policy create -vserver vs1 -name  
employee_exit -retention-period 10years
```

2. Applicare un criterio EBR:

```
snaplock event-retention apply -vserver SVM_name -name policy_name -volume  
volume_name -path path_name
```

Il seguente comando applica il criterio EBR `employee_exit` acceso `vs1` a tutti i file nella directory `d1`:

```
cluster1::>snaplock event-retention apply -vserver vs1 -name  
employee_exit -volume vol1 -path /d1
```

## Creare un registro di controllo

Se utilizzi ONTAP 9.9.1 o versioni precedenti, devi prima creare un aggregato SnapLock e quindi un audit log protetto da SnapLock prima di eseguire un'eliminazione con privilegi o lo spostamento di un volume SnapLock. Il registro di controllo registra la creazione e l'eliminazione degli account amministratore di SnapLock, le modifiche al volume di log, l'eventuale attivazione dell'eliminazione con privilegi, le operazioni di eliminazione con privilegi e le operazioni di spostamento del volume SnapLock.

A partire da ONTAP 9.10.1, non sarà più possibile creare un aggregato SnapLock. Devi utilizzare l'opzione `-snaplock-type` per ["Creare esplicitamente un volume SnapLock"](#) Specificando conformità o impresa come tipo di SnapLock.

### Prima di iniziare

Se utilizzi ONTAP 9.9.1 o versioni precedenti, per creare un aggregato SnapLock devi essere un amministratore del cluster.

### A proposito di questa attività

Non è possibile eliminare un registro di controllo fino a quando non è trascorso il periodo di conservazione del file di registro. Non è possibile modificare un registro di controllo anche dopo che è trascorso il periodo di conservazione. Ciò vale sia per la conformità SnapLock che per le modalità aziendali.



In ONTAP 9.4 e versioni precedenti, non è possibile utilizzare un volume aziendale SnapLock per la registrazione dell'audit. È necessario utilizzare un volume di conformità SnapLock. In ONTAP 9.5 e versioni successive, è possibile utilizzare un volume aziendale SnapLock o un volume di conformità SnapLock per la registrazione dell'audit. In tutti i casi, il volume del log di audit deve essere montato sul percorso di giunzione `/snaplock_audit_log`. Nessun altro volume può utilizzare questo percorso di giunzione.

I registri di controllo di SnapLock sono disponibili in `/snaplock_log` directory sotto la directory principale del volume del registro di controllo, in sottodirectory denominate `privdel_log` (operazioni di eliminazione con privilegi) e `system_log` (tutto il resto). I nomi dei file di log di audit contengono l'indicazione dell'ora della prima operazione registrata, semplificando la ricerca dei record in base all'ora approssimativa in cui sono state eseguite le operazioni.

- È possibile utilizzare `snaplock log file show` per visualizzare i file di log sul volume del registro di controllo.
- È possibile utilizzare `snaplock log file archive` comando per archiviare il file di log corrente e crearne uno nuovo, utile nei casi in cui è necessario registrare le informazioni del log di audit in un file separato.

Per ulteriori informazioni, consulta le pagine man dei comandi.



Un volume di protezione dei dati non può essere utilizzato come volume del registro di controllo di SnapLock.

## Fasi

1. Creare un aggregato SnapLock.

[Creare un aggregato SnapLock](#)

2. Sulla SVM che si desidera configurare per la registrazione dell'audit, creare un volume SnapLock.

[Creare un volume SnapLock](#)

3. Configurare la SVM per la registrazione dell'audit:

```
snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log  
-size size -retention-period default_retention_period
```



Il periodo minimo di conservazione predefinito per i file di log di controllo è di sei mesi. Se il periodo di conservazione di un file interessato supera il periodo di conservazione del log di controllo, il periodo di conservazione del log eredita il periodo di conservazione del file. Pertanto, se il periodo di conservazione di un file cancellato mediante eliminazione con privilegi è di 10 mesi e il periodo di conservazione del registro di controllo è di 8 mesi, il periodo di conservazione del registro viene esteso a 10 mesi. Per ulteriori informazioni sul tempo di conservazione e sul periodo di conservazione predefinito, vedere ["Impostare il tempo di conservazione"](#).

Il seguente comando viene configurato `SVM1` Per la registrazione dell'audit utilizzando il volume SnapLock `logVol1`. Il registro di controllo ha una dimensione massima di 20 GB e viene conservato per otto mesi.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

4. Sulla SVM configurata per la registrazione dell'audit, montare il volume SnapLock nel percorso di giunzione /snaplock\_audit\_log.

### Montare un volume SnapLock

## Verificare le impostazioni SnapLock

È possibile utilizzare `volume file fingerprint start` e `volume file fingerprint dump` Comandi per visualizzare informazioni chiave su file e volumi, tra cui il tipo di file (normale, WORM o appendice WORM), la data di scadenza del volume e così via.

### Fasi

1. Generare un'impronta digitale del file:

```
volume file fingerprint start -vserver SVM_name -file file_path
```

```
svml1::> volume file fingerprint start -vserver svml -file
/vol/slc/vol/f1
File fingerprint operation is queued. Run "volume file fingerprint show
-session-id 16842791" to view the fingerprint session status.
```

Il comando genera un ID sessione che è possibile utilizzare come input per `volume file fingerprint dump` comando.



È possibile utilizzare `volume file fingerprint show` Comando con l'ID di sessione per monitorare l'avanzamento dell'operazione di impronte digitali. Assicurarsi che l'operazione sia stata completata prima di provare a visualizzare l'impronta digitale.

2. Visualizzare l'impronta digitale per il file:

```
volume file fingerprint dump -session-id session_ID
```

```
svml1::> volume file fingerprint dump -session-id 33619976
Vserver:svml
Session-ID:33619976
Volume:slc_vol
Path:/vol/slc_vol/f1
Data
Fingerprint:MOFJVEvxNSJm3C/4Bn5oEEYH5lCrudOzZYK4r5Cfy1g=Metadata
Fingerprint:8iMjqJXiNcqqXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
```

Algorithm:SHA256

Fingerprint Scope:data-and-metadata  
Fingerprint Start Time:1460612586  
Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016  
Fingerprint Version:3  
\*\*SnapLock License:available\*\*  
Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae  
Volume MSID:2152884007  
Volume DSID:1028  
Hostname:my\_host  
Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d  
Volume Containing Aggregate:slc\_aggr1  
Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67  
\*\*SnapLock System ComplianceClock:1460610635  
Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35

GMT 2016

Volume SnapLock Type:compliance  
Volume ComplianceClock:1460610635  
Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016  
Volume Expiry Date:1465880998\*\*  
Is Volume Expiry Date Wraparound:false  
Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016  
Filesystem ID:1028  
File ID:96  
File Type:worm  
File Size:1048576  
Creation Time:1460612515  
Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016  
Modification Time:1460612515  
Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016  
Changed Time:1460610598  
Is Changed Time Wraparound:false  
Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016  
Retention Time:1465880998  
Is Retention Time Wraparound:false  
Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016  
Access Time:-  
Formatted Access Time:-  
Owner ID:0  
Group ID:0  
Owner SID:-  
Fingerprint End Time:1460612586  
Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016

## Gestire i file WORM

### Gestire i file WORM

È possibile gestire i file WORM nei seguenti modi:

- "Esegui il commit dei file su WORM"
- "Assegnare le copie Snapshot a WORM su una destinazione del vault"
- "Mirroring dei file WORM per il disaster recovery"
- "Conservare i file WORM durante i contenziosi"
- "Eliminare i file WORM"

### Esegui il commit dei file su WORM

È possibile eseguire il commit dei file in WORM (write once, Read many) manualmente o automaticamente. È inoltre possibile creare file .WORM appendibili.

#### Esegui il commit dei file in WORM manualmente

Il commit di un file in WORM viene eseguito manualmente rendendo il file di sola lettura. È possibile utilizzare qualsiasi comando o programma adatto su NFS o CIFS per modificare l'attributo Read-write di un file in sola lettura. È possibile scegliere di eseguire il commit manuale dei file se si desidera garantire che un'applicazione abbia terminato la scrittura su un file in modo che il commit del file non venga eseguito in modo prematuro o che si siano riscontrati problemi di scalabilità per lo scanner di autocommit a causa di un elevato numero di volumi.

#### Di cosa hai bisogno

- Il file che si desidera assegnare deve risiedere in un volume SnapLock.
- Il file deve essere scrivibile.

#### A proposito di questa attività

Il volume ComplianceClock Time viene scritto su `ctime` del file quando viene eseguito il comando o il programma. Il tempo di ComplianceClock determina quando è stato raggiunto il tempo di conservazione del file.

#### Fasi

1. Utilizzare un comando o un programma adatto per modificare l'attributo Read-write di un file in sola lettura.

In una shell UNIX, utilizzare il seguente comando per creare un file denominato `document.txt` sola lettura:

```
chmod -w document.txt
```

In una shell Windows, utilizzare il seguente comando per creare un file denominato `document.txt` sola lettura:

```
attrib +r document.txt
```

## Esegui il commit dei file automaticamente SU WORM

La funzione di autocommit di SnapLock consente di assegnare automaticamente i file A WORM. La funzionalità di autocommit commit commette un file allo stato WORM su un volume SnapLock se il file non è stato modificato per la durata del periodo di autocommit. La funzione di invio automatico è disattivata per impostazione predefinita.

### Di cosa hai bisogno

- I file che si desidera assegnare automaticamente devono risiedere in un volume SnapLock.
- Il volume SnapLock deve essere online.
- Il volume SnapLock deve essere un volume di lettura/scrittura.



La funzione di autocommit di SnapLock esegue la scansione di tutti i file nel volume e commit un file se soddisfa i requisiti di autocommit. Potrebbe esserci un intervallo di tempo tra il momento in cui il file è pronto per l'autocommit e il momento in cui viene effettivamente salvato dallo scanner di autocommit SnapLock. Tuttavia, il file è ancora protetto dalle modifiche e dall'eliminazione da parte del file system non appena è idoneo per l'autocommit.

### A proposito di questa attività

Il *periodo di autocommit* specifica il periodo di tempo in cui i file devono rimanere invariati prima di eseguire l'autocommit. La modifica di un file prima che sia trascorso il periodo di autocommit riavvia il periodo di autocommit per il file.

La seguente tabella mostra i valori possibili per il periodo di autocommit:

| Valore      | Unità  | Note                        |
|-------------|--------|-----------------------------|
| nessuno     | -      | L'impostazione predefinita. |
| 5 - 5256000 | minuti | -                           |
| 1 - 87600   | ore    | -                           |
| 1 - 3650    | giorni | -                           |
| 1 - 120     | mesi   | -                           |
| 1 - 10      | anni   | -                           |



Il valore minimo è di 5 minuti e il valore massimo è di 10 anni.

### Fasi

1. Commit automatico dei file su un volume SnapLock in WORM:

```
volume snaplock modify -vserver SVM_name -volume volume_name -autocommit  
-period autocommit_period
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando esegue il commit automatico dei file sul volume `vol1` Di SVM `vs1`, a condizione che i file rimangano invariati per 5 ore:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit  
-period 5hours
```

### Creare un file .WORM appendibile

Un file WORM appendibile conserva i dati scritti in modo incrementale, come le voci di registro. È possibile utilizzare qualsiasi comando o programma adatto per creare un file .WORM appendibile oppure utilizzare la funzione *volume append mode* di SnapLock per creare file .WORM appendibili per impostazione predefinita.

### Utilizzare un comando o un programma per creare un file .WORM appendibile

È possibile utilizzare qualsiasi comando o programma adatto su NFS o CIFS per creare un file .WORM appendibile. Un file WORM appendibile conserva i dati scritti in modo incrementale, come le voci di registro. I dati vengono aggiunti al file in blocchi da 256 KB. Man mano che ogni chunk viene scritto, il chunk precedente diventa protetto DA WORM. Non è possibile eliminare il file finché non è trascorso il periodo di conservazione.

### Di cosa hai bisogno

Il file .WORM appendibile deve risiedere su un volume SnapLock.

### A proposito di questa attività

I dati non devono essere scritti in sequenza nel blocco attivo da 256 KB. Quando i dati vengono scritti nel byte  $n \times 256KB + 1$  del file, il segmento precedente da 256 KB diventa protetto DA WORM.

### Fasi

1. Utilizzare un comando o un programma adatto per creare un file di lunghezza zero con il tempo di conservazione desiderato.

In una shell UNIX, utilizzare il seguente comando per impostare un tempo di conservazione del 21 novembre 2020 alle 6:00 su un file di lunghezza zero denominato `document.txt`:

```
touch -a -t 202011210600 document.txt
```

2. Utilizzare un comando o un programma adatto per modificare l'attributo Read-write del file in sola lettura.

In una shell UNIX, utilizzare il seguente comando per creare un file denominato `document.txt` sola lettura:

```
chmod 444 document.txt
```

3. Utilizzare un comando o un programma adatto per modificare nuovamente l'attributo Read-write del file in Writable (scrivibile).



Questo passaggio non è considerato un rischio di conformità perché non sono presenti dati nel file.



In una shell UNIX, utilizzare il seguente comando per creare un file denominato `document.txt` scrivibile:

```
chmod 777 document.txt
```

4. Utilizzare un comando o un programma adatto per iniziare a scrivere i dati nel file.

In una shell UNIX, utilizzare il seguente comando per scrivere i dati `document.txt`:

```
echo test data >> document.txt
```



Quando non è più necessario aggiungere dati al file, riportare i permessi del file in sola lettura.

#### Utilizzare la modalità di aggiunta del volume per creare file .WORM appendibili

A partire da ONTAP 9.3, è possibile utilizzare la funzione SnapLock *volume append mode* (VAM) per creare file .WORM appendibili per impostazione predefinita. Un file WORM appendibile conserva i dati scritti in modo incrementale, come le voci di registro. I dati vengono aggiunti al file in blocchi da 256 KB. Man mano che ogni chunk viene scritto, il chunk precedente diventa protetto DA WORM. Non è possibile eliminare il file finché non è trascorso il periodo di conservazione.

#### Di cosa hai bisogno

- Il file .WORM appendibile deve risiedere su un volume SnapLock.
- Il volume SnapLock deve essere smontato e vuoto di copie Snapshot e file creati dall'utente.

#### A proposito di questa attività

I dati non devono essere scritti in sequenza nel blocco attivo da 256 KB. Quando i dati vengono scritti nel byte  $n \times 256KB + 1$  del file, il segmento precedente da 256 KB diventa protetto DA WORM.

Se si specifica un periodo di autocommit per il volume, i file .WORM che non vengono modificati per un periodo superiore al periodo di autocommit vengono impegnati in WORM.



VAM non è supportato sui volumi del registro di controllo di SnapLock.

#### Fasi

1. Attiva VAM:

```
volume snaplock modify -vserver SVM_name -volume volume_name -is-volume-append  
-mode-enabled true|false
```

Per un elenco completo delle opzioni, vedere la pagina man del comando.

Il seguente comando attiva la funzione VAM sul volume `vol1` Di `SVMvs1`:

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume  
-append-mode-enabled true
```

2. Utilizzare un comando o un programma adatto per creare file con permessi di scrittura.

Per impostazione predefinita, i file sono associati A WORM.

### Assegnare le copie Snapshot a WORM su una destinazione del vault

È possibile utilizzare SnapLock per SnapVault per proteggere WORM le copie Snapshot sullo storage secondario. Tutte le attività di base di SnapLock vengono eseguite sulla destinazione del vault. Il volume di destinazione viene montato automaticamente in sola lettura, pertanto non è necessario assegnare esplicitamente le copie Snapshot a WORM; pertanto, la creazione di copie Snapshot pianificate sul volume di destinazione utilizzando i criteri SnapMirror non è supportata.

#### Prima di iniziare

- Il cluster di origine deve eseguire ONTAP 8.2.2 o versione successiva.
- Gli aggregati di origine e destinazione devono essere a 64 bit.
- Il volume di origine non può essere un volume SnapLock.
- I volumi di origine e di destinazione devono essere creati in cluster peered con SVM peered.

Per ulteriori informazioni, vedere ["Peering dei cluster"](#).

- Se la funzione di crescita automatica del volume è disattivata, lo spazio libero sul volume di destinazione deve essere superiore di almeno il cinque percento allo spazio utilizzato sul volume di origine.

#### A proposito di questa attività

Il volume di origine può utilizzare storage NetApp o non NetApp. Per lo storage non NetApp, è necessario utilizzare la virtualizzazione FlexArray.



Non è possibile rinominare una copia Snapshot che è stata impegnata nello stato WORM.

È possibile clonare i volumi SnapLock, ma non i file su un volume SnapLock.



I LUN non sono supportati nei volumi SnapLock. Le LUN sono supportate nei volumi SnapLock solo in scenari in cui le copie Snapshot create su un volume non SnapLock vengono trasferite a un volume SnapLock per la protezione come parte della relazione del vault di SnapLock. I LUN non sono supportati nei volumi SnapLock in lettura/scrittura. Tuttavia, le copie Snapshot a prova di manomissione sono supportate sia sui volumi di origine di SnapMirror che sui volumi di destinazione che contengono LUN.

A partire da ONTAP 9.14.1, è possibile specificare i periodi di conservazione per etichette SnapMirror specifiche nella policy di SnapMirror della relazione di SnapMirror, in modo che le copie Snapshot replicate dall'origine al volume di destinazione vengano conservate per il periodo di conservazione specificato nella regola. Se non viene specificato alcun periodo di conservazione, viene utilizzato il periodo di conservazione predefinito del volume di destinazione.

A partire da ONTAP 9.13.1, è possibile ripristinare istantaneamente una copia Snapshot bloccata sul volume SnapLock di destinazione di una relazione del vault di SnapLock creando un FlexClone con l' `snaplock-type` Opzione impostata su "non snaplock" e specifica la copia Snapshot come "snapshot principale" quando si esegue l'operazione di creazione del clone del volume. Scopri di più ["Creazione di un volume FlexClone con un tipo di SnapLock"](#).

Per le configurazioni MetroCluster, è necessario conoscere quanto segue:

- È possibile creare una relazione SnapVault solo tra le SVM di origine della sincronizzazione, non tra una SVM di origine della sincronizzazione e una SVM di destinazione della sincronizzazione.
- È possibile creare una relazione SnapVault da un volume su una SVM di origine della sincronizzazione a una SVM di servizio dati.
- È possibile creare una relazione SnapVault da un volume su una SVM di servizio dati a un volume DP su una SVM di origine sincronizzazione.

L'illustrazione seguente mostra la procedura per l'inizializzazione di una relazione del vault di SnapLock:

## Fasi

1. Identificare il cluster di destinazione.
2. Sul cluster di destinazione, ["Installare la licenza SnapLock"](#), ["Inizializzare l'orologio di conformità"](#), E, se si utilizza una versione di ONTAP precedente alla 9.10.1, ["Creazione di un aggregato SnapLock"](#).
3. Nel cluster di destinazione, creare un volume di destinazione SnapLock di tipo DP di dimensioni uguali o superiori a quelle del volume di origine:

```
volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name  
-snaplock-type compliance|enterprise -type DP -size size
```



A partire da ONTAP 9.10.1, i volumi SnapLock e non SnapLock possono esistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1. Utilizzare l'opzione volume -snaplock-type per specificare un tipo di volume Compliance o Enterprise SnapLock. Nelle versioni di ONTAP precedenti a ONTAP 9.10.1, la modalità SnapLock, Compliance o Enterprise, viene ereditata dall'aggregato. I volumi di destinazione flessibili in base alla versione non sono supportati. L'impostazione della lingua del volume di destinazione deve corrispondere all'impostazione della lingua del volume di origine.

Il seguente comando crea un SnapLock da 2 GB Compliance volume denominato dstvolB poll SVM2 sull'aggregato node01\_aggr:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. Nel cluster di destinazione, impostare il periodo di conservazione predefinito, come descritto in [Impostare il periodo di conservazione predefinito](#).



A un volume SnapLock che è una destinazione del vault è assegnato un periodo di conservazione predefinito. Il valore per questo periodo viene inizialmente impostato su un minimo di 0 anni per i volumi aziendali SnapLock e su un massimo di 30 anni per i volumi di conformità SnapLock. Ogni copia Snapshot di NetApp viene inizialmente impegnata con questo periodo di conservazione predefinito. Il periodo di conservazione può essere esteso in un secondo momento, se necessario. Per ulteriori informazioni, vedere [Imposta la panoramica del tempo di conservazione](#).

5. [Creare una nuova relazione di replica](#) Tra l'origine non SnapLock e la nuova destinazione SnapLock creata

nel passaggio 3.

In questo esempio viene creata una nuova relazione di SnapMirror con il volume SnapLock di destinazione dstvolB utilizzando una policy di XDPDefault. Per eseguire il vault delle copie Snapshot etichettate giornalmente e settimanalmente in base a una pianificazione oraria:

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```



Creare un criterio di replica personalizzato oppure un programma personalizzato se le impostazioni predefinite disponibili non sono adatte.

6. Sulla SVM di destinazione, inizializzare la relazione SnapVault creata nella fase 5:

**snapmirror initialize -destination-path *destination\_path***

Il seguente comando inizializza la relazione tra il volume di origine srcvolA acceso SVM1 e il volume di destinazione dstvolB acceso SVM2:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

7. Una volta inizializzata la relazione e inattiva, utilizzare `snapshot show` Sulla destinazione per verificare il tempo di scadenza SnapLock applicato alle copie Snapshot replicate.

Questo esempio elenca le copie Snapshot sul volume dstvolB che hanno l'etichetta SnapMirror e la data di scadenza SnapLock:

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields  
snapmirror-label, snaplock-expiry-time
```

#### Informazioni correlate

["Peering di cluster e SVM"](#)

["Backup del volume con SnapVault"](#)

#### Mirroring dei file WORM per il disaster recovery

È possibile utilizzare SnapMirror per replicare i file WORM in un'altra posizione geografica per il disaster recovery e altri scopi. Sia il volume di origine che il volume di destinazione devono essere configurati per SnapLock e entrambi i volumi devono avere la stessa modalità SnapLock, Compliance o Enterprise. Vengono replicate tutte le principali proprietà SnapLock del volume e dei file.

#### Prerequisiti

I volumi di origine e di destinazione devono essere creati in cluster peered con SVM peered. Per ulteriori informazioni, vedere ["Peering di cluster e SVM"](#).

## A proposito di questa attività

- A partire da ONTAP 9.5, è possibile replicare i file WORM con la relazione SnapMirror di tipo XDP (Extended Data Protection) piuttosto che con la relazione di tipo DP (Data Protection). La modalità XDP è indipendente dalla versione di ONTAP ed è in grado di differenziare i file memorizzati nello stesso blocco, semplificando notevolmente la risincronizzazione dei volumi replicati in modalità Compliance. Per informazioni su come convertire una relazione di tipo DP esistente in una relazione di tipo XDP, vedere ["Protezione dei dati"](#).
- Un'operazione di risincronizzazione su una relazione SnapMirror di tipo DP non riesce per un volume in modalità di conformità se SnapLock determina che causerà una perdita di dati. Se un'operazione di risincronizzazione non riesce, è possibile utilizzare `volume clone create` per creare un clone del volume di destinazione. È quindi possibile risincronizzare il volume di origine con il clone.
- Una relazione SnapMirror di tipo XDP tra volumi compatibili con SnapLock supporta una risincronizzazione dopo un'interruzione anche se i dati sulla destinazione sono stati diversi dall'origine dopo l'interruzione.

In una risincronizzazione, quando viene rilevata una divergenza di dati tra l'origine e la destinazione oltre lo snapshot comune, viene tagliata una nuova istantanea sulla destinazione per acquisire questa divergenza. Il nuovo snapshot e lo snapshot comune sono entrambi bloccati con un tempo di conservazione come segue:

- Il tempo di scadenza del volume della destinazione
- Se il tempo di scadenza del volume è passato o non è stato impostato, lo snapshot viene bloccato per un periodo di 30 giorni
- Se la destinazione dispone di conservazione a fini giudiziari, il periodo di scadenza del volume effettivo viene mascherato e visualizzato come 'indefinito', tuttavia lo snapshot viene bloccato per la durata del periodo di scadenza del volume effettivo.

Se il volume di destinazione ha un periodo di scadenza successivo a quello di origine, il periodo di scadenza di destinazione viene mantenuto e non viene sovrascritto dal periodo di scadenza del volume di origine successivo alla risincronizzazione.

Se sulla destinazione sono presenti legal-stive che differiscono dall'origine, non è consentita una risincronizzazione. L'origine e la destinazione devono avere le stesse disposizioni legali o tutte le disposizioni legali sulla destinazione devono essere rilasciate prima di tentare una risincronizzazione.

Una copia Snapshot bloccata sul volume di destinazione creato per acquisire i dati divergenti può essere copiata nell'origine utilizzando la CLI eseguendo `snapmirror update -s snapshot` comando. Una volta copiata, l'istantanea continuerà a essere bloccata anche all'origine.


- Le relazioni di protezione dei dati SVM non sono supportate.
- Le relazioni di protezione dei dati di condivisione del carico non sono supportate.

La seguente illustrazione mostra la procedura per inizializzare una relazione SnapMirror:

## System Manager

A partire da ONTAP 9.12.1, è possibile utilizzare Gestione di sistema per impostare la replica di SnapMirror dei file WORM.

### Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi).
2. Fare clic su **Mostra/Nascondi** e selezionare **tipo SnapLock** per visualizzare la colonna nella finestra **volumi**.
3. Individuare un volume SnapLock.
4. Fare clic su  E selezionare **Protect**.
5. Scegliere il cluster di destinazione e la VM di storage di destinazione.
6. Fare clic su **altre opzioni**.
7. Selezionare **Mostra policy legacy** e selezionare **DPDefault (legacy)**.
8. Nella sezione **Destination Configuration details** (Dettagli configurazione destinazione), selezionare **Override transfer schedule** (Ignora pianificazione trasferimento) e selezionare **Hourly** (orario).
9. Fare clic su **Save** (Salva).
10. A sinistra del nome del volume di origine, fare clic sulla freccia per espandere i dettagli del volume, quindi a destra della pagina, esaminare i dettagli della protezione di SnapMirror remoto.
11. Sul cluster remoto, accedere a **Relazioni di protezione**.
12. Individuare la relazione e fare clic sul nome del volume di destinazione per visualizzare i dettagli della relazione.
13. Verificare che il tipo SnapLock del volume di destinazione e altre informazioni SnapLock siano disponibili.

### CLI

1. Identificare il cluster di destinazione.
2. Sul cluster di destinazione, ["Installare la licenza SnapLock"](#), ["Inizializzare l'orologio di conformità"](#), E, se si utilizza una versione di ONTAP precedente alla 9.10.1, ["Creazione di un aggregato SnapLock"](#).
3. Nel cluster di destinazione, creare un volume di destinazione SnapLock di tipo DP di dimensioni uguali o superiori al volume di origine:

```
volume create -vserver SVM_name -volume volume_name -aggregate  
aggregate_name -snaplock-type compliance|enterprise -type DP -size size
```



A partire da ONTAP 9.10.1, i volumi SnapLock e non SnapLock possono esistere sullo stesso aggregato; pertanto, non è più necessario creare un aggregato SnapLock separato se si utilizza ONTAP 9.10.1. Utilizzare l'opzione volume -snaplock-type per specificare un tipo di volume Compliance o Enterprise SnapLock. Nelle versioni di ONTAP precedenti a ONTAP 9.10.1, la modalità SnapLock (Compliance o Enterprise) viene ereditata dall'aggregato. I volumi di destinazione flessibili in base alla versione non sono supportati. L'impostazione della lingua del volume di destinazione deve corrispondere all'impostazione della lingua del volume di origine.

Il seguente comando crea un SnapLock da 2 GB Compliance volume denominato dstvolB poll SVM2 sull'aggregato node01\_aggr:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate  
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. Sulla SVM di destinazione, creare un criterio SnapMirror:

```
snapmirror policy create -vserver SVM_name -policy policy_name
```

Il seguente comando crea il criterio a livello di SVM SVM1-mirror:

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. Sulla SVM di destinazione, creare una pianificazione SnapMirror:

```
job schedule cron create -name schedule_name -dayofweek day_of_week -hour  
hour -minute minute
```

Il comando seguente crea una pianificazione SnapMirror denominata weekendcron:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek  
"Saturday, Sunday" -hour 3 -minute 0
```

6. Sulla SVM di destinazione, creare una relazione SnapMirror:

```
snapmirror create -source-path source_path -destination-path  
destination_path -type XDP|DP -policy policy_name -schedule schedule_name
```

Il comando seguente crea una relazione SnapMirror tra il volume di origine srcvolA acceso SVM1 e il volume di destinazione dstvolB acceso SVM2 e assegna il criterio `SVM1-mirror` e il calendario weekendcron:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination  
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule  
weekendcron
```



Il tipo di XDP è disponibile in ONTAP 9.5 e versioni successive. È necessario utilizzare il tipo di DP in ONTAP 9.4 e versioni precedenti.

7. Sulla SVM di destinazione, inizializzare la relazione SnapMirror:

```
snapmirror initialize -destination-path destination_path
```

Il processo di inizializzazione esegue un *trasferimento baseline* al volume di destinazione. SnapMirror crea una copia Snapshot del volume di origine, quindi trasferisce la copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione. Inoltre, trasferisce al volume di destinazione tutte le altre copie Snapshot presenti nel volume di origine.

Il seguente comando inizializza la relazione tra il volume di origine `srcvolA` acceso SVM1 e il volume di destinazione `dstvolB` acceso SVM2:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

### Informazioni correlate

["Peering di cluster e SVM"](#)

["Preparazione al disaster recovery dei volumi"](#)

["Protezione dei dati"](#)

### Conservare i file WORM durante i contenziosi utilizzando la conservazione a fini legali

A partire da ONTAP 9.3, puoi conservare i file WORM in modalità di conformità per tutta la durata di un contenzioso utilizzando la funzione *conservazione legale*.

#### Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore di SnapLock.

["Creare un account amministratore di SnapLock"](#)

- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

#### A proposito di questa attività

Un file in stato di conservazione legale si comporta come un file WORM con un periodo di conservazione indefinito. È responsabilità dell'utente specificare quando scade il periodo di conservazione legale.

Il numero di file che è possibile inserire in un blocco legale dipende dallo spazio disponibile sul volume.

#### Fasi

1. Avvio di un blocco legale:

```
snaplock legal-hold begin -litigation-name litigation_name -volume volume_name -path path_name
```

Il seguente comando avvia un blocco legale per tutti i file in `vol1`:

```
cluster1::> snaplock legal-hold begin -litigation-name litigation1 -volume vol1 -path /
```

2. Fine di un periodo di conservazione legale:

```
snaplock legal-hold end -litigation-name litigation_name -volume volume_name -path path_name
```

Il seguente comando termina un blocco legale per tutti i file in `vol1`:



```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume  
vol1 -path /
```

## Panoramica sull'eliminazione dei file WORM

È possibile eliminare i file WORM in modalità Enterprise durante il periodo di conservazione utilizzando la funzione di eliminazione con privilegi. Prima di poter utilizzare questa funzione, è necessario creare un account amministratore di SnapLock e, utilizzando l'account, attivare la funzione.

### Creare un account amministratore di SnapLock

Per eseguire un'eliminazione con privilegi, è necessario disporre dei privilegi di amministratore di SnapLock. Questi privilegi sono definiti nel ruolo vsadmin-snaplock. Se non è stato ancora assegnato tale ruolo, è possibile chiedere all'amministratore del cluster di creare un account amministratore SVM con il ruolo di amministratore di SnapLock.

### Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

### Fasi

1. Creare un account amministratore SVM con il ruolo di amministratore di SnapLock:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Il seguente comando attiva l'account amministratore SVM SnapLockAdmin con il predefinito vsadmin-snaplock ruolo di accesso SVM1 utilizzo di una password:

```
cluster1::> security login create -vserver SVM1 -user-or-group-name  
SnapLockAdmin -application ssh -authmethod password -role vsadmin-  
snaplock
```

### Attivare la funzione di eliminazione con privilegi

È necessario attivare esplicitamente la funzionalità di eliminazione con privilegi sul volume Enterprise che contiene i file WORM che si desidera eliminare.

### A proposito di questa attività

Il valore di `-privileged-delete` l'opzione determina se l'eliminazione con privilegi è attivata. I valori possibili sono `enabled`, `disabled`, e `permanently-disabled`.



`permanently-disabled` è lo stato del terminale. Non è possibile attivare l'eliminazione con privilegi sul volume dopo aver impostato lo stato su `permanently-disabled`.

## Fasi

1. Abilitare l'eliminazione con privilegi per un volume aziendale SnapLock:

```
volume snaplock modify -vserver SVM_name -volume volume_name -privileged  
-delete disabled|enabled|permanently-disabled
```

Il comando seguente attiva la funzione di eliminazione con privilegi per il volume Enterprise dataVol acceso SVM1:

```
SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged  
-delete enabled
```

## Eliminare i file WORM in modalità Enterprise

È possibile utilizzare la funzione di eliminazione con privilegi per eliminare i file WORM in modalità Enterprise durante il periodo di conservazione.

### Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore di SnapLock.
- È necessario aver creato un registro di controllo di SnapLock e attivato la funzione di eliminazione con privilegi sul volume aziendale.

### A proposito di questa attività

Non è possibile utilizzare un'operazione di eliminazione con privilegi per eliminare un file WORM scaduto. È possibile utilizzare `volume file retention show` Per visualizzare il tempo di conservazione del file WORM che si desidera eliminare. Per ulteriori informazioni, vedere la pagina man del comando.

## Fase

1. Eliminare un file WORM su un volume Enterprise:

```
volume file privileged-delete -vserver SVM_name -file file_path
```

Il seguente comando elimina il file `/vol/dataVol/f1` Su SVM1:

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

## Spostare un volume SnapLock

A partire da ONTAP 9.8, è possibile spostare un volume SnapLock in un aggregato di destinazione dello stesso tipo, da Enterprise a Enterprise o Compliance a Compliance.

Per spostare un volume SnapLock, è necessario assegnare il ruolo di protezione SnapLock.

### Creare un account amministratore di sicurezza SnapLock

Per eseguire lo spostamento di un volume SnapLock, è necessario disporre dei privilegi di amministratore della sicurezza di SnapLock. Questo privilegio viene concesso con il ruolo *SnapLock*, introdotto in ONTAP 9.8. Se non è stato ancora assegnato tale ruolo, è possibile chiedere all'amministratore del cluster di creare un utente di protezione SnapLock con questo ruolo di protezione SnapLock.

#### Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- È necessario aver effettuato l'accesso con una connessione sicura (SSH, console o ZAPI).

#### A proposito di questa attività

Il ruolo SnapLock è associato alla SVM amministrativa, a differenza del ruolo vsadmin-snaplock, associato alla SVM dei dati.

#### Fase

1. Creare un account amministratore SVM con il ruolo di amministratore di SnapLock:

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

Il seguente comando attiva l'account amministratore SVM SnapLockAdmin con il predefinito snaplock Ruolo per accedere a SVM di amministrazione cluster1 utilizzo di una password:

```
cluster1::> security login create -vserver cluster1 -user-or-group-name  
SnapLockAdmin -application ssh -authmethod password -role snaplock
```

### Spostare un volume SnapLock

È possibile utilizzare `volume move` Comando per spostare un volume SnapLock in un aggregato di destinazione.

#### Di cosa hai bisogno

- È necessario aver creato un registro di controllo protetto da SnapLock prima di eseguire lo spostamento del volume SnapLock.

["Creare un registro di controllo".](#)

- Se si utilizza una versione di ONTAP precedente a ONTAP 9.10.1, l'aggregato di destinazione deve essere dello stesso tipo di SnapLock del volume SnapLock che si desidera spostare, ovvero Compliance to Compliance o Enterprise to Enterprise. A partire da ONTAP 9.10.1, questa restrizione viene rimossa e un aggregato può includere volumi Compliance e Enterprise SnapLock, oltre a volumi non SnapLock.
- Devi essere un utente con il ruolo di sicurezza SnapLock.

#### Fasi

1. Utilizzando una connessione sicura, accedere alla LIF di gestione del cluster di ONTAP:

```
ssh snaplock_user@cluster_mgmt_ip
```

2. Spostamento di un volume SnapLock:

```
volume move start -vserver SVM_name -volume SnapLock_volume_name -destination  
-aggregate destination_aggregate_name
```

3. Controllare lo stato dell'operazione di spostamento del volume:

```
volume move show -volume SnapLock_volume_name -vserver SVM_name -fields  
volume,phase,vserver
```

## Bloccare una copia Snapshot per la protezione dagli attacchi ransomware

A partire da ONTAP 9.12.1, è possibile bloccare una copia Snapshot su un volume non SnapLock per fornire protezione dagli attacchi ransomware. Il blocco delle copie Snapshot garantisce che non possano essere eliminate accidentalmente o in modo illecito.

La funzione clock di conformità SnapLock consente di bloccare le copie Snapshot per un periodo specificato in modo che non possano essere eliminate fino al raggiungimento dell'ora di scadenza. Il blocco delle copie Snapshot le rende a prova di manomissione, proteggendole dalle minacce ransomware. È possibile utilizzare le copie Snapshot bloccate per ripristinare i dati se un volume viene compromesso da un attacco ransomware.

A partire da ONTAP 9.14.1, il blocco delle copie Snapshot supporta la conservazione a lungo termine delle copie Snapshot sulle destinazioni del vault SnapLock e su volumi di destinazione SnapMirror non SnapLock. Il blocco della copia Snapshot viene attivato impostando il periodo di conservazione utilizzando le regole dei criteri di SnapMirror associate a un [etichetta criterio esistente](#). La regola ha la priorità sul periodo di conservazione predefinito impostato sul volume. Se non esiste un periodo di conservazione associato all'etichetta SnapMirror, viene utilizzato il periodo di conservazione predefinito del volume.

### Requisiti e considerazioni sulle copie Snapshot a prova di manomissione

- Se si utilizza l'interfaccia utente di ONTAP, tutti i nodi del cluster devono eseguire ONTAP 9.12.1 o versione successiva. Se si utilizza Gestore di sistema, tutti i nodi devono eseguire ONTAP 9.13.1 o versione successiva.
- ["La licenza SnapLock deve essere installata sul cluster"](#). Questa licenza è inclusa in ["ONTAP uno"](#).
- ["È necessario inizializzare il clock di conformità sul cluster"](#).
- Quando il blocco Snapshot è attivato su un volume, è possibile aggiornare i cluster a una versione di ONTAP successiva a ONTAP 9.12.1; Tuttavia, non è possibile ripristinare una versione precedente di ONTAP fino a quando tutte le copie Snapshot bloccate non hanno raggiunto la data di scadenza e non vengono eliminate e il blocco delle copie Snapshot non viene disattivato.
- Quando un'istantanea è bloccata, il tempo di scadenza del volume viene impostato sul tempo di scadenza della copia Snapshot. Se più di una copia Snapshot è bloccata, il tempo di scadenza del volume riflette il tempo di scadenza maggiore tra tutte le copie Snapshot.
- Il periodo di conservazione per le copie Snapshot bloccate ha la precedenza sul conteggio copie Snapshot, il che significa che il limite di conservazione non viene rispettato se il periodo di conservazione delle copie Snapshot bloccate non è scaduto.

- In una relazione SnapMirror, è possibile impostare un periodo di conservazione su una regola dei criteri del vault mirror e il periodo di conservazione viene applicato alle copie Snapshot replicate sulla destinazione se il volume di destinazione ha attivato il blocco delle copie Snapshot. Il periodo di conservazione ha la precedenza sul numero di conservazione; ad esempio, le copie Snapshot che non hanno superato la scadenza verranno conservate anche se il numero di conservazione viene superato.
- È possibile rinominare una copia Snapshot su un volume non SnapLock. Le operazioni di ridenominazione di Snapshot sul volume primario di una relazione SnapMirror si riflettono sul volume secondario solo se il criterio è MirrorAllSnapshots. Per gli altri tipi di policy, la copia Snapshot rinominata non viene propagata durante gli aggiornamenti.
- Se si utilizza l'interfaccia utente di ONTAP, è possibile ripristinare una copia Snapshot bloccata con `volume snapshot restore` Solo se la copia Snapshot bloccata è la più recente. Se sono presenti copie Snapshot non scadute dopo quella da ripristinare, l'operazione di ripristino della copia Snapshot non riesce.

### **Funzionalità supportate con copie Snapshot antimanomissione**

- Volumi FlexGroup

Il blocco delle copie Snapshot è supportato sui volumi FlexGroup. Il blocco di Snapshot si verifica solo sulla copia Snapshot del componente principale. L'eliminazione del volume FlexGroup è consentita solo se è trascorso il tempo di scadenza del costituente root.

- Conversione da FlexVol a FlexGroup

È possibile convertire un volume FlexVol con copie Snapshot bloccate in un volume FlexGroup. Le copie Snapshot rimangono bloccate dopo la conversione.

- Clone del volume e clone del file

È possibile creare cloni di volume e file da una copia Snapshot bloccata.

### **Funzionalità non supportate**

Le seguenti funzioni attualmente non sono supportate con le copie Snapshot antimanomissione:

- Cloud Volumes ONTAP
- Gruppi di coerenza
- FabricPool
- Volumi FlexCache
- SMtape
- Continuità aziendale SnapMirror (SM-BC)
- Regole di policy di SnapMirror che utilizzano `-schedule` parametro
- SnapMirror sincrono
- Mobilità dei dati delle SVM (utilizzata per la migrazione o il trasferimento di una SVM da un cluster di origine a un cluster di destinazione)

### **Attiva il blocco delle copie Snapshot durante la creazione di un volume**

A partire da ONTAP 9.12.1, è possibile attivare il blocco delle copie Snapshot quando si crea un nuovo volume o quando si modifica un volume esistente utilizzando `-snapshot-locking-enabled` con `volume create` e `volume modify` Comandi nella CLI. A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per

attivare il blocco delle copie Snapshot.

### System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi) e selezionare **Add** (Aggiungi).
2. Nella finestra **Add Volume** (Aggiungi volume), selezionare **More Options** (altre opzioni).
3. Immettere il nome del volume, le dimensioni, la policy di esportazione e il nome della condivisione.
4. Selezionare **Enable Snapshot Locking** (attiva blocco snapshot). Questa selezione non viene visualizzata se la licenza SnapLock non è installata.
5. Se non è già abilitato, selezionare **Inizializza orologio conformità SnapLock**.
6. Salvare le modifiche.
7. Nella finestra **Volumes** (volumi), selezionare il volume aggiornato e scegliere **Overview** (Panoramica).
8. Verificare che **blocco copia snapshot SnapLock** sia visualizzato come **abilitato**.

### CLI

1. Per creare un nuovo volume e attivare il blocco delle copie Snapshot, immettere il seguente comando:

```
volume create -vserver vs1 -volume volume_name -snapshot-locking
-enabled true
```


Il comando seguente attiva il blocco delle copie Snapshot su un nuovo volume denominato vol1:

```
> volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
-locking-enabled true
Warning: Snapshot copy locking is being enabled on volume "vol1" in
Vserver "vs1". It cannot be disabled until all locked Snapshot
copies are past their expiry time. A volume with unexpired locked
Snapshot copies cannot be deleted.
Do you want to continue: {yes|no}: y
[Job 32] Job succeeded: Successful
```

### Attiva il blocco delle copie Snapshot su un volume esistente

A partire da ONTAP 9.12.1, è possibile attivare il blocco delle copie Snapshot su un volume esistente utilizzando l'interfaccia utente di ONTAP. A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per attivare il blocco delle copie Snapshot su un volume esistente.

## System Manager

1. Selezionare **Storage > Volumes** (Storage > volumi).
2. Selezionare  E scegliere **Modifica > Volume**.
3. Nella finestra **Edit Volume** (Modifica volume), individuare la sezione Snapshot Copies (Local) Settings (Impostazioni snapshot Copies (locali)) e selezionare **Enable Snapshot Locking** (attiva blocco snapshot).

Questa selezione non viene visualizzata se la licenza SnapLock non è installata.

4. Se non è già abilitato, selezionare **Inizializza orologio conformità SnapLock**.
5. Salvare le modifiche.
6. Nella finestra **Volumes** (volumi), selezionare il volume aggiornato e scegliere **Overview** (Panoramica).
7. Verificare che **blocco copia snapshot SnapLock** sia visualizzato come **abilitato**.

## CLI

1. Per modificare un volume esistente per attivare il blocco delle copie Snapshot, immettere il seguente comando:

```
volume modify -vserver vservice_name -volume volume_name -snapshot-locking
-enabled true
```

## Creare una policy di copia Snapshot bloccata e applicare la conservazione

A partire da ONTAP 9.12.1, è possibile creare criteri di copia Snapshot per applicare un periodo di conservazione delle copie Snapshot e applicare il criterio a un volume per bloccare le copie Snapshot per il periodo specificato. È inoltre possibile bloccare una copia Snapshot impostando manualmente un periodo di conservazione. A partire da ONTAP 9.13.1, è possibile utilizzare Gestione sistema per creare policy di blocco delle copie Snapshot e applicarle a un volume.

### Creare un criterio di blocco delle copie Snapshot

## System Manager

1. Accedere a **Storage > Storage VM** e selezionare una storage VM.
2. Selezionare **Impostazioni**.
3. Individuare **Snapshot Policies** e selezionare ➔.
4. Nella finestra **Add Snapshot Policy**, inserire il nome del criterio.
5. Selezionare **+ Add**.
6. Fornire i dettagli della pianificazione della copia Snapshot, inclusi il nome della pianificazione, il numero massimo di copie Snapshot da conservare e il periodo di conservazione SnapLock.
7. Nella colonna **SnapLock Retention Period**, immettere il numero di ore, giorni, mesi o anni per conservare le copie Snapshot. Ad esempio, un criterio di copia Snapshot con un periodo di conservazione di 5 giorni blocca una copia Snapshot per 5 giorni dal momento della creazione e non può essere eliminata durante tale periodo. Sono supportati i seguenti intervalli di periodi di conservazione:
  - Anni: 0 - 100
  - Mesi: 0 - 1200
  - Giorni: 0 - 36500
  - Orario: 0 - 24
8. Salvare le modifiche.

## CLI

1. Per creare un criterio di copia Snapshot, immettere il seguente comando:

```
volume snapshot policy create -policy policy_name -enabled true -schedule1  
schedule1_name -count1 maximum_Snapshot_copies -retention-period1  
_retention_period
```

Il seguente comando crea un criterio di blocco delle copie Snapshot:


```
cluster1> volume snapshot policy create -policy policy_name -enabled  
true -schedule1 hourly -count1 24 -retention-period1 "1 days"
```

Una copia Snapshot non viene sostituita se è in stato di conservazione attivo; in altri termini, il conteggio delle trattenute non viene rispettato se sono presenti copie Snapshot bloccate che non sono ancora scadute.

## Applicare un criterio di blocco a un volume



## System Manager

1. Selezionare **Storage > Volumes** (Storage > volumi).
2. Selezionare  E scegliere **Modifica > Volume**.
3. Nella finestra **Edit Volume** (Modifica volume), selezionare **Schedule Snapshot Copies** (Pianifica copie Snapshot).
4. Selezionare il criterio di copia Snapshot di blocco dall'elenco.
5. Se il blocco della copia Snapshot non è già attivato, selezionare **Enable Snapshot Locking** (attiva blocco Snapshot).
6. Salvare le modifiche.

## CLI

1. Per applicare un criterio di blocco delle copie Snapshot a un volume esistente, immettere il seguente comando:

```
volume modify -volume volume_name -vserver vservers_name -snapshot-policy policy_name
```

### Applica il periodo di conservazione durante la creazione manuale della copia Snapshot

È possibile applicare un periodo di conservazione delle copie Snapshot quando si crea manualmente una copia Snapshot. Il blocco della copia Snapshot deve essere attivato sul volume, altrimenti l'impostazione del periodo di conservazione viene ignorata.

## System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi) e selezionare un volume.
2. Nella pagina dei dettagli del volume, selezionare la scheda **copie Snapshot**.
3. Selezionare **+ Add**.
4. Inserire il nome della copia Snapshot e la data di scadenza del SnapLock. È possibile selezionare il calendario per scegliere la data e l'ora di scadenza della conservazione.
5. Salvare le modifiche.
6. Nella pagina **volumi > copie Snapshot**, selezionare **Mostra/Nascondi** e scegliere **ora scadenza SnapLock** per visualizzare la colonna **ora scadenza SnapLock** e verificare che il tempo di conservazione sia impostato.

## CLI

1. Per creare manualmente una copia Snapshot e applicare un periodo di conservazione a blocchi, immettere il seguente comando:


```
volume snapshot create -volume volume_name -snapshot snapshot_copy_name  
-snaplock-expiry-time expiration_date_time
```

Il seguente comando crea una nuova copia Snapshot e imposta il periodo di conservazione:

```
cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot  
snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
```

## Applicare il periodo di conservazione a una copia Snapshot esistente

## System Manager

1. Selezionare **Storage > Volumes** (archiviazione > volumi) e selezionare un volume.
2. Nella pagina dei dettagli del volume, selezionare la scheda **copie Snapshot**.
3. Selezionare la copia Snapshot, quindi  e scegliere **Modify SnapLock Expiration Time** (Modifica ora di scadenza protocollo). È possibile selezionare il calendario per scegliere la data e l'ora di scadenza della conservazione.
4. Salvare le modifiche.
5. Nella pagina **volumi > copie Snapshot**, selezionare **Mostra/Nascondi** e scegliere **ora scadenza SnapLock** per visualizzare la colonna **ora scadenza SnapLock** e verificare che il tempo di conservazione sia impostato.

## CLI

1. Per applicare manualmente un periodo di conservazione a una copia Snapshot esistente, immettere il seguente comando:

```
volume snapshot modify-snaplock-expiry-time -volume volume_name -snapshot snapshot_copy_name -expiry-time expiration_date_time
```

Nell'esempio seguente viene applicato un periodo di conservazione a una copia Snapshot esistente:

```
cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1  
-snapshot snap2 -expiry-time "11/10/2022 09:00:00"
```

## Modifica di un criterio esistente per applicare la conservazione a lungo termine

A partire da ONTAP 9.14.1, è possibile modificare una policy SnapMirror esistente aggiungendo una regola per impostare la conservazione a lungo termine delle copie Snapshot. La regola viene utilizzata per ignorare il periodo di conservazione dei volumi predefinito sulle destinazioni del vault SnapLock e sui volumi di destinazione non SnapLock SnapMirror.

1. Aggiunta di una regola a una policy SnapMirror esistente:

```
snapmirror policy add-rule -vserver <SVM name> -policy <policy name>  
-snapmirror-label <label name> -keep <number of Snapshot copies> -retention  
-period [<integer> days|months|years]
```

Nell'esempio seguente viene creata una regola che applica un periodo di conservazione di 6 mesi al criterio esistente denominato "lockvault":

```
snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror  
-label test1 -keep 10 -retention-period "6 months"
```

## API SnapLock

È possibile utilizzare le API Zephyr per l'integrazione con la funzionalità SnapLock negli

script o nell'automazione del workflow. Le API utilizzano la messaggistica XML su HTTP, HTTPS e Windows DCE/RPC. Per ulteriori informazioni, vedere ["Documentazione sull'automazione ONTAP"](#).

#### **file-fingerprint-abortire**

Interrompere un'operazione di impronta digitale del file.

#### **file-fingerprint-dump**

Visualizzare le informazioni sull'impronta digitale del file.

#### **file-fingerprint-get-iter**

Visualizza lo stato delle operazioni di impronte digitali del file.

#### **file-fingerprint-start**

Generare un'impronta digitale del file.

#### **snaplock-archive-vserver-log**

Archiviare il file di log di audit attivo.

#### **snaplock-create-vserver-log**

Creare una configurazione del registro di controllo per una SVM.

#### **snaplock-delete-vserver-log**

Eliminare una configurazione del registro di controllo per una SVM.

#### **snaplock-file-privileged-delete**

Eseguire un'operazione di eliminazione con privilegi.

#### **snaplock-get-file-retention**

Ottenere il periodo di conservazione di un file.

#### **snaplock-get-node-compliance-clock**

Ottenere la data e l'ora del nodo ComplianceClock.

#### **snaplock-get-vserver-active-log-files-iter**

Visualizza lo stato dei file di log attivi.

#### **snaplock-get-vserver-log-iter**

Visualizzare la configurazione del registro di controllo.

### **snaplock-modify-vserver-log**

Modificare la configurazione del registro di controllo per una SVM.

### **snaplock-set-file-retention**

Impostare il tempo di conservazione di un file.

### **snaplock-set-node-compliance-clock**

Impostare la data e l'ora del nodo ComplianceClock.

### **snaplock-volume-set-privileged-delete**

Impostare l'opzione Privileged-delete su un volume aziendale SnapLock.

### **volume-get-snaplock-attrs**

Ottenere gli attributi di un volume SnapLock.

### **volume-set-snaplock-attrs**

Impostare gli attributi di un volume SnapLock.

## **Gruppi di coerenza**

### **Panoramica dei gruppi di coerenza**

Un gruppo di coerenza è un insieme di volumi gestiti come singola unità. In ONTAP, i gruppi di coerenza offrono una gestione semplice e una garanzia di protezione per un carico di lavoro applicativo che copre più volumi.

È possibile utilizzare gruppi di coerenza per semplificare la gestione dello storage. Immaginate di disporre di un database importante che comprende venti LUN. È possibile gestire le LUN su base individuale o trattare le LUN come un dataset solitario, organizzandole in un singolo gruppo di coerenza.

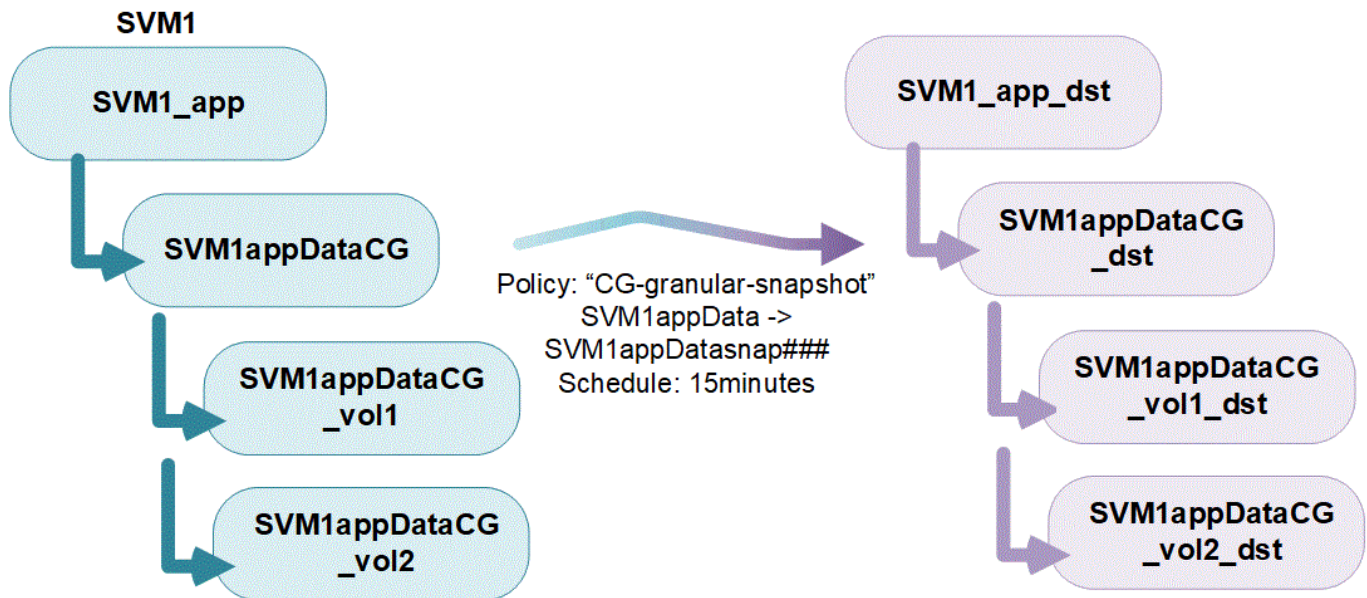
I gruppi di coerenza facilitano la gestione del carico di lavoro dell'applicazione, fornendo policy di protezione locali e remote facilmente configurabili e copie Snapshot simultanee coerenti con il crash o coerenti con l'applicazione di una raccolta di volumi in un momento specifico. Le copie Snapshot di un gruppo di coerenza permettono il ripristino di un intero workload dell'applicazione.

### **Informazioni sui gruppi di coerenza**

I gruppi di coerenza supportano qualsiasi volume FlexVol indipendentemente dal protocollo (NAS, SAN o NVMe) e possono essere gestiti tramite l'API REST di ONTAP o in Gestione sistema nella voce di menu **Storage > Consistency Groups**. A partire da ONTAP 9.14.1, è possibile gestire i gruppi di coerenza con l'interfaccia a riga di comando di ONTAP.

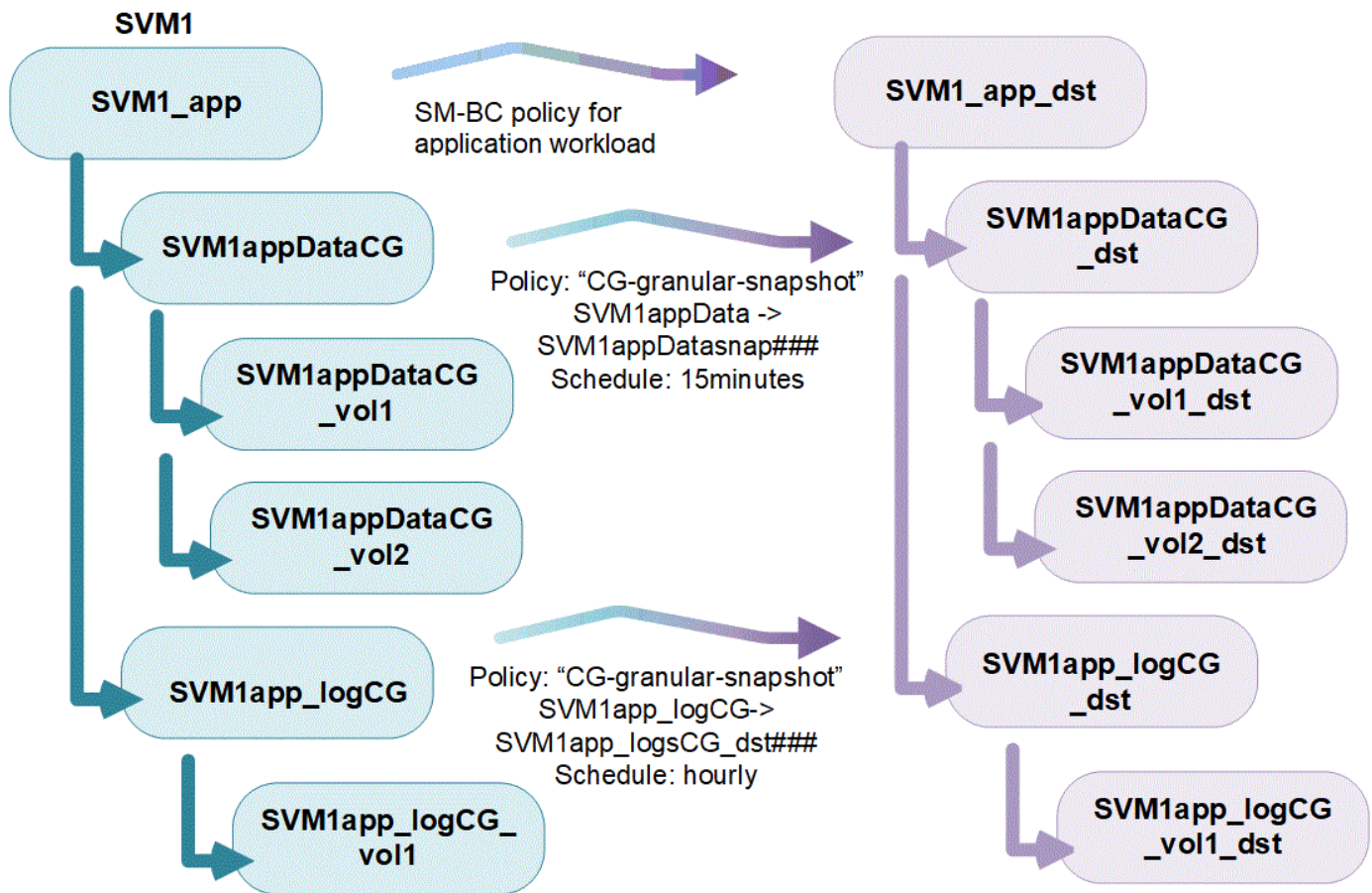
I gruppi di coerenza possono esistere come singole entità, come un insieme di volumi, o in una relazione gerarchica, che consiste di altri gruppi di coerenza. I singoli volumi possono avere una propria policy Snapshot granulare a livello di volume. Inoltre, è possibile utilizzare una policy di Snapshot a livello di gruppo di coerenza. Il gruppo di coerenza può avere solo una relazione di continuità aziendale SnapMirror (SM-BC) e una policy condivisa SM-BC, che possono essere utilizzate per ripristinare l'intero gruppo di coerenza.

Il seguente diagramma illustra come utilizzare un singolo gruppo di coerenza. I dati di un'applicazione ospitata su SVM1 si estende su due volumi: vol1 e vol2. Una policy Snapshot nel gruppo di coerenza acquisisce le copie Snapshot dei dati ogni 15 minuti.



I carichi di lavoro delle applicazioni più grandi potrebbero richiedere più gruppi di coerenza. In queste situazioni, è possibile creare gruppi di coerenza gerarchici, in cui un singolo gruppo di coerenza diventa i componenti secondari di un gruppo di coerenza padre. Il gruppo di coerenza padre può includere fino a cinque gruppi di coerenza figlio. Come nei singoli gruppi di coerenza, è possibile applicare una policy di protezione remota SM-BC all'intera configurazione dei gruppi di coerenza (padre e figlio) per ripristinare il carico di lavoro dell'applicazione.

Nell'esempio seguente, un'applicazione è ospitata su SVM1. L'amministratore ha creato un gruppo di coerenza principale, SVM1\_app, che include due gruppi di coerenza figlio: SVM1appDataCG per i dati e SVM1app\_logCG per i log. Ogni gruppo di coerenza figlio dispone della propria policy Snapshot. Copie Snapshot dei volumi in SVM1appDataCG ogni 15 minuti. Snapshot di SVM1app\_logCG vengono presi ogni ora. Il gruppo di coerenza padre SVM1\_app Dispone di una policy SM-BC che replica i dati per garantire un servizio continuo in caso di disastro.



A partire da ONTAP 9.12.1, il supporto dei gruppi di coerenza [cloning](#) e modificando i membri della coerenza con [aggiunta o rimozione di volumi](#) In Gestione di sistema e nell'API REST di ONTAP. A partire da ONTAP 9.12.1, l'API REST ONTAP supporta anche:

- Creazione di gruppi di coerenza con nuovi volumi NFS o SMB o spazi dei nomi NVMe.
- Aggiunta di volumi NFS o SMB nuovi o esistenti o spazi dei nomi NVMe a gruppi di coerenza esistenti.

Per ulteriori informazioni sull'API REST di ONTAP, fare riferimento a. "[Documentazione di riferimento API REST di ONTAP](#)".

## Monitorare i gruppi di coerenza

A partire da ONTAP 9.13.1, i gruppi di coerenza offrono il monitoraggio della capacità e delle prestazioni in tempo reale e cronologico, offrendo informazioni dettagliate sulle prestazioni delle applicazioni e dei singoli gruppi di coerenza.

I dati di monitoring vengono aggiornati ogni cinque minuti e vengono conservati per un massimo di un anno. Puoi tenere traccia delle metriche per:

- Performance: IOPS, latenza e throughput
- Capacità: Dimensioni, logica utilizzata, disponibile

È possibile visualizzare i dati di monitoraggio nella scheda **Panoramica** del menu del gruppo di coerenza in System Manager o richiederli nell'API REST. A partire da ONTAP 9.14.1, è possibile visualizzare le metriche del gruppo di coerenza con l'interfaccia CLI utilizzando il `consistency-group metrics show` comando.





In ONTAP 9.13.1, è possibile recuperare solo le metriche storiche utilizzando l'API REST. A partire da ONTAP 9.14.1, sono disponibili anche le metriche cronologiche in System Manager.

## Proteggere i gruppi di coerenza

I gruppi di coerenza offrono protezione attraverso:

- Policy di Snapshot
- [Continuità aziendale SnapMirror \(SM-BC\)](#)
- [\[mcc\]](#) (A partire da ONTAP 9.11.1)
- [SnapMirror asincrono](#) (A partire da ONTAP 9.13.1)
- ["Disaster recovery SVM"](#) (A partire da ONTAP 9.14.1)

La creazione di un gruppo di coerenza non attiva automaticamente la protezione. È possibile impostare policy di protezione locali e remote durante la creazione o dopo la creazione di un gruppo di coerenza.

Per configurare la protezione su un gruppo di coerenza, vedere ["Proteggere un gruppo di coerenza"](#).

Per utilizzare la protezione remota, è necessario soddisfare i requisiti di [Implementazioni di Business Continuity SnapMirror](#).



Non è possibile stabilire relazioni SM-BC sui volumi montati per l'accesso NAS.

## Gruppi di coerenza nelle configurazioni MetroCluster

A partire da ONTAP 9.11.1, è possibile eseguire il provisioning di gruppi di coerenza con nuovi volumi in un cluster all'interno di una configurazione MetroCluster. Il provisioning di questi volumi viene eseguito su aggregati mirrorati.

Una volta eseguito il provisioning, è possibile spostare i volumi associati ai gruppi di coerenza tra aggregati mirrorati e senza mirror. Pertanto, i volumi associati ai gruppi di coerenza possono essere posizionati su aggregati mirrorati, aggregati senza mirror o entrambi. È possibile modificare gli aggregati mirrorati contenenti volumi associati ai gruppi di coerenza in modo che diventino senza mirror. Allo stesso modo, è possibile modificare aggregati senza mirror contenenti volumi associati a gruppi di coerenza per abilitare il mirroring.

I volumi e le copie Snapshot associati ai gruppi di coerenza posizionati sugli aggregati con mirroring vengono replicati nel sito remoto (sito B). Il contenuto dei volumi sul sito B fornisce una garanzia di ordine di scrittura per il gruppo di coerenza, consentendo il ripristino dal sito B in caso di disastro. Puoi accedere alle copie Snapshot del gruppo di coerenza utilizzando il gruppo di coerenza con l'API REST e System Manager sui cluster che eseguono ONTAP 9.11.1 o versioni successive. A partire da ONTAP 9.14.1, è possibile accedere anche alle copie Snapshot con l'interfaccia a riga di comando di ONTAP.

Se alcuni o tutti i volumi associati a un gruppo di coerenza si trovano su aggregati senza mirror che non sono attualmente accessibili, LE operazioni GET o DELETE sul gruppo di coerenza si comportano come se i volumi locali o gli aggregati di hosting non fossero in linea.

## Configurazioni di gruppi di coerenza per la replica

Se il sito B esegue ONTAP 9.10.1 o versioni precedenti, solo i volumi associati ai gruppi di coerenza situati negli aggregati mirrorati vengono replicati nel sito B. Le configurazioni dei gruppi di coerenza vengono replicate solo nel sito B, se entrambi i siti eseguono ONTAP 9.11.1 o versione successiva. Dopo l'aggiornamento del sito B a ONTAP 9.11.1, i dati per i gruppi di coerenza sul sito A che hanno tutti i volumi



associati posizionati su aggregati mirrorati vengono replicati nel sito B.



Si consiglia di mantenere almeno il 20% di spazio libero per gli aggregati con mirroring, per performance e disponibilità dello storage ottimali. Sebbene il suggerimento sia del 10% per gli aggregati non speculari, il 10% di spazio aggiuntivo può essere utilizzato dal filesystem per assorbire le modifiche incrementali. I cambiamenti incrementali aumentano l'utilizzo dello spazio per gli aggregati con mirroring grazie all'architettura copy-on-write basata su Snapshot di ONTAP. Il mancato rispetto di queste Best practice può avere un impatto negativo sulle prestazioni.

## Considerazioni sull'upgrade

I gruppi di coerenza creati con SM-BC in ONTAP 9.8 e 9.9.1 verranno automaticamente aggiornati e gestiti in **Storage > Consistency Groups** in System Manager o nell'API REST di ONTAP quando si esegue l'aggiornamento a ONTAP 9.10.1 o versioni successive. Per ulteriori informazioni sull'aggiornamento da ONTAP 9.8 o 9.9.1, vedere ["Considerazioni sull'upgrade e il revert di SM-BC"](#).

Le copie Snapshot del gruppo di coerenza create nell'API REST possono essere gestite tramite l'interfaccia del Gruppo di coerenza di System Manager e tramite gli endpoint delle API REST del gruppo di coerenza. A partire da ONTAP 9.14.1, è possibile gestire anche gli Snapshot del gruppo di coerenza con l'interfaccia a riga di comando di ONTAP.



Copie Snapshot create con i comandi ONTAPI `cg-start` e `cg-commit` Sono riconosciuti come Snapshot del gruppo di coerenza e pertanto non possono essere gestiti tramite l'interfaccia del gruppo di coerenza di System Manager o gli endpoint del gruppo di coerenza nell'API REST di ONTAP. A partire da ONTAP 9.14.1, queste copie Snapshot possono essere mirrorati sul volume di destinazione, se si sta utilizzando una policy SnapMirror asincrona. Per ulteriori informazioni, vedere [Configurare la protezione asincrona di SnapMirror](#).

## Funzionalità supportate dalla release

|                                        | ONTAP<br>9.14.1 | ONTAP<br>9.13.1 | ONTAP<br>9.12.1  | ONTAP<br>9.11.1 | ONTAP<br>9.10.1 |
|----------------------------------------|-----------------|-----------------|------------------|-----------------|-----------------|
| Gruppi di coerenza gerarchica          | ✓               | ✓               | ✓                | ✓               | ✓               |
| Protezione locale con copie Snapshot   | ✓               | ✓               | ✓                | ✓               | ✓               |
| Continuità aziendale di SnapMirror     | ✓               | ✓               | ✓                | ✓               | ✓               |
| Supporto MetroCluster                  | ✓               | ✓               | ✓                | ✓               |                 |
| Commit bifase (solo API REST)          | ✓               | ✓               | ✓                | ✓               |                 |
| Tag di applicazioni e componenti       | ✓               | ✓               | ✓                |                 |                 |
| Clonare i gruppi di coerenza           | ✓               | ✓               | ✓                |                 |                 |
| Aggiungere e rimuovere volumi          | ✓               | ✓               | ✓                |                 |                 |
| Crea CGS con nuovi volumi NAS          | ✓               | ✓               | Solo API<br>REST |                 |                 |
| Crea CGS con i nuovi NVMe<br>Namespace | ✓               | ✓               | Solo API<br>REST |                 |                 |

|                                                         | ONTAP<br>9.14.1 | ONTAP<br>9.13.1 | ONTAP<br>9.12.1 | ONTAP<br>9.11.1 | ONTAP<br>9.10.1 |
|---------------------------------------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| Spostare i volumi tra i gruppi di coerenza figlio       | ✓               | ✓               |                 |                 |                 |
| Modificare la geometria del gruppo di coerenza          | ✓               | ✓               |                 |                 |                 |
| Monitoraggio                                            | ✓               | ✓               |                 |                 |                 |
| SnapMirror asincrono (solo singoli gruppi di coerenza)  | ✓               | ✓               |                 |                 |                 |
| Disaster recovery SVM (solo gruppi di coerenza singoli) | ✓               |                 |                 |                 |                 |
| Supporto CLI                                            | ✓               |                 |                 |                 |                 |

## Scopri di più sui gruppi di coerenza

### Consistency Groups for Application Management & Protection

With NetApp ONTAP 9.10.1 + System Manager

© 2022 NetApp, Inc. All rights reserved.





## Ulteriori informazioni

- ["Documentazione sull'automazione ONTAP"](#)
- [Continuità aziendale di SnapMirror](#)
- [Nozioni di base sul disaster recovery asincrono di SnapMirror](#)
- ["Documentazione MetroCluster"](#)

## Limiti del gruppo di coerenza

Durante la pianificazione e la gestione dei gruppi di coerenza, tenere conto dei limiti degli oggetti nell'ambito del cluster e del gruppo di coerenza padre o figlio.

## Limiti imposti

Nella tabella seguente vengono acquisiti i limiti per i gruppi di coerenza. Sono previsti limiti separati per i gruppi di coerenza che utilizzano SnapMirror Business Continuity (SM-BC). Per ulteriori informazioni, vedere ["SM-BC restrizioni e limitazioni per i limiti"](#).

| Limite                                                                                                                              | Scopo                      | Minimo               | Massimo                                        |
|-------------------------------------------------------------------------------------------------------------------------------------|----------------------------|----------------------|------------------------------------------------|
| Numero di gruppi di coerenza                                                                                                        | Cluster                    | 0                    | Uguale al numero massimo di volumi nel cluster |
| Numero di gruppi di coerenza padre                                                                                                  | Cluster                    | 0                    | Uguale al numero massimo di volumi nel cluster |
| Numero di gruppi di coerenza individuali e principali                                                                               | Cluster                    | 0                    | Uguale al numero massimo di volumi nel cluster |
| Numero di volumi in un gruppo di coerenza                                                                                           | Singolo gruppo di coerenza | 1 volume             | 80 volumi                                      |
| Numero di volumi nel figlio di un gruppo di coerenza padre                                                                          | Gruppo di coerenza padre   | 1 volume             | 80 volumi                                      |
| Numero di volumi in un gruppo di coerenza figlio                                                                                    | Gruppo di coerenza figlio  | 1 volume             | 80 volumi                                      |
| Numero di gruppi di coerenza figlio in un gruppo di coerenza padre                                                                  | Gruppo di coerenza padre   | 1 gruppo di coerenza | 5 gruppi di coerenza                           |
| Numero di relazioni di disaster recovery delle SVM in cui è presente un gruppo di coerenza (disponibile a partire dal ONTAP 9.14.1) | Cluster                    | 0                    | 32                                             |

## Limiti non applicati

La pianificazione minima supportata delle copie Snapshot per i gruppi di coerenza è di 30 minuti. Basata su ["Test per i gruppi flessibili"](#), Che condividono la stessa infrastruttura Snapshot dei gruppi di coerenza.

## Configurare un singolo gruppo di coerenza

È possibile creare gruppi di coerenza con volumi esistenti o nuove LUN o volumi (a seconda della versione di ONTAP). È possibile associare un volume o un LUN a un solo gruppo di coerenza alla volta.

### A proposito di questa attività

- In ONTAP dalla versione 9.10.1 alla 9.11.1, la modifica dei volumi membro di un gruppo di coerenza dopo la sua creazione non è supportata.

A partire da ONTAP 9.12.1, è possibile modificare i volumi membri di un gruppo di coerenza. Per ulteriori informazioni su questo processo, fare riferimento a [Modificare un gruppo di coerenza](#).

### **Creare un gruppo di coerenza con nuove LUN o volumi**

In ONTAP dalla versione 9.10.1 alla versione 9.12.1, è possibile creare un gruppo di coerenza utilizzando nuove LUN. A partire da ONTAP 9.13.1, System Manager supporta anche la creazione di un gruppo di coerenza con nuovi namespace NVMe o nuovi volumi NAS. (Questo è supportato anche nell'API REST di ONTAP a partire da ONTAP 9.12.1).

## System Manager

### Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare **+Aggiungi**, quindi selezionare il protocollo per l'oggetto di storage.

In ONTAP dalla versione 9.10.1 alla 9.12.1, l'unica opzione per un nuovo oggetto di storage è **l'utilizzo di nuove LUN**. A partire da ONTAP 9.13.1, System Manager supporta la creazione di gruppi di coerenza con nuovi namespace NVMe e nuovi volumi NAS.

3. Assegnare un nome al gruppo di coerenza. Indicare il numero di volumi o LUN e la capacità per volume o LUN.
  - a. **Tipo di applicazione:** Se si utilizza ONTAP 9.12.1 o versione successiva, selezionare un tipo di applicazione. Se non viene selezionato alcun valore, al gruppo di coerenza viene assegnato il tipo **Altro** per impostazione predefinita. Scopri di più sulla coerenza dei tag in [Tag di applicazioni e componenti](#). Se si intende creare un gruppo di coerenza con un criterio di protezione remota, è necessario utilizzare **Altro**.
  - b. Per **nuovi LUN**: Selezionare il sistema operativo host e il formato LUN. Inserire le informazioni dell'iniziatore host.
  - c. Per **nuovi volumi NAS**: Scegliere l'opzione di esportazione appropriata (NFS o SMB/CIFS) in base alla configurazione NAS della SVM.
  - d. Per **nuovi spazi dei nomi NVMe**: Selezionare il sistema operativo host e il sottosistema NVMe.
4. Per configurare i criteri di protezione, aggiungere un gruppo di coerenza figlio o i permessi di accesso, selezionare **altre opzioni**.
5. Selezionare **Salva**.
6. Verificare che il gruppo di coerenza sia stato creato tornando al menu principale del gruppo di coerenza in cui verrà visualizzato una volta completato il lavoro. Se si imposta una policy di protezione, si potrà sapere che è stata applicata quando viene visualizzato uno shield verde sotto la policy appropriata, remota o locale.

### CLI

A partire da ONTAP 9.14.1, puoi creare un nuovo gruppo di coerenza con nuovi volumi utilizzando l'interfaccia a riga di comando di ONTAP. Parametri specifici dipendono se i volumi sono SAN, NVMe o NFS.

#### Crea un gruppo di coerenza con i volumi NFS

1. Creare il gruppo di coerenza:

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volume-prefix -volume-count number -size size -export-policy policy_name
```

#### Crea un gruppo di coerenza con i volumi SAN

1. Creare il gruppo di coerenza:

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -lun lun_name -size size -lun-count number -igroup igroup_name
```

#### Crea un gruppo di coerenza con i namespace NVMe

1. Creare il gruppo di coerenza:

```
consistency-group create -vserver SVM_name -consistency-group  
consistency_group_name -namespace namespace_name -volume-count number  
-namespace-count number -size size -subsystem subsystem_name
```

**Al termine**

1. Verificare che il gruppo di coerenza sia stato creato utilizzando `consistency-group show` comando.

**Creare un gruppo di coerenza con i volumi esistenti**

È possibile utilizzare i volumi esistenti per creare un gruppo di coerenza.

## System Manager

### Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare **+Aggiungi**, quindi **utilizzando volumi esistenti**.
3. Assegnare un nome al gruppo di coerenza e selezionare la VM di storage.
  - a. **Tipo di applicazione:** Se si utilizza ONTAP 9.12.1 o versione successiva, selezionare un tipo di applicazione. Se non viene selezionato alcun valore, al gruppo di coerenza viene assegnato il tipo **Altro** per impostazione predefinita. Scopri di più sulla coerenza dei tag in [Tag di applicazioni e componenti](#). Se il gruppo di coerenza ha una relazione SM-BC, è necessario utilizzare **Altro**.
4. Selezionare i volumi esistenti da includere. Saranno disponibili per la selezione solo i volumi che non fanno già parte di un gruppo di coerenza.



Se si crea un gruppo di coerenza con i volumi esistenti, il gruppo di coerenza supporta i volumi FlexVol. I volumi con relazioni SnapMirror sincrone o asincrone possono essere aggiunti ai gruppi di coerenza, ma non sono compatibili con i gruppi di coerenza. I gruppi di coerenza non supportano i bucket S3 o le VM di storage con relazioni SVMMDR.

5. Selezionare **Salva**.
6. Verificare che il gruppo di coerenza sia stato creato tornando al menu principale del gruppo di coerenza in cui verrà visualizzato una volta completato il lavoro ONTAP. Se è stata scelta una policy di protezione, confermarla selezionando il gruppo di coerenza dal menu. Se si imposta una policy di protezione, si potrà sapere che è stata applicata quando viene visualizzato uno shield verde sotto la policy appropriata, remota o locale.

### CLI

A partire da ONTAP 9.14.1, puoi creare un gruppo di coerenza con i volumi esistenti utilizzando l'interfaccia a riga di comando di ONTAP.

### Fasi

1. Eseguire il `consistency-group create` comando. Il `-volumes` parameter accetta un elenco separato da virgole di nomi di volumi.

```
consistency-group create -vserver SVM_name -consistency-group consistency-group-name -volume volumes
```

2. Visualizzare il gruppo di coerenza utilizzando `consistency-group show` comando.

### Passi successivi

- [Proteggere un gruppo di coerenza](#)
- [Modificare un gruppo di coerenza](#)
- [Clonare un gruppo di coerenza](#)

## Configurare un gruppo di coerenza gerarchico

I gruppi di coerenza gerarchica consentono di gestire grandi carichi di lavoro su più volumi, creando un gruppo di coerenza padre che funge da ombrello per i gruppi di

coerenza figlio.

I gruppi di coerenza gerarchica hanno un padre che può includere fino a cinque singoli gruppi di coerenza. I gruppi di coerenza gerarchica possono supportare diverse policy Snapshot locali tra gruppi di coerenza o singoli volumi. Se si utilizza un criterio di protezione remota, questo verrà applicato all'intero gruppo di coerenza gerarchico (principale e figlio).

A partire da ONTAP 9.13.1, è possibile [modificare la geometria dei gruppi di coerenza](#) e [spostare i volumi tra i gruppi di coerenza figlio](#).

Per i limiti degli oggetti sui gruppi di coerenza, vedere [Limiti degli oggetti per i gruppi di coerenza](#).

### **Creare un gruppo di coerenza gerarchica con nuove LUN o volumi**

Quando si crea un gruppo di coerenza gerarchica, è possibile compilarlo con nuove LUN. A partire da ONTAP 9.13.1, puoi anche utilizzare nuovi namespace NVMe e volumi NAS.



## System Manager

### Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare **+Aggiungi**, quindi selezionare il protocollo per l'oggetto di storage.

In ONTAP dalla versione 9.10.1 alla 9.12.1, l'unica opzione per un nuovo oggetto di storage è **l'utilizzo di nuove LUN**. A partire da ONTAP 9.13.1, System Manager supporta la creazione di gruppi di coerenza con nuovi namespace NVMe e nuovi volumi NAS.

3. Assegnare un nome al gruppo di coerenza. Indicare il numero di volumi o LUN e la capacità per volume o LUN.
  - a. **Tipo di applicazione:** Se si utilizza ONTAP 9.12.1 o versione successiva, selezionare un tipo di applicazione. Se non viene selezionato alcun valore, al gruppo di coerenza viene assegnato il tipo **Altro** per impostazione predefinita. Scopri di più sulla coerenza dei tag in [Tag di applicazioni e componenti](#). Se si prevede di utilizzare una policy di protezione remota, è necessario scegliere **Altro**.
4. Selezionare il sistema operativo host e il formato LUN. Inserire le informazioni dell'iniziatore host.
  - a. Per **nuovi LUN**: Selezionare il sistema operativo host e il formato LUN. Inserire le informazioni dell'iniziatore host.
  - b. Per **nuovi volumi NAS**: Scegliere l'opzione di esportazione appropriata (NFS o SMB/CIFS) in base alla configurazione NAS della SVM.
  - c. Per **nuovi spazi dei nomi NVMe**: Selezionare il sistema operativo host e il sottosistema NVMe.
5. Per aggiungere un gruppo di coerenza figlio, selezionare **altre opzioni**, quindi **+Aggiungi gruppo di coerenza figlio**.
6. Selezionare il livello di performance, il numero di LUN o volumi e la capacità per LUN o volume. Indicare le configurazioni di esportazione appropriate o le informazioni del sistema operativo in base al protocollo in uso.
7. Facoltativamente, selezionare un criterio di snapshot locale e impostare le autorizzazioni di accesso.
8. Ripetere la procedura per un massimo di cinque gruppi di coerenza figlio.
9. Selezionare **Salva**.
10. Verificare che il gruppo di coerenza sia stato creato tornando al menu principale del gruppo di coerenza in cui verrà visualizzato una volta completato il lavoro ONTAP. Se si imposta un criterio di protezione, controllare il criterio appropriato, remoto o locale, che dovrebbe visualizzare uno schermo verde con un segno di spunta.

### CLI

A partire da ONTAP 9.14.1, è possibile creare un nuovo gruppo di coerenza gerarchica utilizzando la CLI.

### Fase

1. Creare il nuovo gruppo di coerenza utilizzando `consistency-group create` comando.

Il `volume-count` parametro imposta il numero di volumi in ogni gruppo di coerenza figlio. È possibile creare un gruppo di coerenza di origine con un massimo di cinque gruppi di coerenza child.

```
consistency-group create -vserver SVM_name -consistency-group
consistency_group_name -parent-consistency-group
parent_consistency_group_name -cg-count number_of_child_consistency_groups
```

```
-volume volume_prefix -volume-count number -size size -export-policy  
policy_name -storage-service extreme
```

## Creare un gruppo di coerenza gerarchica con i volumi esistenti

È possibile organizzare i volumi esistenti in un gruppo di coerenza gerarchico.

### System Manager

#### Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare **+Aggiungi**, quindi **utilizzando volumi esistenti**.
3. Selezionare la VM di storage.
4. Selezionare i volumi esistenti da includere. Saranno disponibili per la selezione solo i volumi che non fanno già parte di un gruppo di coerenza.
5. Per aggiungere un gruppo di coerenza figlio, selezionare **+Aggiungi gruppo di coerenza figlio**. Creare i gruppi di coerenza necessari, che verranno nominati automaticamente.
  - a. **Tipo di componente**: Se si utilizza ONTAP 9.12.1 o versione successiva, selezionare un tipo di componente "dati", "registri" o "Altro". Se non viene selezionato alcun valore, al gruppo di coerenza viene assegnato il tipo **Altro** per impostazione predefinita. Scopri di più sulla coerenza dei tag in [Tag di applicazioni e componenti](#). Se si intende utilizzare una policy di protezione remota, è necessario utilizzare **Altro**.
6. Assegnare i volumi esistenti a ciascun gruppo di coerenza.
7. Facoltativamente, selezionare un criterio Snapshot locale.
8. Ripetere la procedura per un massimo di cinque gruppi di coerenza figlio.
9. Selezionare **Salva**.
10. Verificare che il gruppo di coerenza sia stato creato tornando al menu principale del gruppo di coerenza in cui verrà visualizzato una volta completato il lavoro ONTAP. Se è stata scelta una policy di protezione, confermarla selezionando il gruppo di coerenza dal menu; sotto il tipo di policy appropriato, viene visualizzato uno shield verde con un segno di spunta all'interno di essa.

#### CLI

A partire da ONTAP 9.14.1, è possibile creare un gruppo di coerenza gerarchica utilizzando la CLI.

#### Fasi

1. Provisioning di un nuovo gruppo di coerenza di origine e assegnazione dei volumi a un nuovo gruppo di coerenza child:

```
consistency-group create -vserver svm_name -consistency-group  
child_consistency_group_name -parent-consistency-group  
parent_consistency_group_name -volumes volume_names
```

2. Invio `y` per confermare la creazione di un nuovo gruppo di coerenza principale e secondario.

### Passi successivi

- [Modificare la geometria di un gruppo di coerenza](#)

- [Modificare un gruppo di coerenza](#)
- [Proteggere un gruppo di coerenza](#)

## Proteggere i gruppi di coerenza

I gruppi di coerenza offrono una protezione locale e remota facilmente gestibile per LE applicazioni SAN, NAS e NVMe che si estendono su più volumi.

La creazione di un gruppo di coerenza non attiva automaticamente la protezione. Le policy di protezione possono essere impostate al momento della creazione o dopo la creazione del gruppo di coerenza. È possibile proteggere i gruppi di coerenza utilizzando:

- Copie snapshot locali
- Continuità aziendale SnapMirror (SM-BC)
- [MetroCluster \(inizio 9.11.1\)](#)
- SnapMirror asincrono (inizio 9.13.1)
- Disaster recovery SVM asincrono (inizio 9.14.1)

Se si utilizzano gruppi di coerenza nidificati, è possibile impostare criteri di protezione diversi per i gruppi di coerenza padre e figlio.

A partire da ONTAP 9.11.1, i gruppi di coerenza offrono [Creazione Snapshot di un gruppo di coerenza in due fasi](#). L'operazione Snapshot a due fasi esegue un controllo preliminare, accertandosi che la copia Snapshot venga acquisita correttamente.

Il ripristino può avvenire per un intero gruppo di coerenza, per un singolo gruppo di coerenza in una configurazione gerarchica o per singoli volumi all'interno del gruppo di coerenza. Il ripristino può essere ottenuto selezionando il gruppo di coerenza da cui si desidera eseguire il ripristino, selezionando il tipo di copia Snapshot e identificando la copia Snapshot su cui basare il ripristino. Per ulteriori informazioni su questo processo, vedere ["Ripristinare un volume da una copia Snapshot precedente"](#).

## Configurare un criterio Snapshot locale


L'impostazione di un criterio di protezione snapshot locale consente di creare un criterio che copre tutti i volumi in un gruppo di coerenza.

### A proposito di questa attività

La pianificazione minima supportata delle copie Snapshot per i gruppi di coerenza è di 30 minuti. Basata su ["Test per i gruppi flessibili"](#), Che condividono la stessa infrastruttura Snapshot dei gruppi di coerenza.

## System Manager

### Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza creato dal menu del gruppo di coerenza.
3. Nella parte superiore destra della pagina di panoramica per il gruppo di coerenza, selezionare **Modifica**.
4. Selezionare la casella di controllo accanto a **Schedule Snapshot Copies (local)**.
5. Selezionare una policy Snapshot. Per configurare un nuovo criterio personalizzato, fare riferimento a ["Creare una policy di protezione dei dati personalizzata"](#).
6. Selezionare **Salva**.
7. Tornare al menu della panoramica del gruppo di coerenza. Nella colonna di sinistra sotto **Snapshot Copies (Local)**, lo stato sarà Protected (protetto) accanto a .

### CLI

A partire da ONTAP 9.14.1, è possibile modificare il criterio di protezione di un gruppo di coerenza utilizzando l'interfaccia CLI.

### Fase

1. Immettere il seguente comando per impostare o modificare il criterio di protezione:

Se si modifica il criterio di protezione di una coerenza figlio, è necessario identificare il gruppo di coerenza padre utilizzando `-parent-consistency-group` *parent\_consistency\_group\_name* parametro.

```
consistency-group modify -vserver svm_name -consistency-group  
consistency_group_name -snapshot-policy policy_name
```

## Crea una copia Snapshot on-demand

Se devi creare una copia Snapshot del tuo gruppo di coerenza al di fuori di una policy normalmente pianificata, puoi crearne una on-demand.

## System Manager

### Fasi

1. Accedere a **archiviazione > gruppi di coerenza**.
2. Seleziona il gruppo di coerenza per cui desideri creare una copia Snapshot on-demand.
3. Passare alla scheda **Snapshot Copies** e selezionare **+Add**.
4. Fornire un **Name** e una **SnapMirror Label**. Nel menu a discesa per **coerenza**, selezionare **applicazione coerente** o **Crash coerente**.
5. Selezionare **Salva**.

### CLI

A partire da ONTAP 9.14.1, puoi creare una copia Snapshot on-demand di un gruppo di coerenza utilizzando la CLI.

### Fase

1. Creare la copia Snapshot:

Per impostazione predefinita, il tipo di Snapshot è coerente con il crash. È possibile modificare il tipo di istantanea con l'opzione `-type` parametro.

```
consistency-group snapshot create -vserver svm_name -consistency-group  
consistency_group_name -snapshot snapshot_name
```

## Creare Snapshot del gruppo di coerenza in due fasi

A partire da ONTAP 9.11.1, i gruppi di coerenza supportano commit a due fasi per la creazione di snapshot nel CG (Consistency group), che eseguono un controllo preliminare prima di salvare la copia Snapshot. Questa funzione è disponibile solo con l'API REST di ONTAP.

La creazione di snapshot CG in due fasi è disponibile solo per la creazione di Snapshot, non per il provisioning di gruppi di coerenza o il ripristino di gruppi di coerenza.

Un'istantanea CG in due fasi suddivide il processo di creazione delle snapshot in due fasi:

1. Nella prima fase, l'API esegue i controlli preliminari e attiva la creazione di snapshot. La prima fase include un parametro di timeout che indica il tempo necessario per il commit della copia Snapshot.
2. Se la richiesta nella fase uno viene completata correttamente, è possibile richiamare la seconda fase all'interno dell'intervallo designato dalla prima fase, assegnando la copia Snapshot all'endpoint appropriato.

### Prima di iniziare

- Per utilizzare la creazione di snapshot CG in due fasi, tutti i nodi del cluster devono eseguire ONTAP 9.11.1 o versione successiva.
- Solo una chiamata attiva di un'operazione Snapshot del gruppo di coerenza è supportata su un'istanza di un gruppo di coerenza alla volta, sia che si tratti di una fase singola che di due fasi. Se si tenta di richiamare un'operazione snapshot mentre è in corso un'altra operazione, si verifica un errore.
- Quando si richiama la creazione snapshot, è possibile impostare un valore di timeout opzionale compreso tra 5 e 120 secondi. Se non viene fornito alcun valore di timeout, l'operazione scade per impostazione predefinita di 7 secondi. Nell'API, impostare il valore di timeout con `action_timeout` parametro.

Nell'interfaccia CLI, utilizzare il `-timeout` allarme.

## Fasi

Puoi completare una snapshot in due fasi con l'API REST o, a cominciare da ONTAP 9.14.1, l'interfaccia a riga di comando di ONTAP. Questa operazione non è supportata in System Manager.



Se si richiama la creazione di Snapshot con l'API, è necessario assegnare la copia Snapshot all'API. Se si richiama la creazione di Snapshot con la CLI, è necessario assegnare la copia Snapshot con la CLI. I metodi di miscelazione non sono supportati.

## CLI

A partire da ONTAP 9.14.1, è possibile creare una copia Snapshot in due fasi utilizzando l'interfaccia a riga di comando.

### Fasi

1. Avviare l'istantanea:

```
consistency-group snapshot start -vserver svm_name -consistency-group  
consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds  
-write-fence {true|false}]
```

2. Verificare che l'istantanea sia stata acquisita:

```
consistency-group snapshot show
```

3. Inserimento dello snapshot:

```
consistency-group snapshot commit svm_name -consistency-group  
consistency_group_name -snapshot snapshot_name
```

## API

1. Richiamare la creazione di Snapshot. Inviare una richiesta POST all'endpoint del gruppo di coerenza utilizzando `action=start` parametro.

```
curl -k -X POST 'https://<IP_address>/application/consistency-  
groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H  
"accept: application/hal+json" -H "content-type: application/json"  
-d '  
{  
  "name": "<snapshot_name>",  
  "consistency_type": "crash",  
  "comment": "<comment>",  
  "snapmirror_label": "<SnapMirror_label>"  
}'
```

2. Se la richiesta POST ha esito positivo, l'output include un uuid snapshot. Utilizzando tale uuid, inviare una richiesta di PATCH per salvare la copia Snapshot.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept: application/hal+json" -H "content-type: application/json"
```

For more information about the ONTAP REST API, see [link:https://docs.netapp.com/us-en/ontap-automation/reference/api\\_reference.html](https://docs.netapp.com/us-en/ontap-automation/reference/api_reference.html) [API reference^] or the [link:https://devnet.netapp.com/restapi.php](https://devnet.netapp.com/restapi.php) [ONTAP REST API page^] at the NetApp Developer Network for a complete list of API endpoints.

## Impostare la protezione remota per un gruppo di coerenza

I gruppi di coerenza offrono protezione remota tramite SM-BC e, a partire da ONTAP 9.13.1, SnapMirror asincrono.

### Configurare la protezione con SM-BC

È possibile utilizzare SM-BC per garantire che le copie Snapshot dei gruppi di coerenza creati nel proprio gruppo di coerenza vengano copiate nella destinazione. Per ulteriori informazioni su SM-BC o su come configurare SM-BC utilizzando la CLI, vedere [Configurare la protezione per la business continuity](#).

### Prima di iniziare

- Non è possibile stabilire relazioni SM-BC sui volumi montati per l'accesso NAS.
- Le etichette dei criteri nel cluster di origine e di destinazione devono corrispondere.
- SM-BC non replica le copie Snapshot per impostazione predefinita, a meno che non venga aggiunta una regola con un'etichetta SnapMirror al predefinito `AutomatedFailOver`. Le copie di policy e Snapshot vengono create con tale etichetta.

Per ulteriori informazioni su questo processo, fare riferimento a ["Proteggere con SM-BC"](#).

- [Implementazioni a cascata](#) Non sono supportati con SM-BC.
- A partire da ONTAP 9.13.1, è possibile eseguire operazioni senza interruzioni [aggiungere volumi a un gruppo di coerenza](#) Con una relazione SM-BC attiva. Qualsiasi altra modifica apportata a un gruppo di coerenza richiede di interrompere la relazione SM-BC, modificare il gruppo di coerenza, quindi ristabilire e risincronizzare la relazione.



Per configurare SM-BC con la CLI, vedere [Proteggere con SM-BC](#).


### Procedura per System Manager

1. Assicurarsi di aver soddisfatto il ["Prerequisiti per l'utilizzo di SM-BC"](#).
2. Selezionare **Storage > Consistency groups**.
3. Selezionare il gruppo di coerenza creato dal menu del gruppo di coerenza.
4. Nella parte superiore destra della pagina panoramica, selezionare **More** (Altro), quindi **Protect** (protezione).
5. System Manager compila automaticamente le informazioni sul lato di origine. Selezionare il cluster e la VM di storage appropriati per la destinazione. Selezionare un criterio di protezione. Assicurarsi che l'opzione



**Inizializza relazione** sia selezionata.

6. Selezionare **Salva**.

7. Il gruppo di coerenza deve essere inizializzato e sincronizzato. Verificare che la sincronizzazione sia stata completata correttamente tornando al menu **Consistency group**. Viene visualizzato lo stato **SnapMirror (Remote)** Protected accanto a. .

### Configurare la protezione asincrona di SnapMirror

A partire da ONTAP 9.13.1, è possibile configurare la protezione SnapMirror asincrona per un singolo gruppo di coerenza. A partire da ONTAP 9.14.1, puoi utilizzare SnapMirror asincrono per replicare le copie Snapshot granulari del volume nel cluster di destinazione usando la relazione del gruppo di coerenza.

#### A proposito di questa attività

Per replicare le copie Snapshot granulari per volume, devi eseguire ONTAP 9.14.1 o versioni successive. Per le policy MirrorAndVault e Vault, l'etichetta SnapMirror della policy di Snapshot granulare per il volume deve corrispondere alla regola dei criteri di SnapMirror del gruppo di coerenza. Gli Snapshot granulari del volume si basano sul valore di mantenimento della policy SnapMirror del gruppo di coerenza, che viene calcolata indipendentemente dagli Snapshot del gruppo di coerenza. Ad esempio, se disponi di una policy per mantenere due copie Snapshot sulla destinazione, puoi disporre di due copie Snapshot granulari del volume e due copie Snapshot del gruppo di coerenza.

Durante la risincronizzazione del rapporto di SnapMirror con le copie Snapshot granulari del volume, puoi conservare le copie Snapshot granulari del volume con il `-preserve` allarme. Le copie Snapshot granulari del volume più recenti delle copie Snapshot del gruppo di coerenza vengono conservate. Se non è presente una copia Snapshot del gruppo di coerenza, non è possibile trasferire copie Snapshot granulari del volume nell'operazione di risincronizzazione.

#### Prima di iniziare

- La protezione asincrona di SnapMirror è disponibile solo per singoli gruppi di coerenza. Non è supportato per i gruppi di coerenza gerarchica. Per convertire un gruppo di coerenza gerarchica in un singolo gruppo di coerenza, vedere [modificare l'architettura del gruppo di coerenza](#).
- Le etichette dei criteri nel cluster di origine e di destinazione devono corrispondere.
- È possibile senza interruzioni [aggiungere volumi a un gruppo di coerenza](#) Con una relazione SnapMirror asincrona attiva. Qualsiasi altra modifica apportata a un gruppo di coerenza richiede di interrompere la relazione SnapMirror, modificare il gruppo di coerenza, quindi ristabilire e risincronizzare la relazione.
- Se è stato configurato un rapporto di protezione SnapMirror asincrono per più singoli volumi, è possibile convertire tali volumi in un gruppo di coerenza mantenendo al contempo le copie Snapshot esistenti. Per convertire correttamente i volumi:
  - Deve essere presente una copia Snapshot comune dei volumi.
  - È necessario interrompere la relazione SnapMirror esistente, [aggiungere i volumi a un singolo gruppo di coerenza](#), quindi risincronizzare la relazione utilizzando il seguente flusso di lavoro.

#### Fasi

1. Dal cluster di destinazione, selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza creato dal menu del gruppo di coerenza.
3. Nella parte superiore destra della pagina panoramica, selezionare **More** (Altro), quindi **Protect** (protezione).
4. System Manager compila automaticamente le informazioni sul lato di origine. Selezionare il cluster e la VM di storage appropriati per la destinazione. Selezionare un criterio di protezione. Assicurarsi che l'opzione


**Inizializza relazione** sia selezionata.

Quando si seleziona un criterio asincrono, è possibile scegliere **Ignora pianificazione trasferimento**.



La pianificazione minima supportata (Recovery Point Objective, o RPO) per i gruppi di coerenza con SnapMirror asincrono è di 30 minuti.

5. Selezionare **Salva**.

6. Il gruppo di coerenza deve essere inizializzato e sincronizzato. Verificare che la sincronizzazione sia stata completata correttamente tornando al menu **Consistency group**. Viene visualizzato lo stato **SnapMirror (Remote)** Protected accanto a .

### Configurare il disaster recovery delle SVM

A partire da ONTAP 9.14.1, [Disaster recovery SVM](#) supporta i gruppi di coerenza per eseguire il mirroring delle informazioni del gruppo di coerenza dall'origine al cluster di destinazione.

Se stai abilitando il disaster recovery delle SVM in una SVM che contiene già un gruppo di coerenza, segui i workflow di configurazione delle SVM per [System Manager](#) o il [CLI ONTAP](#).

Se stai aggiungendo un gruppo di coerenza a una SVM che si trova in una relazione di disaster recovery SVM attiva e funzionante, devi aggiornare la relazione di disaster recovery della SVM dal cluster di destinazione. Per ulteriori informazioni, vedere [Aggiornare manualmente una relazione di replica](#). È necessario aggiornare la relazione ogni volta che si espande il gruppo di coerenza.

### Limitazioni

- Il disaster recovery delle SVM non supporta i gruppi di coerenza gerarchici.
- Il disaster recovery delle SVM non supporta gruppi di coerenza protetti con SnapMirror asincrono. È necessario interrompere il rapporto SnapMirror prima di configurare il disaster recovery delle SVM.
- Entrambi i cluster devono eseguire ONTAP 9.14.1 o versione successiva.
- Le relazioni di fan-out non sono supportate per le configurazioni di disaster recovery delle SVM che contengono gruppi di coerenza.
- Per altri limiti, vedere [limiti del gruppo di coerenza](#).

### Visualizzare le relazioni

System Manager visualizza le mappe LUN nel menu **protezione > Relazioni**. Quando si seleziona una relazione di origine, System Manager visualizza una visualizzazione delle relazioni di origine. Selezionando un volume, è possibile approfondire queste relazioni per visualizzare un elenco delle LUN contenute e delle relazioni del gruppo iniziatore. Queste informazioni possono essere scaricate come cartella di lavoro Excel dalla vista del singolo volume; l'operazione di download viene eseguita in background.

### Informazioni correlate

- ["Clonare un gruppo di coerenza"](#)
- ["Configurare le copie Snapshot"](#)
- ["Creare policy di protezione dei dati personalizzate"](#)
- ["Ripristino da copie Snapshot"](#)
- ["Ripristinare un volume da una copia Snapshot precedente"](#)
- ["Panoramica di SM-BC"](#)

- ["Documentazione sull'automazione ONTAP"](#)
- [Nozioni di base sul disaster recovery asincrono di SnapMirror](#)

## Modificare i volumi membri in un gruppo di coerenza

A partire da ONTAP 9.12.1, è possibile modificare un gruppo di coerenza rimuovendo volumi o aggiungendo volumi (espandendo il gruppo di coerenza). A partire da ONTAP 9.13.1, è possibile spostare i volumi tra i gruppi di coerenza child se condividono un'origine comune.

### Aggiungere volumi a un gruppo di coerenza

A partire da ONTAP 9.12.1, puoi aggiungere volumi senza interruzioni a un gruppo di coerenza.

#### A proposito di questa attività

- Non è possibile aggiungere volumi associati a un altro gruppo di coerenza.
- I gruppi di coerenza supportano i protocolli NAS, SAN e NVMe.
- È possibile aggiungere fino a 16 volumi alla volta a un gruppo di coerenza se le regolazioni sono all'interno del complessivo [limiti del gruppo di coerenza](#).
- A partire da ONTAP 9.13.1, puoi aggiungere volumi senza interruzioni a un gruppo di coerenza con una policy di protezione SnapMirror Business Continuity (SM-BC) o asincrona.
- Quando si aggiungono volumi a un gruppo di coerenza protetto da SM-BC, lo stato della relazione SM-BC cambia in "Expanding" (in espansione) fino a quando il mirroring e la protezione non vengono configurati per il nuovo volume. Se si verifica un disastro sul cluster primario prima del completamento di questo processo, il gruppo di coerenza torna alla sua composizione originale come parte dell'operazione di failover.
- In ONTAP 9.12.1 e versioni precedenti, *non è possibile* aggiungere volumi a un gruppo di coerenza in una relazione SM-BC. È necessario prima interrompere la relazione SM-BC, modificare il gruppo di coerenza, quindi ripristinare la protezione con SM-BC.
- A partire da ONTAP 9.12.1, l'API REST ONTAP supporta l'aggiunta di volumi *nuovi* o esistenti a un gruppo di coerenza. Per ulteriori informazioni sull'API REST di ONTAP, fare riferimento a ["Documentazione di riferimento API REST di ONTAP"](#).

A partire da ONTAP 9.13.1, questa funzionalità è supportata in Gestione sistema.

- Quando si espande un gruppo di coerenza, le copie Snapshot del gruppo di coerenza acquisite prima della modifica saranno considerate parziali. Qualsiasi operazione di ripristino basata su tale copia Snapshot rifletterà il gruppo di coerenza nel momento in cui lo snapshot viene creato.
- Se si utilizza ONTAP da 9.10.1 a 9.11.1, non è possibile modificare un gruppo di coerenza. Per modificare la configurazione di un gruppo di coerenza in ONTAP 9.10.1 o 9.11.1, è necessario eliminare il gruppo di coerenza, quindi creare un nuovo gruppo di coerenza con i volumi che si desidera includere.
- A partire da ONTAP 9.14.1, puoi replicare gli Snapshot granulari del volume nel cluster di destinazione utilizzando SnapMirror asincrono. Quando si espande un gruppo di coerenza utilizzando SnapMirror asincrono, gli Snapshot granulari dei volumi vengono replicati solo dopo aver espanso il gruppo di coerenza quando la policy SnapMirror è MirrorAll o MirrorAndVault. Vengono replicati solo gli Snapshot granulari del volume più recenti rispetto allo Snapshot del gruppo di coerenza di base.
- Se Aggiungi volumi a un gruppo di coerenza in una relazione di disaster recovery della SVM (supportato a partire da ONTAP 9.14.1), devi aggiornare la relazione di disaster recovery della SVM dal cluster di

destinazione dopo aver espanso il gruppo di coerenza. Per ulteriori informazioni, vedere [Aggiornare manualmente una relazione di replica](#).

## Esempio 22. Fasi

### System Manager

A partire da ONTAP 9.12.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera modificare.
3. Se si sta modificando un singolo gruppo di coerenza, nella parte superiore del menu **Volumes** (volumi), selezionare **More** (Altro), quindi **Expand** (Espandi) per aggiungere un volume.

Se si modifica un gruppo di coerenza figlio, identificare il gruppo di coerenza padre che si desidera modificare. Selezionare il pulsante **>** per visualizzare i gruppi di coerenza secondari, quindi selezionare **⋮** accanto al nome del gruppo di coerenza figlio che si desidera modificare. Da questo menu, selezionare **Espandi**.

4. Selezionare fino a 16 volumi da aggiungere al gruppo di coerenza.
5. Selezionare **Salva**. Al termine dell'operazione, visualizzare i volumi aggiunti di recente nel menu **Volumes** del gruppo di coerenza.

### CLI

A partire da ONTAP 9.14.1, è possibile aggiungere volumi a un gruppo di coerenza utilizzando l'interfaccia a riga di comando di ONTAP.

#### Aggiungere volumi esistenti

1. Inserire il seguente comando. Il `-volumes` parameter accetta un elenco di volumi separati da virgole.



Includere solo il `-parent-consistency-group` parametro se il gruppo di coerenza si trova in una relazione gerarchica.

```
consistency-group volume add -vserver svm_name -consistency-group  
consistency_group_name -parent-consistency-group parent_consistency_group  
-volume volumes
```

#### Aggiungere nuovi volumi

La procedura per aggiungere nuovi volumi dipende dal protocollo utilizzato.



Includere solo il `-parent-consistency-group` parametro se il gruppo di coerenza si trova in una relazione gerarchica.

- Per aggiungere nuovi volumi senza esportarli:

```
consistency-group volume create -vserver SVM_name -consistency-group  
child_consistency_group -parent-consistency-group existingParentCg -volume  
volume_name -size size
```

- Per aggiungere nuovi volumi NFS:

```
consistency-group volume create -vserver SVM_name -consistency-group  
consistency_group_name -volume volume-prefix -volume-count number -size  
size -export-policy policy_name
```

- Per aggiungere nuovi volumi SAN:

```
consistency-group volume create -vserver SVM_name -consistency-group  
consistency_group_name -lun lun_name -size size -lun-count number -igroup  
igroup_name
```

- Per aggiungere nuovi namespace NVMe:

```
consistency-group volume create -vserver SVM_name -consistency-group  
consistency_group_name -namespace namespace_name -volume-count number  
-namespace-count number -size size -subsystem subsystem_name
```

## Rimuovere i volumi da un gruppo di coerenza

I volumi rimossi da un gruppo di coerenza non vengono eliminati. Rimangono attivi nel cluster.

### A proposito di questa attività

- Non puoi rimuovere volumi da un gruppo di coerenza in una relazione di disaster recovery SM-BC o SVM. È necessario interrompere prima la relazione SM-BC per modificare il gruppo di coerenza e quindi ristabilire la relazione.
- Se un gruppo di coerenza non contiene volumi dopo l'operazione di rimozione, il gruppo di coerenza viene eliminato.
- Quando un volume viene rimosso da un gruppo di coerenza, le istantanee esistenti del gruppo di coerenza rimangono ma vengono considerate non valide. Le istantanee esistenti non possono essere utilizzate per ripristinare il contenuto del gruppo di coerenza. Le snapshot granulari dei volumi rimangono valide.
- Se si elimina un volume dal cluster, questo viene automaticamente rimosso dal gruppo di coerenza.
- Per modificare la configurazione di un gruppo di coerenza in ONTAP 9.10.1 o 9.11.1, è necessario eliminare il gruppo di coerenza e creare un nuovo gruppo di coerenza con i volumi membro desiderati.
- L'eliminazione di un volume dal cluster comporta la rimozione automatica del gruppo di coerenza.

## System Manager

A partire da ONTAP 9.12.1, è possibile eseguire questa operazione con Gestione sistema.

### Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza singolo o secondario che si desidera modificare.
3. Nel menu **Volumes**, selezionare le caselle di controllo accanto ai singoli volumi che si desidera rimuovere dal gruppo di coerenza.
4. Selezionare **Rimuovi volumi dal gruppo di coerenza**.
5. Confermare che la rimozione dei volumi causerà l'invalidità di tutte le copie Snapshot del gruppo di coerenza e selezionare **Rimuovi**.

### CLI

A partire da ONTAP 9.14.1, puoi rimuovere i volumi da un gruppo di coerenza utilizzando la CLI.

### Fase

1. Rimuovere i volumi. Il `-volumes` parameter accetta un elenco di volumi separati da virgole.

Includere solo il `-parent-consistency-group` parametro se il gruppo di coerenza si trova in una relazione gerarchica.

```
consistency-group volume remove -vserver SVM_name -consistency-group  
consistency_group_name -parent-consistency-group  
parent_consistency_group_name -volume volumes
```

## Spostare i volumi tra i gruppi di coerenza

A partire da ONTAP 9.13.1, è possibile spostare i volumi tra gruppi di coerenza child che condividono un'immagine di origine.

### A proposito di questa attività

- È possibile spostare i volumi solo tra gruppi di coerenza nidificati nello stesso gruppo di coerenza padre.
- Le istantanee del gruppo di coerenza esistente diventano invalide e non più accessibili come snapshot del gruppo di coerenza. Le snapshot dei singoli volumi rimangono valide.
- Le copie Snapshot del gruppo di coerenza padre rimangono valide.
- Se si spostano tutti i volumi da un gruppo di coerenza figlio, tale gruppo di coerenza verrà eliminato.
- Le modifiche apportate a un gruppo di coerenza devono essere rispettate [limiti del gruppo di coerenza](#).

## System Manager

A partire da ONTAP 9.12.1, è possibile eseguire questa operazione con Gestione sistema.

### Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza padre che contiene i volumi che si desidera spostare. Individuare il gruppo di coerenza figlio, quindi espandere il menu **volumi**. Selezionare i volumi che si desidera spostare.
3. Selezionare **Sposta**.
4. Scegliere se spostare i volumi in un nuovo gruppo di coerenza o in un gruppo esistente.
  - a. Per passare a un gruppo di coerenza esistente, selezionare **gruppo di coerenza figlio esistente**, quindi scegliere il nome del gruppo di coerenza dal menu a discesa.
  - b. Per passare a un nuovo gruppo di coerenza, selezionare **nuovo gruppo di coerenza figlio**. Immettere un nome per il nuovo gruppo di coerenza figlio e selezionare un tipo di componente.
5. Selezionare **Sposta**.

### CLI

A partire da ONTAP 9.14.1, puoi spostare i volumi tra gruppi di coerenza utilizzando l'interfaccia a riga di comando di ONTAP.

#### Spostamento dei volumi in un nuovo gruppo di coerenza figlio

1. Il seguente comando crea un nuovo gruppo di coerenza figlio che contiene i volumi designati.

Quando crei il nuovo gruppo di coerenza, puoi designare nuove policy di Snapshot, QoS e tiering.

```
consistency-group volume reassign -vserver SVM_name -consistency-group  
source_child_consistency_group -parent-consistency-group  
parent_consistency_group -volume volumes -new-consistency-group  
consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering  
-policy policy]
```

#### Spostamento dei volumi in un gruppo di coerenza figlio esistente

1. Riassegnare i volumi. Il `-volumes` parameter accetta un elenco separato da virgole di nomi di volumi.

```
consistency-group volume reassign -vserver SVM_name -consistency-group  
source_child_consistency_group -parent-consistency-group  
parent_consistency_group -volume volumes -to-consistency-group  
target_consistency_group
```

## Informazioni correlate

- [Limiti del gruppo di coerenza](#)
- [Clonare un gruppo di coerenza](#)



## Modificare la geometria del gruppo di coerenza

A partire da ONTAP 9.13.1, è possibile modificare la geometria di un gruppo di coerenza. La modifica della geometria di un gruppo di coerenza consente di modificare la configurazione dei gruppi di coerenza figlio o padre senza interrompere le operazioni in corso.

La modifica della geometria del gruppo di coerenza avrà un impatto sulle copie Snapshot esistenti.



Non è possibile modificare la geometria di un gruppo di coerenza configurato con un criterio di protezione remota. È necessario prima interrompere la relazione di protezione, modificare la geometria, quindi ripristinare la protezione remota.

## Aggiungere un nuovo gruppo di coerenza figlio

A partire da ONTAP 9.13.1, è possibile aggiungere un nuovo gruppo di coerenza figlio a un gruppo di coerenza padre esistente.

### Prima di iniziare

- Un gruppo di coerenza padre può contenere un massimo di cinque gruppi di coerenza figlio. Vedere [limiti del gruppo di coerenza](#) per altri limiti.
- Non è possibile aggiungere un gruppo di coerenza figlio a un singolo gruppo di coerenza. Devi prima [\[promuovi\]](#) il gruppo di coerenza, quindi è possibile aggiungere un gruppo di coerenza figlio.
- Le copie Snapshot esistenti del gruppo di coerenza acquisite prima dell'operazione di espansione verranno considerate parziali. Qualsiasi operazione di ripristino basata su tale copia snapshot rifletterà il gruppo di coerenza nel momento in cui la copia Snapshot viene eseguita.

## Esempio 23. Fasi

### System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza padre a cui si desidera aggiungere un gruppo di coerenza figlio.
3. Accanto al nome del gruppo di coerenza padre, selezionare **Altro**, quindi **Aggiungi nuovo gruppo di coerenza figlio**.
4. Immettere un nome per il gruppo di coerenza.
5. Scegliere se si desidera aggiungere volumi nuovi o esistenti.
  - a. Se si stanno aggiungendo volumi esistenti, selezionare **volumi esistenti**, quindi scegliere i volumi dal menu a discesa.
  - b. Se si stanno aggiungendo nuovi volumi, selezionare **nuovi volumi**, quindi specificare il numero di volumi e le relative dimensioni.
6. Selezionare **Aggiungi**.

### CLI

A partire da ONTAP 9.14.1, è possibile aggiungere un gruppo di coerenza figlio utilizzando la CLI di ONTAP.

#### Aggiungere un gruppo di coerenza figlio con nuovi volumi

1. Creare il nuovo gruppo di coerenza. Fornire i valori per il nome del gruppo di coerenza, il prefisso del volume, il numero di volumi, le dimensioni del volume, il servizio di archiviazione, e nome della policy di esportazione:

```
consistency-group create -vserver SVM_name -consistency-group  
consistency_group -parent-consistency-group parent_consistency_group  
-volume-prefix prefix -volume-count number -size size -storage-service  
service -export-policy policy_name
```

#### Aggiungere un gruppo di coerenza figlio con i volumi esistenti

1. Creare il nuovo gruppo di coerenza. Il `volumes` parameter accetta un elenco separato da virgole di nomi di volumi.

```
consistency-group create -vserver SVM_name -consistency-group  
new_consistency_group -parent-consistency-group parent_consistency_group  
-volumes volume
```

## Scollegare un gruppo di coerenza figlio

A partire da ONTAP 9.13.1, è possibile rimuovere un gruppo di coerenza figlio dal relativo gruppo padre, convertendolo in un singolo gruppo di coerenza.

### Prima di iniziare

- La rimozione di un gruppo di coerenza figlio causa l'invalidità e l'inaccessibilità degli snapshot del gruppo di coerenza padre. Gli snapshot granulari del volume rimangono validi.

- Le copie Snapshot esistenti del singolo gruppo di coerenza rimangono valide.
- Questa operazione non riesce se esiste un singolo gruppo di coerenza esistente con lo stesso nome del gruppo di coerenza figlio che si intende scollegare. Se si verifica questo scenario, è necessario rinominare il gruppo di coerenza quando lo si scollega.

## Esempio 24. Fasi

### System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza padre che contiene il figlio che si desidera scollegare.
3. Accanto al gruppo di coerenza figlio che si desidera scollegare, selezionare **Altro**, quindi **Scollega dall'origine**.
4. Facoltativamente, rinominare il gruppo di coerenza e selezionare un tipo di applicazione.
5. Selezionare **stacca**.

### CLI

A partire da ONTAP 9.14.1, è possibile scollegare un gruppo di coerenza figlio utilizzando l'interfaccia a riga di comando di ONTAP.

1. Staccare il gruppo di coerenza. Facoltativamente, rinominare il gruppo di coerenza autonomo con `-new-name` parametro.

```
consistency-group detach -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group parent_consistency_group
[-new-name new_name]
```

## Sposta un singolo gruppo di coerenza esistente in un gruppo di coerenza di origine

A partire da ONTAP 9.13.1, è possibile convertire un singolo gruppo di coerenza esistente in un gruppo di coerenza figlio. È possibile spostare il gruppo di coerenza in un gruppo di coerenza padre esistente o creare un nuovo gruppo di coerenza padre durante l'operazione di spostamento.

### Prima di iniziare

- Il gruppo di coerenza padre deve avere un massimo di quattro figli. Un gruppo di coerenza padre può contenere un massimo di cinque gruppi di coerenza figlio. Vedere [limiti del gruppo di coerenza](#) per altri limiti.
- Le copie Snapshot esistenti del gruppo di coerenza *padre* catturate prima di questa operazione saranno considerate parziali. Qualsiasi operazione di ripristino basata su una di queste copie Snapshot rifletterà il gruppo di coerenza nel momento in cui la copia Snapshot viene eseguita.
- Le snapshot dei gruppi di coerenza esistenti del singolo gruppo di coerenza rimangono valide.

## Esempio 25. Fasi

### System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera convertire.
3. Selezionare **Altro**, quindi **spostarsi in un gruppo di coerenza diverso**.
4. Facoltativamente, immettere un nuovo nome per il gruppo di coerenza e selezionare un tipo di componente. Per impostazione predefinita, il tipo di componente sarà altro.
5. Scegliere se si desidera migrare a un gruppo di coerenza padre esistente o creare un nuovo gruppo di coerenza padre:
  - a. Per migrare a un gruppo di coerenza padre esistente, selezionare **gruppo di coerenza esistente**, quindi scegliere il gruppo di coerenza dal menu a discesa.
  - b. Per creare un nuovo gruppo di coerenza padre, selezionare **nuovo gruppo di coerenza**, quindi specificare un nome per il nuovo gruppo di coerenza.
6. Selezionare **Sposta**.

### CLI

A partire da ONTAP 9.14.1, puoi spostare un singolo gruppo di coerenza sotto un gruppo di coerenza di origine utilizzando l'interfaccia a riga di comando di ONTAP.

#### Spostare un gruppo di coerenza in un nuovo gruppo di coerenza di origine

1. Creare il nuovo gruppo di coerenza di origine. Il `-consistency-groups` il parametro migrerà tutti i gruppi di coerenza esistenti al nuovo padre.

```
consistency-group attach -vserver svm_name -consistency-group  
parent_consistency_group -consistency-groups child_consistency_group
```

#### Spostare un gruppo di coerenza in un gruppo di coerenza esistente

1. Spostare il gruppo di coerenza:

```
consistency-group add -vserver SVM_name -consistency-group  
consistency_group -parent-consistency-group parent_consistency_group
```

## Promuovere un gruppo di coerenza figlio

A partire da ONTAP 9.13.1, puoi promuovere un singolo gruppo di coerenza in un gruppo di coerenza di origine. Quando si promuove un singolo gruppo di coerenza a un gruppo padre, si crea anche un nuovo gruppo di coerenza figlio che eredita tutti i volumi nel singolo gruppo di coerenza originale.

### Prima di iniziare

- Se si desidera convertire un gruppo di coerenza figlio in un gruppo di coerenza padre, è necessario innanzitutto [\[detach\]](#) il gruppo di coerenza figlio quindi seguire questa procedura.
- Le copie Snapshot esistenti del gruppo di coerenza rimangono valide dopo la promozione del gruppo di coerenza.

## Esempio 26. Fasi

### System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera promuovere.
3. Selezionare **Altro**, quindi **Promuovi al gruppo di coerenza padre**.
4. Inserire un **Nome** e selezionare un **tipo di componente** per il gruppo di coerenza figlio.
5. Selezionare **Promuovi**.

### CLI

A partire da ONTAP 9.14.1, puoi spostare un singolo gruppo di coerenza sotto un gruppo di coerenza di origine utilizzando l'interfaccia a riga di comando di ONTAP.

1. Promuovere il gruppo di coerenza. Questo comando creerà un gruppo di coerenza principale e un gruppo secondario.

```
consistency-group promote -vserver SVM_name -consistency-group  
existing_consistency_group -new-name new_child_consistency_group
```

## Consente di declassare un padre in un singolo gruppo di coerenza

A partire da ONTAP 9.13.1, puoi demotare un gruppo di coerenza di origine in un singolo gruppo di coerenza. Il deeming del padre appiattisce la gerarchia del gruppo di coerenza, rimuovendo tutti i gruppi di coerenza figlio associati. Tutti i volumi nel gruppo di coerenza rimarranno nel nuovo gruppo di coerenza singolo.

### Prima di iniziare

- Le copie Snapshot esistenti del gruppo di coerenza padre rimangono valide dopo essere state retrocesse a una singola coerenza. Le copie Snapshot esistenti di uno qualsiasi dei gruppi di coerenza figlio associati di quel padre diventeranno non valide, ma le singole snapshot dei volumi al loro interno continuano ad essere accessibili come snapshot granulari dei volumi.

## Esempio 27. Fasi

### System Manager

A partire da ONTAP 9.13.1, è possibile eseguire questa operazione con Gestione sistema.

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza padre che si desidera declassare.
3. Selezionare **Altro**, quindi **Demodi a singolo gruppo di coerenza**.
4. Un avviso informa che tutti i gruppi di coerenza figlio associati verranno eliminati e i relativi volumi verranno spostati nel nuovo gruppo di coerenza singolo. Selezionare **Demote** per confermare di aver compreso l'impatto.

### CLI

A partire da ONTAP 9.14.1, puoi demotizzare un gruppo di coerenza utilizzando l'interfaccia a riga di comando di ONTAP.

1. Demotare il gruppo di coerenza. Utilizzare l'opzione `-new-name` parametro per rinominare il gruppo di coerenza.

```
consistency-group demote -vserver SVM_name -consistency-group  
parent_consistency_group [-new-name new_consistency_group_name]
```

## Modificare i tag dell'applicazione e del componente

A partire da ONTAP 9.12.1, i gruppi di coerenza supportano l'etichettatura di componenti e applicazioni. I tag di applicazioni e componenti sono uno strumento di gestione che consente di filtrare e identificare diversi carichi di lavoro nei gruppi di coerenza.

### A proposito di questa attività

I gruppi di coerenza offrono due tipi di tag:

- **Tag applicazione:** Si applicano ai singoli gruppi di coerenza e ai gruppi di coerenza padre. I tag applicativi forniscono l'etichettatura per carichi di lavoro come MongoDB, Oracle o SQL Server. Il tag di applicazione predefinito per i gruppi di coerenza è **Altro**.
- **Tag dei componenti:** I figli nei gruppi di coerenza gerarchica hanno tag dei componenti invece di tag delle applicazioni. Le opzioni per i tag dei componenti sono "dati", "registri" o "Altro". Il valore predefinito è Other (Altro).

È possibile applicare tag durante la creazione di gruppi di coerenza o dopo la creazione di gruppi di coerenza.




Se il gruppo di coerenza ha una relazione SM-BC, è necessario utilizzare **Altro** come tag dell'applicazione o del componente.

### Fasi

A partire da ONTAP 9.12.1, è possibile modificare i tag delle applicazioni e dei componenti utilizzando Gestione di sistema. A partire da ONTAP 9.14.1, è possibile modificare i tag delle applicazioni e dei componenti utilizzando l'interfaccia CLI di ONTAP.

## System Manager

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza di cui si desidera modificare il tag. Selezionare  Accanto al nome del gruppo di coerenza, quindi **Modifica**.
3. Nel menu a discesa, scegliere l'applicazione o il tag del componente appropriato.
4. Selezionare **Salva**.

## CLI

A partire da ONTAP 9.14.1, è possibile modificare l'applicazione o il tag del componente di un gruppo di coerenza esistente utilizzando l'interfaccia CLI di ONTAP.

### Modificare il tag dell'applicazione

1. I tag dell'applicazione accettano un numero limitato di stringhe preimpostate. Per vedere, l'elenco accettato di stringhe, eseguire il comando seguente:

```
consistency-group modify -vserver svm_name -consistency-group  
consistency_group -application-type ?
```

2. Scegliere la stringa appropriata dall'output, quindi modificare il gruppo di coerenza:

```
consistency-group modify -vserver svm_name -consistency-group  
consistency_group -application-type application_type
```

### Modificare il tag del componente

1. Modificare il tipo di componente. Il tipo di componente può essere dati, registri o altro. Se si utilizza SM-BC, deve essere "Altro".

```
consistency-group modify -vserver svm -consistency-group  
child_consistency_group -parent-consistency-group parent_consistency_group  
-application-component-type [data|logs|other]
```

## Clonare un gruppo di coerenza

A partire da ONTAP 9.12.1, è possibile clonare un gruppo di coerenza per creare una copia di un gruppo di coerenza e del relativo contenuto. La clonazione di un gruppo di coerenza crea una copia della configurazione del gruppo di coerenza, dei relativi metadati come il tipo di applicazione e di tutti i volumi e i relativi contenuti come file, directory, LUN o spazi dei nomi NVMe.

### A proposito di questa attività

Durante la clonazione di un gruppo di coerenza, è possibile clonarlo con la configurazione corrente, ma con il contenuto del volume così come sono o in base a un gruppo di coerenza esistente Snapshot.

La clonazione di un gruppo di coerenza è supportata solo per l'intero gruppo di coerenza. Non è possibile clonare un singolo gruppo di coerenza figlio in una relazione gerarchica: È possibile clonare solo la configurazione completa del gruppo di coerenza.

Quando si clonano gruppi di coerenza, i seguenti componenti non vengono clonati:

- IGroups
- Mappe LUN

- Sottosistemi NVMe
- Mappe dei sottosistemi dello spazio dei nomi NVMe

#### **Prima di iniziare**

- Quando si clonano gruppi di coerenza, ONTAP non crea condivisioni SMB per i volumi clonati se non viene specificato un nome di condivisione. \* I gruppi di coerenza clonati non vengono montati se non viene specificato un percorso di giunzione.
- Se si tenta di clonare un gruppo di coerenza basato su un'istantanea che non riflette i volumi costituenti correnti del gruppo di coerenza, l'operazione non verrà eseguita correttamente.
- Dopo aver clonato un gruppo di coerenza, è necessario eseguire l'operazione di mappatura appropriata.

Fare riferimento a [Mappare igroups a più LUN](#) oppure [Mappare uno spazio dei nomi NVMe in un sottosistema](#) per ulteriori informazioni.

- La clonazione di un gruppo di coerenza non è supportata per un gruppo di coerenza in una relazione di Business Continuity SnapMirror o con qualsiasi volume DP associato.



## System Manager

### Fasi

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera clonare dal menu **Consistency Group**.
3. Nella parte superiore destra della pagina panoramica del gruppo di coerenza, selezionare **Clone**.
4. Immettere un nome per il nuovo gruppo di coerenza clonato o accettare il nome predefinito.
  - a. Scegliere se si desidera attivare **"Thin Provisioning"**.
  - b. Scegliere **Split Clone** se si desidera separare il gruppo di coerenza dall'origine e allocare ulteriore spazio su disco per il gruppo di coerenza clonato.
5. Per clonare il gruppo di coerenza nello stato corrente, scegliere **Aggiungi una nuova copia Snapshot**.

Per clonare il gruppo di coerenza in base a uno snapshot, scegliere **Usa una copia Snapshot esistente**. Selezionando questa opzione si apre un nuovo sottomenu. Scegliere l'istantanea che si desidera utilizzare come base per l'operazione di clonazione.

6. Selezionare **Clone**.
7. Tornare al menu **Consistency Group** per confermare che il gruppo di coerenza è stato clonato.

### CLI

A partire da ONTAP 9.14.1, è possibile clonare un gruppo di coerenza utilizzando la CLI.

#### Clonare un gruppo di coerenza

1. Il `consistency-group clone create` command clona il gruppo di coerenza al suo stato corrente point-in-time. Per basare l'operazione di cloning su uno Snapshot, includere il `-source-snapshot` parametro.

```
consistency-group clone create -vserver svm_name -consistency-group clone_name -source-consistency-group consistency_group_name [-source-snapshot snapshot_name]
```

### Passi successivi

- [Mappare igroups a più LUN](#)
- [Mappare uno spazio dei nomi NVMe in un sottosistema](#)

## Eliminare un gruppo di coerenza

Se si decide di non avere più bisogno di un gruppo di coerenza, è possibile eliminarlo.


### A proposito di questa attività

- L'eliminazione di un gruppo di coerenza elimina l'istanza del gruppo di coerenza e *non* influisce sui volumi o sui LUN costituenti. L'eliminazione di un gruppo di coerenza non comporta l'eliminazione delle istantanee presenti su ciascun volume, ma non sarà più accessibile come snapshot del gruppo di coerenza. Tuttavia, gli Snapshot possono continuare a essere gestiti come normali snapshot granulari del volume.
- ONTAP elimina automaticamente un gruppo di coerenza se tutti i volumi del gruppo vengono eliminati.

- L'eliminazione di un gruppo di coerenza principale comporta l'eliminazione di tutti i gruppi di coerenza secondari associati.
- Se si utilizza una versione di ONTAP compresa tra 9.10.1 e 9.12.0, i volumi possono essere rimossi da un gruppo di coerenza solo se il volume stesso viene cancellato, nel qual caso il volume viene automaticamente rimosso dal gruppo di coerenza. A partire da ONTAP 9.12.1, è possibile rimuovere i volumi da un gruppo di coerenza senza eliminare tale gruppo. Per ulteriori informazioni su questo processo, fare riferimento a [Modificare un gruppo di coerenza](#).

## Esempio 28. Fasi

### System Manager

1. Selezionare **Storage > Consistency groups**.
2. Selezionare il gruppo di coerenza che si desidera eliminare.
3. Accanto al nome del gruppo di coerenza, selezionare  Quindi **Elimina**.

### CLI

A partire da ONTAP 9.14.1, è possibile eliminare un gruppo di coerenza utilizzando l'interfaccia CLI.

### Eliminare un gruppo di coerenza

1. Eliminare il gruppo di coerenza:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

## Continuità aziendale di SnapMirror

### Panoramica di SnapMirror Business Continuity

SnapMirror Business Continuity (SM-BC), noto anche come SnapMirror Active Sync, permette ai servizi di business di continuare a funzionare anche attraverso un guasto completo del sito, supportando le applicazioni per il failover in modo trasparente utilizzando una copia secondaria. Per attivare un failover con SM-BC non sono richiesti né interventi manuali né script aggiuntivi.

SM-BC è disponibile a partire da ONTAP 9.8. SM-BC è supportato su cluster AFF o cluster ASA (All-Flash SAN Array), in cui i cluster primari e secondari possono essere AFF o ASA. SM-BC protegge le applicazioni con LUN iSCSI o FCP.

### Benefici

SM-BC offre i seguenti vantaggi:

- Disponibilità continua per applicazioni business-critical
- Possibilità di ospitare applicazioni critiche in modo alternato dal sito primario e secondario
- Gestione semplificata delle applicazioni mediante gruppi di coerenza per una coerenza dipendente dell'ordine di scrittura
- Possibilità di testare il failover per ciascuna applicazione

- Creazione istantanea di cloni mirror senza impatto sulla disponibilità delle applicazioni
- A partire da ONTAP 9.11.1, SM-BC supporta [SnapRestore a file singolo](#).
- A partire da ONTAP 9.14.1, SM-BC supporta Windows failover Clustering e. ["Prenotazioni permanenti SCSI 3"](#), migliorando l'alta disponibilità.

## Casi di utilizzo

### Implementazione dell'applicazione per RTO (Zero Recovery Time Object)

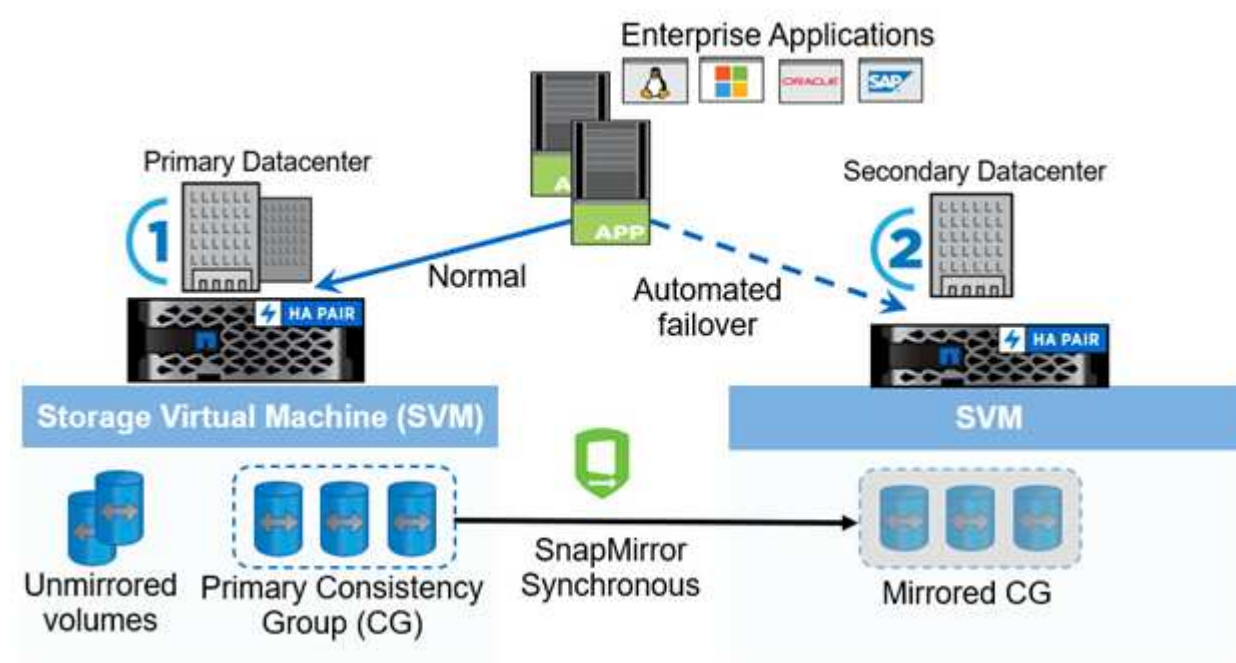
In un'implementazione SM-BC, si disporrà di un cluster primario e secondario. Un LUN nel cluster primario (L1P) avrà un mirror (L1S) Sul secondario; entrambi i LUN condividono lo stesso ID seriale e vengono riportati come LUN di lettura/scrittura sull'host. Tuttavia, le operazioni di lettura e scrittura vengono servite solo al LUN primario, L1P. Any scrive nel mirror L1S sono serviti dal proxy.

### Scenario di disastro

Con SM-BC, è possibile replicare in modo sincrono più volumi per un'applicazione tra siti in ubicazioni geograficamente distribuite. È possibile eseguire automaticamente il failover sulla copia secondaria in caso di interruzione del primario, consentendo così la business continuity per le applicazioni di primo livello.

## Architettura

La figura seguente illustra il funzionamento della funzione di continuità aziendale di SnapMirror a un livello elevato.



Nella sezione uno del diagramma, un'applicazione viene implementata su una SVM nel data center primario. I volumi che sono stati aggiunti al gruppo di coerenza primario sono protetti con SM-BC e vengono mirrorati nel gruppo di coerenza secondario di un data center secondario. In caso di interruzione, i volumi nel gruppo di coerenza primario effettueranno il failover nel gruppo di coerenza mirrorato. I volumi non appartenenti a un gruppo di coerenza mirrorato non vengono serviti in caso di failover.

## Ulteriori informazioni

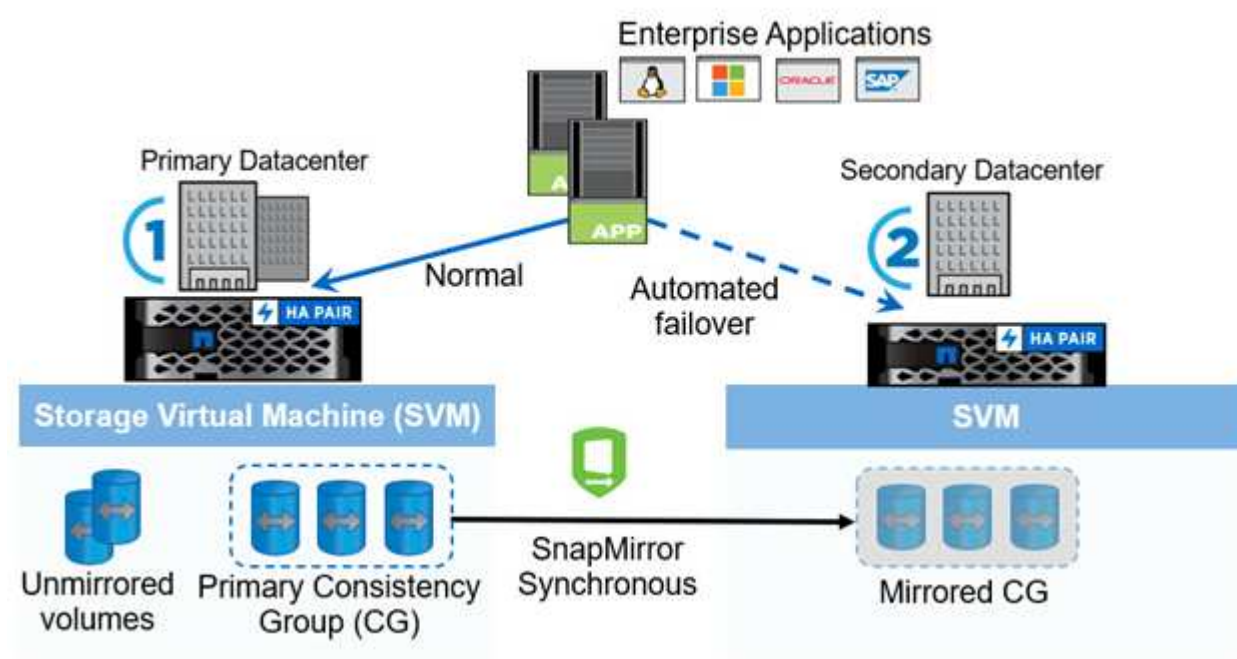
- ["TR-4878: Business continuity SnapMirror"](#)

## Concetti chiave

La business continuity SnapMirror (SM-BC) utilizza funzionalità come i gruppi di coerenza e il mediatore ONTAP per garantire la replica e il servizio dei dati anche in caso di disastro. Durante la pianificazione dell'implementazione di SM-BC, è importante comprendere i concetti essenziali di SM-BC e della relativa architettura.

## Architettura

La figura seguente illustra una panoramica di alto livello di un'implementazione SM-BC.



Il diagramma mostra un'applicazione aziendale ospitata su una VM di storage (SVM) nel data center primario. La SVM contiene cinque volumi, tre dei quali fanno parte di un gruppo di coerenza. I tre volumi nel gruppo di coerenza vengono mirrorati in un data center secondario. In circostanze normali, tutte le operazioni di scrittura vengono eseguite sul data center primario; in effetti, questo data center funge da origine per le operazioni di i/o, mentre il data center secondario funge da destinazione.

In caso di disastro nel data center primario, il mediatore ONTAP indirizzerà il data center secondario a fungere da principale, servendo tutte le operazioni di i/o. Verranno serviti solo i volumi di cui è stato eseguito il mirroring nel gruppo di coerenza. Qualsiasi operazione relativa agli altri due volumi sulla SVM sarà interessata dall'evento di disastro.

## Concetti essenziali

La comprensione dei seguenti termini ti aiuterà a implementare SM-BC.

### Gruppo di coerenza

Un gruppo di coerenza è un insieme di volumi o LUN che forniscono una garanzia di coerenza dell'ordine di

scrittura per il carico di lavoro dell'applicazione che deve essere protetto per la business continuity. Un gruppo di coerenza garantisce che tutti i volumi di questo set di dati vengano disattivati e quindi sottoposti a snap nello stesso momento, fornendo un punto di ripristino coerente con i dati tra i volumi per quel set di dati.

In SM-BC, creerai un gruppo di coerenza primario e secondario per la replica e la protezione dei dati. Il gruppo di coerenza secondario servirà i dati in caso di interruzione.

Per ulteriori informazioni sui gruppi di coerenza, vedere ["Panoramica dei gruppi di coerenza"](#).

### **Costituente**

Un singolo volume o LUN che fa parte di un gruppo di coerenza, protetto dalla relazione SM-BC.

### **Mediatore ONTAP**

I mediatori ONTAP monitorano i due cluster ONTAP e orchestrano il failover in caso di guasto del sistema di storage primario. Con il mediatore ONTAP, l'applicazione si ricollega automaticamente alle risorse del sistema di storage secondario.

Con le informazioni sullo stato di salute del mediatore ONTAP, i cluster possono distinguere tra guasto LIF intercluster e guasto del sito. Quando il sito non funziona, ONTAP Mediator trasmette on-demand le informazioni sullo stato di salute al cluster peer, facilitando il cluster peer al failover.

Scopri di più su ["Mediatore ONTAP"](#).

### **Failover pianificato**

Un'operazione manuale per modificare i ruoli delle copie in una relazione SM-BC. I siti primari diventano i secondari, mentre i siti secondari diventano quelli primari.

### **Failover automatico non pianificato (AUFO)**

Un'operazione automatica per eseguire un failover sulla copia mirror. L'operazione richiede l'assistenza di Mediator per rilevare che la copia principale non è disponibile.

### **Fuori sincronizzazione (OOS)**

Quando l'i/o dell'applicazione non viene replicato nel sistema di storage secondario, viene segnalato come **fuori sincronizzazione**. Uno stato fuori sincronizzazione indica che i volumi secondari non sono sincronizzati con il primario (origine) e che la replica di SnapMirror non avviene.

Se lo stato mirror è `Snapmirrored`, indica un errore di trasferimento o un errore dovuto a un'operazione non supportata.

### **RPO zero**

RPO è l'acronimo di Recovery Point Objective, ovvero la quantità di perdita di dati ritenuta accettabile in un determinato periodo di tempo. Zero RPO indica che non è accettabile alcuna perdita di dati.

### **RTO zero**

RTO è l'acronimo di Recovery Time Objective (obiettivo tempo di ripristino), ovvero il tempo ritenuto accettabile per il ritorno di un'applicazione alle normali operazioni in seguito a un'interruzione, un guasto o un altro evento di perdita di dati. Zero RTO significa che non è accettabile alcun downtime.

## **Pianificare**

### **Prerequisiti**

Durante la pianificazione dell'implementazione di SnapMirror Business Continuity,

assicurarsi di aver soddisfatto i diversi requisiti di configurazione hardware, software e di sistema.

#### Hardware

- Sono supportati solo cluster ha a due nodi
- Entrambi i cluster devono essere AFF (incluso AFF C-Series) o ASA (senza combinazione)

#### Software

- ONTAP 9.8 o versione successiva
- Mediatore ONTAP 1.2 o versione successiva
- Un server Linux o una macchina virtuale per il mediatore ONTAP che esegue una delle seguenti operazioni:

| Versione del mediatore ONTAP | Versioni Linux supportate                                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1,7                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3</li><li>• Rocky Linux 8 e 9</li></ul>         |
| 1.6                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1, 9.2</li><li>• Rocky Linux 8 e 9</li></ul>               |
| 1.5                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul> |
| 1.4                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul> |
| 1.3                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul>           |
| 1.2                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1</li><li>• CentOS: 7.6, 7.7, 7.8</li></ul>                               |

#### Licensing

- La licenza SnapMirror Synchronous (SM-S) deve essere applicata a entrambi i cluster
- La licenza SnapMirror deve essere applicata su entrambi i cluster



Se i sistemi storage ONTAP sono stati acquistati prima di giugno 2019, vedere ["Chiavi di licenza master NetApp ONTAP"](#) Per ottenere la licenza SM-S richiesta.

La licenza SnapMirror sincrona e SnapMirror è inclusa in ["ONTAP uno"](#).

## Ambiente di rete

- Il tempo di round trip (RTT) di latenza tra cluster deve essere inferiore a 10 millisecondi.
- Le prenotazioni persistenti SCSI-3 sono **non** supportate con SM-BC .

## Protocolli supportati

- Sono supportati solo i protocolli SAN (non NFS/SMB).
- Sono supportati solo i protocolli Fibre Channel e iSCSI.
- L'IPSpace predefinito è richiesto da SM-BC per le relazioni peer del cluster. IPspace personalizzato non supportato.

## Sicurezza NTFS

Lo stile di sicurezza NTFS **non** è supportato sui volumi SM-BC.

## Mediatore ONTAP

- Il provisioning del mediatore ONTAP viene eseguito esternamente e collegato a ONTAP per il failover trasparente delle applicazioni.
- Per essere pienamente funzionale e per abilitare il failover automatico non pianificato, il mediatore ONTAP esterno deve essere fornito e configurato con cluster ONTAP.
- Il supporto ONTAP deve essere installato in un terzo dominio di errore, separato dai due cluster ONTAP.
- Quando si installa il mediatore ONTAP, è necessario sostituire il certificato autofirmato con un certificato valido firmato da una CA mainstream affidabile.
- Per ulteriori informazioni sul mediatore ONTAP, vedere ["Preparare l'installazione del servizio ONTAP Mediator"](#).

## Volumi di destinazione in lettura/scrittura

- Le relazioni SM-BC non sono supportate sui volumi di destinazione in lettura/scrittura. Prima di poter utilizzare un volume di lettura/scrittura, è necessario convertirlo in un volume DP creando una relazione SnapMirror a livello di volume ed eliminando la relazione. Per ulteriori informazioni, vedere ["Conversione delle relazioni esistenti in relazioni SM-BC"](#)

## Grandi LUN e grandi volumi

Il supporto per LUN di grandi dimensioni e grandi volumi (superiori a 100 TB) dipende dalla versione di ONTAP in uso e dalla piattaforma.



### ONTAP 9.12.1P2 e versioni successive

- Per ONTAP 9.12.1 P2 e versioni successive, SMBC supporta LUN di grandi dimensioni e volumi superiori a 100 TB su ASA e AFF (inclusa la serie C).



Per le versioni ONTAP 9.12.1P2 e successive, è necessario assicurarsi che i cluster primario e secondario siano All-Flash SAN Array o All Flash Array e che abbiano installato ONTAP 9.12.1 P2 o versione successiva. Se il cluster secondario esegue una versione precedente a ONTAP 9.12.1P2 o se il tipo di array non è lo stesso del cluster primario, la relazione sincrona può uscire dalla sincronizzazione se il volume primario supera i 100 TB.

### ONTAP 9.8 - 9.12.1P1

- Per le release ONTAP tra ONTAP 9,8 e 9.12.1 P1 (incluse), LUN di grandi dimensioni e volumi maggiori di 100TB TB sono supportati solo sugli array SAN all-flash.



Per le release ONTAP tra ONTAP 9,8 e 9.12.1 P2, è necessario verificare che i cluster primario e secondario siano array SAN all-flash e che abbiano installato ONTAP 9,8 o versione successiva. Se il cluster secondario esegue una versione precedente a ONTAP 9,8 o se non si tratta di un array All-Flash SAN, la relazione sincrona può disattivarsi se il volume primario cresce oltre 100 TB.

### Ulteriori informazioni

- ["Hardware Universe"](#)
- ["Panoramica del mediatore ONTAP"](#)

### Configurazioni e funzionalità supportate

La Business Continuity di SnapMirror è compatibile con numerosi sistemi operativi e altre funzionalità di ONTAP. Scopri i dettagli e le configurazioni consigliate.

#### Configurazioni supportate

SM-BC è supportato da numerosi sistemi operativi, tra cui:

- AIX (a partire da ONTAP 9.11.1)
- HP-UX (a partire da ONTAP 9.10.1)
- Solaris 11.4 (a partire da ONTAP 9.10.1)

#### AIX

A partire da ONTAP 9.11.1, AIX è supportato con SM-BC. Con una configurazione AIX, il cluster primario è il cluster "attivo".

In una configurazione AIX, i failover sono disruptive. Con ogni failover, sarà necessario eseguire una nuova scansione sull'host per riprendere le operazioni di i/O.

Per configurare l'host AIX con SM-BC, consultare l'articolo della Knowledge base ["Come configurare un host AIX per SnapMirror Business Continuity \(SM-BC\)"](#).



## HP-UX

A partire da ONTAP 9.10.1, è supportato SM-BC per HP-UX.

### Limitazioni con HP-UX

Un evento di failover automatico non pianificato (AUFO) sul cluster master isolato può essere causato da un guasto a due eventi quando viene persa la connessione tra il cluster primario e quello secondario e viene persa anche la connessione tra il cluster primario e il mediatore. Questo è considerato un evento raro, a differenza di altri eventi AUFO.

- In questo scenario, potrebbero essere necessari più di 120 secondi per il ripristino dell'i/o sull'host HP-UX. A seconda delle applicazioni in esecuzione, questo potrebbe non causare interruzioni i/o o messaggi di errore.
- Per risolvere il problema, è necessario riavviare le applicazioni sull'host HP-UX che hanno una tolleranza di interruzione inferiore a 120 secondi.

### Consigli per l'impostazione degli host Solaris

A partire da ONTAP 9.10.1, SM-BC supporta Solaris 11.4.

Per garantire che le applicazioni client Solaris non siano disgregative quando si verifica uno switchover di failover del sito non pianificato in un ambiente SM-BC, modificare le impostazioni predefinite del sistema operativo Solaris. Per configurare Solaris con le impostazioni consigliate, consultare l'articolo della Knowledge base ["Impostazioni consigliate per il supporto degli host Solaris nella configurazione di SnapMirror Business Continuity \(SM-BC\)"](#).

### Clustering di failover Windows

A partire da ONTAP 9.14.1, il clustering di failover Windows è supportato con SM-BC. Per ulteriori informazioni, vedere ["TR-4878: Business continuity SnapMirror"](#).

### Integrazioni ONTAP

SM-BC offre supporto per altre funzionalità di ONTAP, tra cui:

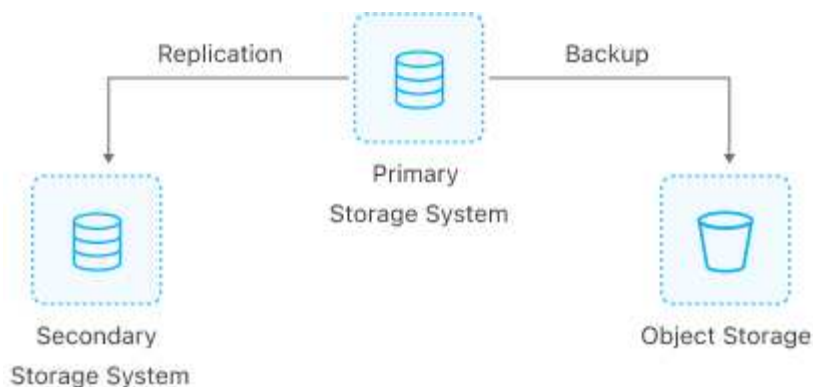
- Configurazioni fan-out
- Copia NDMP (a partire da ONTAP 9.13.1)
- Ripristino parziale dei file (a partire da ONTAP 9.12.1)

### FabricPool

SM-BC supporta i volumi di origine e di destinazione sugli aggregati FabricPool con la policy di tiering None (Nessuno), Snapshot (Snapshot) o Auto (automatico). SM-S SM-BC non supporta gli aggregati FabricPool che utilizzano una policy di tiering di tutti.

### Configurazioni fan-out

In una [configurazioni fan-out](#), È possibile eseguire il mirroring del volume di origine su un endpoint di destinazione SM-BC e su una o più relazioni SnapMirror asincrone.



SM-BC supporta [configurazioni fan-out](#) con `MirrorAllSnapshots E`, a partire da ONTAP 9.11.1, il `MirrorAndVault` policy. Le configurazioni fan-out non sono supportate in SM-BC con `XDPDefault` policy.

Se si verifica un failover sulla destinazione SM-BC in una configurazione fan-out, è necessario manualmente [ripristinare la protezione nella configurazione fan-out](#).

### Ripristino NDMP

A partire da ONTAP 9.13.1, è possibile utilizzare NDMP per copiare e ripristinare i dati con SM-BC. L'utilizzo di NDMP consente di spostare i dati nell'origine SM-BC per completare un ripristino senza interrompere la protezione. Questo è particolarmente utile nelle configurazioni fan-out.

Per ulteriori informazioni su questo processo, vedere [Trasferire i dati utilizzando la copia ndmp](#).

### Ripristino parziale del file

A partire da ONTAP 9.12.1, il ripristino parziale del LUN è supportato per i volumi SM-BC. Per informazioni su questo processo, fare riferimento a. "[Ripristinare parte di un file da una copia Snapshot](#)".

### Limiti a oggetti per la business continuity di SnapMirror

Durante la preparazione all'utilizzo e alla gestione di SnapMirror Business Continuity, tenere presenti le seguenti limitazioni.

#### Gruppi di coerenza in un cluster

I limiti dei gruppi di coerenza per un cluster con SM-BC vengono calcolati in base alle relazioni e dipendono dalla versione di ONTAP utilizzata. I limiti sono indipendenti dalla piattaforma.

| Versione di ONTAP                  | Numero massimo di relazioni |
|------------------------------------|-----------------------------|
| ONTAP 9.8-9.9.1                    | 5                           |
| ONTAP 9.10.1                       | 20                          |
| ONTAP 9.11.1 e versioni successive | 50                          |

#### Volumi per gruppo di coerenza

Il numero massimo di volumi per gruppo di coerenza con SM-BC è indipendente dalla piattaforma.

| Versione di ONTAP                  | Numero massimo di volumi supportati in una relazione di gruppo di coerenza |
|------------------------------------|----------------------------------------------------------------------------|
| ONTAP 9.8-9.9.1                    | 12                                                                         |
| ONTAP 9.10.1 e versioni successive | 16                                                                         |

## Volumi

I limiti di volume in SM-BC vengono calcolati in base al numero di endpoint, non al numero di relazioni. Un gruppo di coerenza con 12 volumi contribuisce a 12 endpoint sul cluster primario e secondario. Le relazioni sincroni di SM-BC e SnapMirror contribuiscono al numero totale di endpoint.

Nella tabella seguente sono inclusi gli endpoint massimi per piattaforma.

| S. No | Piattaforma | Endpoint per ha per SM-BC |              |                                    | Endpoint di sincronizzazione generale e SM-BC per ha |              |                                    |
|-------|-------------|---------------------------|--------------|------------------------------------|------------------------------------------------------|--------------|------------------------------------|
|       |             | ONTAP 9.8-9.9.1           | ONTAP 9.10.1 | ONTAP 9.11.1 e versioni successive | ONTAP 9.8-9.9.1                                      | ONTAP 9.10.1 | ONTAP 9.11.1 e versioni successive |
| 1     | AFF         | 60                        | 200          | 400                                | 80                                                   | 200          | 400                                |
| 2     | ASA         | 60                        | 200          | 400                                | 80                                                   | 200          | 400                                |

## Limiti degli oggetti SAN

I limiti degli oggetti SAN sono inclusi nella tabella seguente. I limiti si applicano indipendentemente dalla piattaforma.

| Oggetto in una relazione SM-BC                        | Conta                                                                                                                                           |
|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| LUN per volume                                        | 256                                                                                                                                             |
| Mappe LUN per nodo                                    | <ul style="list-style-type: none"> <li>• 4096 (ONTAP 9,10 e versioni successive)</li> <li>• 2048 (ONTAP 9.9.1 e versioni precedenti)</li> </ul> |
| Mappe LUN per cluster                                 | <ul style="list-style-type: none"> <li>• 8192 (ONTAP 9,10 e versioni successive)</li> <li>• 4096 (ONTAP 9.9.1 e versioni precedenti)</li> </ul> |
| LIF per SVM (con almeno un volume in relazione SM-BC) | 256                                                                                                                                             |
| LIF tra cluster per nodo                              | 4                                                                                                                                               |
| LIF tra cluster per cluster                           | 8                                                                                                                                               |

## Informazioni correlate

- ["Hardware Universe"](#)
- ["Limiti del gruppo di coerenza"](#)

## Installazione e configurazione

### Configurare il mediatore ONTAP e i cluster per la business continuity SnapMirror

SnapMirror Business Continuity (SM-BC) utilizza cluster peered per garantire la disponibilità dei dati in caso di failover. Il mediatore ONTAP è una risorsa chiave che garantisce la business continuity, monitorando lo stato di salute di ogni cluster. Per configurare SM-BC, è necessario prima installare il mediatore ONTAP e assicurarsi che i cluster primari e secondari siano configurati correttamente.

Una volta installato il mediatore ONTAP e configurato i cluster, è necessario [\[initialize-the-ontap-mediator\]](#) Il mediatore ONTAP da utilizzare con SM-BC. Devi quindi [Creare, inizializzare e mappare il gruppo di coerenza per SM-BC](#)

#### Mediatore ONTAP

Il mediatore ONTAP stabilisce un quorum per i cluster ONTAP in una relazione SM-BC. Coordina il failover automatico quando viene rilevato un guasto, determinando quale cluster agisce come principale e garantendo che i dati vengano serviti da e verso la destinazione corretta.

#### Prerequisiti per il mediatore ONTAP

- Il mediatore ONTAP include un proprio set di prerequisiti. È necessario soddisfare questi prerequisiti prima di installare il mediatore.

Per ulteriori informazioni, vedere ["Preparare l'installazione del servizio ONTAP Mediator"](#).

- Per impostazione predefinita, il supporto ONTAP fornisce il servizio tramite la porta TCP 31784. Assicurarsi che la porta 31784 sia aperta e disponibile tra i cluster ONTAP e il mediatore.

#### Installare il mediatore ONTAP e confermare la configurazione del cluster

Procedere con ciascuna delle seguenti operazioni. Per ogni fase, è necessario confermare che la configurazione specifica è stata eseguita. Utilizza il link incluso dopo ogni passaggio per ottenere ulteriori informazioni in base alle necessità.

#### Fasi

1. Installare il servizio ONTAP Mediator prima di assicurarsi che i cluster di origine e di destinazione siano configurati correttamente.

[Preparazione all'installazione o all'aggiornamento del servizio ONTAP Mediator](#)

2. Verificare che esista una relazione di peering del cluster tra i cluster.



L'IPSpace predefinito è richiesto da SM-BC per le relazioni peer del cluster. Un IPspace personalizzato non è supportato.

[Configurare le relazioni peer](#)

3. Verificare che le VM di storage siano create su ciascun cluster.

[Creazione di una SVM](#)

4. Verificare l'esistenza di una relazione peer tra le VM di storage su ciascun cluster.

### Creazione di una relazione di peering SVM

5. Verificare che i volumi esistano per le LUN.

### Creazione di un volume

6. Verificare che sia stata creata almeno una LIF SAN su ciascun nodo del cluster.

### "Considerazioni per le LIF in un ambiente SAN cluster"

### "Creazione di una LIF"

7. Verificare che i LUN necessari siano creati e mappati a un igroup, che viene utilizzato per mappare i LUN all'iniziatore sull'host dell'applicazione.

### Creare LUN e mappare igroups

8. Eseguire nuovamente la scansione dell'host dell'applicazione per rilevare eventuali nuove LUN.

### Inizializzare il mediatore ONTAP per SM-BC

Una volta installato il mediatore ONTAP e confermata la configurazione del cluster, è necessario inizializzare il mediatore ONTAP per il monitoraggio del cluster. È possibile inizializzare il supporto ONTAP utilizzando Gestione di sistema o l'interfaccia utente di ONTAP.

## System Manager

Con Gestione di sistema, è possibile configurare il server ONTAP Mediator per il failover automatico. È inoltre possibile sostituire SSL e CA autofirmati con certificati SSL e CA validati di terze parti, se non è già stato fatto.

### Fasi

1. Accedere a **protezione > Panoramica > Mediator > Configura**.
2. Selezionare **Aggiungi** e immettere le seguenti informazioni sul server ONTAP Mediator:
  - Indirizzo IPv4
  - Nome utente
  - Password
  - Certificato

### CLI

È possibile inizializzare il mediatore ONTAP dal cluster primario o secondario utilizzando l'interfaccia CLI di ONTAP. Quando si invia il `mediator add` Su un cluster, il mediatore ONTAP viene aggiunto automaticamente sull'altro cluster.

### Fasi

1. Inizializzare Mediator su uno dei cluster:

```
snapmirror mediator add -mediator-address IP_Address -peer-cluster  
cluster_name -username user_name
```

### Esempio

```
cluster1::> snapmirror mediator add -mediator-address 192.168.10.1  
-peer-cluster cluster2 -username mediatoradmin  
Notice: Enter the mediator password.  
  
Enter the password: *****  
Enter the password again: *****
```

2. Controllare lo stato della configurazione del Mediator:

```
snapmirror mediator show
```

| Mediator Address | Peer Cluster | Connection Status | Quorum Status |
|------------------|--------------|-------------------|---------------|
| 192.168.10.1     | cluster-2    | connected         | true          |

Quorum Status Indica se le relazioni del gruppo di coerenza SnapMirror sono sincronizzate con il mediatore; uno stato di `true` indica che la sincronizzazione è stata eseguita correttamente.

## Proteggere con SnapMirror Business Continuity

La configurazione della protezione mediante la business continuity di SnapMirror implica la selezione delle LUN nel cluster di origine di ONTAP e l'aggiunta di tali LUN a un gruppo di coerenza.

### Prima di iniziare

- È necessario disporre di un ["Licenza SnapMirror Synchronous"](#).
- È necessario essere un amministratore di cluster o di macchine virtuali per lo storage.
- Tutti i volumi costituenti di un gruppo di coerenza devono trovarsi in una singola VM di storage (SVM).
  - Le LUN possono risiedere su volumi diversi.
- Il cluster di origine e di destinazione non può essere lo stesso.
- Non è possibile stabilire relazioni di gruppo di coerenza SM-BC tra cluster ASA e cluster non ASA.
- L'IPSpace predefinito è richiesto da SM-BC per le relazioni peer del cluster. IPSpace personalizzato non supportato.
- Il nome del gruppo di coerenza deve essere univoco.
- I volumi sul cluster secondario (di destinazione) devono essere di tipo DP.
- Le SVM primarie e secondarie devono essere in relazione peered.

### Fasi

È possibile configurare un gruppo di coerenza utilizzando l'interfaccia utente di ONTAP o Gestione sistema.

A partire da ONTAP 9.10.1, ONTAP offre un endpoint di gruppo coerente e un menu in Gestione sistema, che offre utility di gestione aggiuntive. Se si utilizza ONTAP 9.10.1 o versione successiva, vedere ["Configurare un gruppo di coerenza"](#) quindi ["configurare la protezione"](#) Per creare una relazione SM-BC.

## System Manager

1. Sul cluster primario, accedere a **protezione > Panoramica > Proteggi per la business continuity > Proteggi LUN**.
2. Selezionare i LUN che si desidera proteggere e aggiungerli a un gruppo di protezione.
3. Selezionare il cluster di destinazione e SVM.
4. Per impostazione predefinita, l'opzione **Inizializza relazione** è selezionata. Fare clic su **Save** (Salva) per iniziare la protezione.
5. Accedere a **Dashboard > Performance** per verificare l'attività IOPS per le LUN.
6. Nel cluster di destinazione, utilizzare System Manager per verificare che la protezione per la relazione di business continuity sia sincronizzata: **Protezione > relazioni**.

## CLI

1. Creare una relazione di gruppo di coerenza dal cluster di destinazione.  
``destination::> snapmirror create -source-path source-path -destination-path destination-path -cg-item -mappings volume-path -policy policy-name`

È possibile mappare fino a 12 volumi costitutivi utilizzando `cg-item-mappings` sul `snapmirror create` comando.

Nell'esempio seguente vengono creati due gruppi di coerenza: `cg_src_` on the source with ``vol1` e `vol2` e un gruppo di coerenza di destinazione mirrorato, `cg_dst`.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOver
```

2. Dal cluster di destinazione, inizializzare il gruppo di coerenza.

```
destination::> snapmirror initialize -destination-path destination-
consistency-group
```

3. Verificare che l'operazione di inizializzazione sia stata completata correttamente. Lo stato deve essere `InSync`.

```
snapmirror show
```

4. Su ciascun cluster, creare un igroup in modo da poter mappare le LUN all'iniziatore sull'host dell'applicazione.  
`lun igroup create -igroup name -protocol fc|iscsi -ostype os -initiator initiator_name`

5. Su ciascun cluster, mappare i LUN all'igroup:

```
lun map -path path_name -igroup igroup_name
```

6. Verificare che la mappatura LUN sia stata completata correttamente con `lun map` comando. Quindi, è possibile scoprire i nuovi LUN sull'host dell'applicazione.



## Gestire SM-BC e proteggere i dati

### Creare una copia Snapshot comune

Oltre alle operazioni di copia Snapshot regolarmente pianificate, è possibile creare manualmente un file comune **"Copia Snapshot"** Tra i volumi nel gruppo di coerenza SnapMirror primario e i volumi nel gruppo di coerenza SnapMirror secondario.

#### A proposito di questa attività

- In ONTAP 9.8, l'intervallo di creazione dello snapshot pianificato è di un'ora.

A partire da ONTAP 9.9.1, l'intervallo è di 12 ore.

#### Prima di iniziare

- La relazione del gruppo SnapMirror deve essere sincronizzata.

#### Fasi

1. Creare una copia Snapshot comune:

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Monitorare l'avanzamento dell'aggiornamento:

```
destination::>snapmirror show -fields -newest-snapshot
```

### Eeguire un failover pianificato

In un failover pianificato, è possibile cambiare i ruoli dei cluster primario e secondario, in modo che il cluster secondario prenda il controllo dal cluster primario. Durante un failover, il cluster secondario elabora le richieste di input e output in locale senza interrompere le operazioni del client.

È possibile eseguire un failover pianificato per verificare lo stato della configurazione di disaster recovery o per eseguire la manutenzione sul cluster primario.

#### A proposito di questa attività

L'amministratore del cluster secondario avvia un failover pianificato. L'operazione richiede la commutazione dei ruoli primario e secondario in modo che il cluster secondario prenda il posto del primario. Il nuovo cluster primario può quindi iniziare a elaborare le richieste di input e output localmente senza interrompere le operazioni del client.

#### Prima di iniziare

- La relazione SM-BC deve essere sincronizzata.
- Non è possibile avviare un failover pianificato quando è in corso un'operazione senza interruzioni. Le operazioni senza interruzioni includono spostamenti di volumi, trasferimenti di aggregazioni e failover dello storage.
- Il mediatore ONTAP deve essere configurato, connesso e in quorum.

#### Fasi

È possibile eseguire un failover pianificato utilizzando l'interfaccia utente di ONTAP o Gestione di sistema.

## System Manager

1. In System Manager, selezionare **protezione > Panoramica > Relazioni**.
2. Identificare la relazione SM-BC che si desidera eseguire il failover. Accanto al nome, selezionare ...  
Accanto al nome della relazione, quindi selezionare **failover**.
3. Per monitorare lo stato del failover, utilizzare `snapmirror failover show` Nella CLI di ONTAP.

## CLI

1. Dal cluster di destinazione, avviare l'operazione di failover:

```
destination::>snapmirror failover start -destination-path  
vs1_dst:/cg/cg_dst
```

2. Monitorare l'avanzamento del failover:

```
destination::>snapmirror failover show
```

3. Una volta completata l'operazione di failover, è possibile monitorare lo stato della relazione di protezione di Synchronous SnapMirror dalla destinazione:

```
destination::>snapmirror show
```

## Ripristino da operazioni di failover automatiche non pianificate

Un'operazione di failover automatico non pianificato (AUFO) si verifica quando il cluster primario è inattivo o isolato. Il mediatore ONTAP rileva quando si verifica un failover ed esegue un failover automatico non pianificato sul cluster secondario. Il cluster secondario viene convertito nel cluster primario e inizia a servire i client. Questa operazione viene eseguita solo con l'assistenza del mediatore ONTAP.




Dopo il failover automatico non pianificato, è importante eseguire nuovamente la scansione dei percorsi i/o del LUN host in modo che non vi sia alcuna perdita dei percorsi i/O.

## Ristabilire la relazione di protezione dopo un failover non pianificato

È possibile ristabilire la relazione di protezione utilizzando Gestione di sistema o l'interfaccia utente di ONTAP.

## System Manager

### Fasi

1. Accedere a **protezione > Relazioni** e attendere che lo stato della relazione mostri "InSync".
2. Per riprendere le operazioni sul cluster di origine, fare clic su  E selezionare **failover**.

### CLI

È possibile monitorare lo stato del failover automatico non pianificato utilizzando `snapmirror failover show` comando.

Ad esempio:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
      Source Path: vs1:/cg/scg3
Destination Path: vs3:/cg/dcg3
Failover Status: completed
      Error Reason:
      End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
      Failover Type: unplanned
Error Reason codes: -
```

Fare riferimento a ["Riferimento EMS"](#) per informazioni sui messaggi di evento e sulle azioni correttive.

### Riprendere la protezione in una configurazione fan-out dopo il failover

In caso di failover sul cluster secondario nella relazione SM-BC, la destinazione asincrona di SnapMirror diventa malsana. È necessario ripristinare manualmente la protezione eliminando e ricreando la relazione con l'endpoint asincrono di SnapMirror.

### Fasi

1. Verificare che il failover sia stato completato correttamente:  
`snapmirror failover show`
2. Nell'endpoint SnapMirror asincrono, eliminare l'endpoint fan-out:  
`snapmirror delete -destination-path destination_path`
3. Sul terzo sito, creare relazioni SnapMirror asincrone tra il nuovo volume primario SM-BC e il volume di destinazione fan-out asincrono:  
`snapmirror create -source-path source_path -destination-path destination_path -policy MirrorAllSnapshots -schedule schedule`
4. Risincronizzare la relazione:  
`snapmirror resync -destination-path destination_path`
5. Verificare lo stato e la salute della relazione:  
`snapmirror show`

## Monitorare le operazioni di Business Continuity di SnapMirror

È possibile monitorare le seguenti operazioni di Business Continuity SnapMirror (SM-BC) per garantire lo stato di salute della configurazione SM-BC:

- Mediatore ONTAP
- Operazioni di failover pianificate
- Operazioni di failover automatiche non pianificate
- Disponibilità SM-BC

### Mediatore ONTAP

Durante le normali operazioni, lo stato del mediatore ONTAP deve essere connesso. Se si trova in qualsiasi altro stato, potrebbe essere presente una condizione di errore. È possibile rivedere ["Messaggi EMS \(Event Management System\)"](#) per determinare l'errore e le azioni correttive appropriate.

### Operazioni di failover pianificate

È possibile monitorare lo stato e l'avanzamento di un'operazione di failover pianificata utilizzando `snapmirror failover show` comando. Ad esempio:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Una volta completata l'operazione di failover, è possibile monitorare lo stato di protezione di Synchronous SnapMirror dal nuovo cluster di destinazione. Ad esempio:

```
ClusterA::> snapmirror show
```

Fare riferimento a ["Riferimento EMS"](#) per informazioni sui messaggi di evento e sulle azioni correttive.

### Operazioni di failover automatiche non pianificate

Durante un failover automatico non pianificato, è possibile monitorare lo stato dell'operazione utilizzando `snapmirror failover show` comando.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
      Source Path: vs1:/cg/scg3
      Destination Path: vs3:/cg/dcg3
      Failover Status: completed
      Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
      Failover Type: unplanned
Error Reason codes: -
```

Fare riferimento a ["Riferimento EMS"](#) per informazioni sui messaggi di evento e sulle azioni correttive.

## Disponibilità SM-BC

È possibile verificare la disponibilità della relazione SM-BC utilizzando una serie di comandi, sul cluster primario, sul cluster secondario o su entrambi.

I comandi utilizzati includono `snapmirror mediator show` sul cluster primario e secondario per controllare lo stato di connessione e quorum, il `snapmirror show` e il `volume show` comando. Ad esempio:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86    SMBC_B          connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86    SMBC_A          connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source          Destination Mirror Relationship Total
Last
Path            Type Path          State Status          Progress Healthy
Updated
-----
-----
vs0:/cg/cg1 XDP vs1:/cg/cg1_dp Snapmirrored InSync -         true -
vs0:vol1      XDP vs1:vol1_dp  Snapmirrored InSync -         true -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs0      vol1      true          false          Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs1      vol1_dp false          true           No-consensus
```

## Aggiungere o rimuovere volumi a un gruppo di coerenza

Con il variare dei requisiti dei carichi di lavoro delle applicazioni, potrebbe essere necessario aggiungere o rimuovere volumi da un gruppo di coerenza per garantire la continuità del business. Il processo di aggiunta e rimozione di volumi in una relazione SM-BC attiva dipende dalla versione di ONTAP in uso.

Nella maggior parte dei casi, si tratta di un processo di interruzione che richiede di interrompere la relazione SnapMirror, modificare il gruppo di coerenza e riprendere la protezione. A partire da ONTAP 9.13.1, l'aggiunta di volumi a un gruppo di coerenza con una relazione SM-BC attiva è un'operazione senza interruzioni.

### A proposito di questa attività

- In ONTAP dalla versione 9.8 alla 9.9.1, è possibile aggiungere o rimuovere volumi a un gruppo di coerenza utilizzando l'interfaccia utente di ONTAP.
- A partire da ONTAP 9.10.1, si consiglia di eseguire la gestione ["gruppi di coerenza"](#) Tramite Gestore di sistema o con l'API REST di ONTAP.

Se si desidera modificare la composizione del gruppo di coerenza aggiungendo o rimuovendo un volume, è necessario prima eliminare la relazione originale e quindi creare nuovamente il gruppo di coerenza con la nuova composizione.

- A partire da ONTAP 9.13.1, è possibile aggiungere senza interruzioni volumi a un gruppo di coerenza con una relazione SM-BC attiva dall'origine o dalla destinazione.

La rimozione dei volumi è un'operazione di interruzione. Prima di procedere con la rimozione dei volumi, è necessario interrompere la relazione di SnapMirror.

## ONTAP 9.8-9.13.0

### Prima di iniziare

- Non è possibile iniziare a modificare il gruppo di coerenza mentre si trova in InSync stato.
- Il volume di destinazione deve essere di tipo DP.
- Il nuovo volume aggiunto per espandere il gruppo di coerenza deve disporre di una coppia di copie Snapshot comuni tra i volumi di origine e di destinazione.

### Fasi

Gli esempi illustrati in due mappature di volumi:  $\text{vol\_src1} \longleftrightarrow \text{vol\_dst1}$  e  $\text{vol\_src2} \longleftrightarrow \text{vol\_dst2}$ , in una relazione di gruppo di coerenza tra i punti finali  $\text{vs1\_src}:/\text{cg}/\text{cg\_src}$  e  $\text{vs1\_dst}:/\text{cg}/\text{cg\_dst}$ .

1. Sui cluster di origine e di destinazione, verificare la presenza di un'istantanea comune tra i cluster di origine e di destinazione con il comando `snapshot show -vserver svm_name -volume volume_name -snapshot snapmirror`

```
source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot snapmirror*
```

```
destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot snapmirror*
```

2. Se non esiste una copia Snapshot comune, creare e inizializzare una relazione SnapMirror di FlexVol:

```
destination::>snapmirror initialize -source-path vs1_src:vol_src3 -destination-path vs1_dst:vol_dst3
```

3. Eliminare la relazione del gruppo di coerenza:

```
destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
```

4. Rilasciare la relazione SnapMirror di origine e conservare le copie Snapshot comuni:

```
source::>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol_dst3
```

5. Annullare la mappatura dei LUN ed eliminare la relazione esistente del gruppo di coerenza:

```
destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup <igroup_name>
```



I LUN di destinazione non sono mappati, mentre i LUN sulla copia primaria continuano a servire l'i/o host

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst -relationship-info-only true
```

6. Se si utilizza ONTAP da 9.10.1 a 9.13.0, eliminare e ricreare il gruppo di coerenza sull'origine con la

composizione corretta. Seguire la procedura descritta in [Eliminare un gruppo di coerenza](#) e poi [Configurare un singolo gruppo di coerenza](#). In ONTAP 9.10.1 e versioni successive, è necessario eseguire le operazioni di eliminazione e creazione in Gestore di sistema o con l'API REST di ONTAP; non esiste alcuna procedura CLI.

**Se si utilizza ONTAP 9.8, 9.0 o 9.9.1, passare alla fase successiva.**

7. Creare il nuovo gruppo di coerenza sulla destinazione con la nuova composizione:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src  
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,  
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Risincronizzare la relazione del gruppo di coerenza RTO zero per assicurarsi che sia sincronizzata:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Rimappare i LUN non mappati nella fase 5:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```


10. Eseguire nuovamente la scansione dei percorsi i/o del LUN host per ripristinare tutti i percorsi dei LUN.

#### ONTAP 9.13.1 e versioni successive

A partire da ONTAP 9.13.1, è possibile aggiungere volumi senza interruzioni a un gruppo di coerenza con una relazione SM-BC attiva. SM-BC supporta l'aggiunta di volumi sia dall'origine che dalla destinazione.

Per ulteriori informazioni sull'aggiunta di volumi dal gruppo di coerenza di origine, vedere [Modificare un gruppo di coerenza](#).

#### Aggiungere un volume dal cluster di destinazione

1. Nel cluster di destinazione, selezionare **protezione > relazioni**.
2. Individuare la relazione SM-BC a cui si desidera aggiungere volumi. Selezionare  Quindi **espandere**.
3. Selezionare le relazioni dei volumi i cui volumi devono essere aggiunti al gruppo di coerenza
4. Selezionare **Espandi**.

#### Convertire le relazioni esistenti in relazioni SM-BC

Se si dispone di una relazione SnapMirror sincrona esistente tra un cluster di origine e di destinazione, è possibile convertirla in una relazione SM-BC. Ciò consente di associare i volumi mirrorati a un gruppo di coerenza, garantendo zero RPO in un carico di lavoro multi-volume. Inoltre, è possibile conservare le snapshot SnapMirror esistenti se è necessario ripristinarle in un momento specifico prima di stabilire la relazione SM-BC.

#### Prima di iniziare

- Deve esistere una relazione SnapMirror sincrona RPO zero tra il cluster primario e secondario.
- Prima di poter creare la relazione SnapMirror zero RTO, è necessario rimuovere la mappatura di tutti i LUN del volume di destinazione.



- SM-BC supporta solo i protocolli SAN (non NFS/CIFS). Assicurarsi che nessun componente del gruppo di coerenza sia montato per l'accesso NAS.

#### A proposito di questa attività

- È necessario essere un amministratore di cluster e SVM sui cluster primario e secondario.
- Non è possibile convertire zero RPO in zero RTO Sync modificando il criterio SnapMirror.
- Assicurarsi che i LUN siano dismappati prima di emettere `snapmirror create` comando.

Se i LUN esistenti sul volume secondario sono mappati e l' AutomatedFailover il criterio è configurato, il `snapmirror create` genera un errore.

#### Fasi

1. Dal cluster secondario, eseguire un aggiornamento di SnapMirror sulla relazione esistente:

```
destination::>snapmirror update -destination-path vs1_dst:vol1
```

2. Verificare che l'aggiornamento di SnapMirror sia stato completato correttamente:

```
destination::>snapmirror show
```

3. Interrompere ciascuna delle relazioni sincrone RPO zero:

```
destination::>snapmirror quiesce -destination-path vs1_dst:vol1
```

```
destination::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. Eliminare ciascuna delle relazioni sincrone RPO zero:

```
destination::>snapmirror delete -destination-path vs1_dst:vol1
```

```
destination::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Rilasciare la relazione SnapMirror di origine, conservando le copie Snapshot comuni:

```
source::>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol1
```

```
source::>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol2
```

6. Creare una relazione SnapMirror sincrona RTO zero di gruppo:

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy AutomatedFailover
```

7. Risincronizzare il gruppo di coerenza:

```
destination::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. Eseguire nuovamente la scansione dei percorsi i/o del LUN host per ripristinare tutti i percorsi dei LUN.

## Aggiorna e ripristina ONTAP con SM-BC

A partire da ONTAP 9.8, SnapMirror Business Continuity (SM-BC) è supportato. L'aggiornamento e il ripristino del cluster ONTAP hanno implicazioni sulle relazioni SM-BC a seconda della versione di ONTAP a cui si esegue l'aggiornamento o il ripristino.

### Aggiorna ONTAP con SM-BC

Per utilizzare SM-BC, tutti i nodi dei cluster di origine e destinazione devono eseguire ONTAP 9,8 o versioni successive.

Quando si aggiorna ONTAP con relazioni SM-BC attive, è necessario utilizzare [Upgrade automatici e senza interruzioni \(ANDU\)](#). L'utilizzo di ANDU garantisce che le relazioni SM-BC siano sincronizzate e integre durante il processo di aggiornamento.

Non ci sono passaggi di configurazione per preparare le implementazioni di SM-BC per gli aggiornamenti ONTAP. Tuttavia, prima e dopo l'aggiornamento, si consiglia di verificare che:

- Sincronizzazione delle relazioni SM-BC.
- Nel registro eventi non sono presenti errori correlati a SnapMirror.
- Il mediatore è online e sano da entrambi i cluster.
- Tutti gli host sono in grado di visualizzare correttamente tutti i percorsi per proteggere le LUN.



Quando esegui l'upgrade dei cluster da ONTAP 9,8 o 9.9.1 a ONTAP 9.10.1 e versioni successive, ONTAP crea nuove funzionalità [gruppi di coerenza](#). Su cluster sia di origine che di destinazione per relazioni SM-BC che possono essere configurate usando System Manager.



Il `snapmirror quiesce` e `snapmirror resume` I comandi non sono supportati con SM-BC.

### Ripristinare ONTAP 9.9.1 da ONTAP 9.10.1

Per ripristinare le relazioni da 9.10.1 a 9.9.1, è necessario eliminare le relazioni SM-BC, seguite dall'istanza del gruppo di coerenza 9.10.1. I gruppi di coerenza con una relazione SM-BC attiva non possono essere cancellati. Tutti i volumi FlexVol che sono stati aggiornati alla versione 9.10.1 precedentemente associati a un altro smart container o a un'applicazione aziendale nel 9.9.1 o precedente non saranno più associati al revert. L'eliminazione dei gruppi di coerenza non elimina i volumi costituenti o le snapshot granulari del volume. Fare riferimento a ["Eliminare un gruppo di coerenza"](#) Per ulteriori informazioni su questa attività in ONTAP 9.10.1 e versioni successive.

### Ripristinare ONTAP 9.7 da ONTAP 9.8



SM-BC non è supportato con cluster misti ONTAP 9.7 e ONTAP 9.8.

Quando si passa da ONTAP 9.8 a ONTAP 9.7, è necessario tenere presente quanto segue:

- Se il cluster ospita una destinazione SM-BC, il ripristino a ONTAP 9.7 non è consentito fino a quando la relazione non viene interrotta ed eliminata.
- Se il cluster ospita un'origine SM-BC, il ripristino di ONTAP 9.7 non è consentito fino al rilascio della relazione.
- Tutti i criteri di SnapMirror SM-BC personalizzati creati dall'utente devono essere cancellati prima di

tornare a ONTAP 9.7.

Per soddisfare questi requisiti, vedere ["Rimuovere una configurazione SM-BC"](#).

## Fasi

1. Eseguire un controllo di revert da uno dei cluster nella relazione SM-BC:

```
cluster::*> system node revert-to -version 9.7 -check-only
```

Esempio:

```
cluster::*> system node revert-to -version 9.7 -check-only
Error: command failed: The revert check phase failed. The following
issues must be resolved before revert can be completed. Bring the data
LIFs down on running vservers. Command to list the running vservers:
vserver show -admin-state running Command to list the data LIFs that are
up: network interface show -role data -status-admin up Command to bring
all data LIFs down: network interface modify {-role data} -status-admin
down
Disable snapshot policies.
    Command to list snapshot policies: "snapshot policy show".
    Command to disable snapshot policies: "snapshot policy modify
-vserver
    * -enabled false"

    Break off the initialized online data-protection (DP) volumes and
delete
    Uninitialized online data-protection (DP) volumes present on the
local
    node.
    Command to list all online data-protection volumes on the local
node:
    volume show -type DP -state online -node <local-node-name>
    Before breaking off the initialized online data-protection volumes,
quiesce and abort transfers on associated SnapMirror relationships
and
    wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship: snapmirror
abort
    Command to see if the Relationship Status of a SnapMirror
relationship
    is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
    of a SnapMirror relationship with a policy of type "vault":
```

```

snapmirror
break -delete-snapshots
Uninitialized data-protection volumes are reported by the
"snapmirror
break" command when applied on a DP volume.
Command to delete volume: volume delete

Delete current version snapshots in advanced privilege level.
Command to list snapshots: "snapshot show -fs-version 9.8"
Command to delete snapshots: "snapshot prepare-for-revert -node
<nodename>"

Delete all user-created policies of the type active-strict-sync-
mirror
and active-sync-mirror.
The command to see all active-strict-sync-mirror and active-sync-
mirror
type policies is:
snapmirror policy show -type
active-strict-sync-mirror,active-sync-mirror
The command to delete a policy is :
snapmirror policy delete -vserver <SVM-name> -policy <policy-name>

```

Per informazioni sul ripristino dei cluster, vedere ["Ripristina ONTAP"](#).

## Rimuovere una configurazione SM-BC

Se non si richiede più una protezione SnapMirror sincronizzata con RTO pari a zero, è possibile eliminare la relazione SM-BC.

### A proposito di questa attività

- Prima di eliminare la relazione SM-BC, tutte le LUN nel cluster di destinazione devono essere dismappate.
- Una volta che i LUN sono stati dismappati e l'host è stato nuovamente scansionato, la destinazione SCSI notifica agli host che l'inventario LUN è stato modificato. Le LUN esistenti sui volumi secondari RTO zero cambiano per riflettere una nuova identità dopo l'eliminazione della relazione RTO zero. Gli host rilevano le LUN del volume secondario come nuove LUN che non hanno alcuna relazione con le LUN del volume di origine.
- I volumi secondari rimangono volumi DP dopo l'eliminazione della relazione. È possibile eseguire il `snapmirror break` comando per convertirli in lettura/scrittura.
- L'eliminazione della relazione non è consentita nello stato di failover quando la relazione non viene invertita.

### Fasi

1. Dal cluster secondario, rimuovere la relazione del gruppo di coerenza SM-BC tra l'endpoint di origine e l'endpoint di destinazione:

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. Dal cluster primario, rilasciare la relazione del gruppo di coerenza e le copie Snapshot create per la relazione:

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. Eseguire una nuova scansione dell'host per aggiornare l'inventario del LUN.
4. A partire da ONTAP 9.10.1, l'eliminazione della relazione SnapMirror non elimina il gruppo di coerenza. Se si desidera eliminare il gruppo di coerenza, è necessario utilizzare Gestione sistema o l'API REST di ONTAP. Vedere [Eliminare un gruppo di coerenza](#) per ulteriori informazioni.

## Rimuovere il mediatore ONTAP

Se si desidera rimuovere una configurazione di ONTAP Mediator esistente dai cluster ONTAP, è possibile farlo utilizzando `snapmirror mediator remove` comando.

### Fasi

1. Rimuovi mediatore ONTAP:

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster  
cluster_xyz
```

## Risolvere i problemi

### L'operazione di eliminazione di SnapMirror non riesce nello stato di takeover

#### Problema:

Quando ONTAP 9.9.1 viene installato in un cluster, eseguire `snapmirror delete` il comando non riesce quando una relazione di gruppo di coerenza SM-BC è in stato di Takeover.

```
C2_cluster::> snapmirror delete vs1:/cg/dd
```

```
Error: command failed: RPC: Couldn't make connection
```

#### Soluzione

Quando i nodi in una relazione SM-BC sono in stato di Takeover, eseguire l'operazione di eliminazione e rilascio di SnapMirror con l'opzione "-force" impostata su true.

```
C2_cluster::> snapmirror delete vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
        "vs1:/cg/dd" will be deleted, however the items of the
destination
        Consistency Group might not be made writable, deletable, or
modifiable
        after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

## Errore durante la creazione di una relazione SnapMirror e l'inizializzazione del gruppo di coerenza

### Problema:

La creazione della relazione SnapMirror e l'inizializzazione del gruppo di coerenza non riesce.

### Soluzione:


Assicurarsi di non aver superato il limite di gruppi di coerenza per cluster. I limiti del gruppo di coerenza in SM-BC sono indipendenti dalla piattaforma e differiscono in base alla versione di ONTAP. Vedere ["Ulteriori restrizioni e limitazioni"](#) Per le limitazioni basate sulla versione di ONTAP.

### Errore:

Se l'inizializzazione del gruppo di coerenza è bloccata, controllare lo stato delle inizializzazioni del gruppo di coerenza con l'API REST di ONTAP, Gestore di sistema o il comando `sn show -expand`.

### Soluzione:

Se l'inizializzazione dei gruppi di coerenza non riesce, rimuovere la relazione SM-BC, eliminare il gruppo di coerenza, quindi ricreare la relazione e inicializzarla. Questo flusso di lavoro varia a seconda della versione di ONTAP in uso.

| Se si utilizza ONTAP 9.8-9.9.1                                                                                                                                                                                                                                    | Se si utilizza ONTAP 9.10.1 o versione successiva                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. <a href="#">"Rimuovere la configurazione SM-BC"</a></li> <li>2. <a href="#">"Creare una relazione di gruppo di coerenza"</a></li> <li>3. <a href="#">"Inizializzare la relazione del gruppo di coerenza"</a></li> </ol> | <ol style="list-style-type: none"> <li>1. In <b>protezione &gt; Relazioni</b>, individuare la relazione SM-BC nel gruppo di coerenza. Selezionare , Quindi <b>Delete</b> per rimuovere la relazione SM-BC.</li> <li>2. <a href="#">"Eliminare il gruppo di coerenza"</a></li> <li>3. <a href="#">"Configurare il gruppo di coerenza"</a></li> </ol> |

## Failover pianificato non riuscito

### Problema:

Dopo aver eseguito il `snapmirror failover start` il comando, l'output per `snapmirror failover show` command visualizza un messaggio che indica che è in

corso un'operazione senza interruzioni.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
08:35:04 08:35:04
```

**Causa:**

Un failover pianificato non può iniziare quando è in corso un'operazione senza interruzioni, tra cui lo spostamento del volume, il trasferimento degli aggregati e il failover dello storage.

**Soluzione:**

Attendere il completamento dell'operazione senza interruzioni e provare a eseguire nuovamente l'operazione di failover.

**Il mediatore ONTAP non è raggiungibile o lo stato del quorum del mediatore è falso**

**Problema:**

Dopo aver eseguito il `snapmirror failover start` il comando, l'output per `snapmirror failover show` Viene visualizzato un messaggio che indica che Mediator non è configurato.

Vedere ["Inizializzare il mediatore ONTAP"](#).

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

**Causa:**

Il mediatore non è configurato o si sono riscontrati problemi di connettività di rete.

**Soluzione:**

Se il mediatore ONTAP non è configurato, è necessario configurare il mediatore ONTAP prima di poter stabilire una relazione SM-BC. Risolvere eventuali problemi di connettività di rete. Assicurarsi che Mediator sia connesso e che lo stato del quorum sia vero sia sul sito di origine che su quello di destinazione utilizzando il comando `snapmirror mediator show`. Per ulteriori informazioni, vedere [Configurare il mediatore ONTAP](#).

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.234.10.143      cluster2      connected      true
```

## Failover automatico non pianificato non attivato sul sito B

### Problema:

Un guasto nel sito A non attiva un failover non pianificato sul sito B.

### Possibile causa n. 1:

Il mediatore ONTAP non è configurato. Per determinare se questa è la causa, eseguire il `snapmirror mediator show` Sul cluster del sito B.

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

Questo esempio indica che il mediatore ONTAP non è configurato sul sito B.

### Soluzione:

Assicurarsi che il mediatore ONTAP sia configurato su entrambi i cluster, che lo stato sia connesso e che il quorum sia impostato su vero.

### Possibile causa n. 2:

Il gruppo di coerenza SnapMirror non è sincronizzato. Per determinare se questa è la causa, visualizzare il registro eventi per visualizzare se il gruppo di coerenza era sincronizzato durante il momento in cui si è verificato un errore del sito A.

```
cluster::*> event log show -event *out.of.sync*

Time                Node                Severity          Event
-----
10/1/2020 23:26:12  sti42-vsims-ucs511w ERROR             sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

### Soluzione:

Completare i seguenti passaggi per eseguire un failover forzato sul sito B.

1. Annullare la mappatura di tutte le LUN appartenenti al gruppo di coerenza dal sito B.
2. Eliminare la relazione del gruppo di coerenza SnapMirror utilizzando `force` opzione.



3. Inserire il `snapmirror break` Sul gruppo di coerenza i volumi costituenti per convertire i volumi da DP a R/W, per abilitare l'i/o dal sito B.
4. Avviare i nodi del sito A per creare una relazione RTO zero dal sito B al sito A.
5. Rilasciare il gruppo di coerenza con `relationship-info-only` On-site A per conservare una copia Snapshot comune e annullare la mappatura delle LUN appartenenti al gruppo di coerenza.
6. Convertire i volumi sul sito A da R/W a DP impostando una relazione a livello di volume utilizzando il criterio Sync o il criterio Async.
7. Eseguire il `snapmirror resync` per sincronizzare le relazioni.
8. Eliminare le relazioni di SnapMirror con il criterio di sincronizzazione sul sito A.
9. Rilasciare le relazioni di SnapMirror con il criterio Sync utilizzando `relationship-info-only true` On-site B.
10. Creare una relazione di gruppo di coerenza tra il sito B e il sito A.
11. Eseguire una risincronizzazione del gruppo di coerenza dal sito A, quindi verificare che il gruppo di coerenza sia sincronizzato.
12. Eseguire nuovamente la scansione dei percorsi i/o del LUN host per ripristinare tutti i percorsi dei LUN.

#### **Collegamento tra il sito B e il mediatore inattivo e il sito A inattivo**

Per verificare la connessione del mediatore ONTAP, utilizzare `snapmirror mediator show` comando. Se lo stato della connessione non è raggiungibile e il sito B non è in grado di raggiungere il sito A, si avrà un'uscita simile a quella riportata di seguito. Per ripristinare la connessione, attenersi alla procedura descritta nella soluzione

```

cluster::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.237.86.17      C1_cluster      unreachable      true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::*> snapmirror show -expand
Source                Destination Mirror  Relationship    Total
Last
Path                Type  Path                State  Status                Progress  Healthy
Updated
-----
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::*> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability
Authentication
-----
C1_cluster              1-80-000011              Unavailable      ok

```

## Soluzione

Forzare un failover per abilitare l'i/o dal sito B e quindi stabilire una relazione RTO zero dal sito B al sito A. Completare i seguenti passaggi per eseguire un failover forzato sul sito B.

1. Annullare la mappatura di tutte le LUN appartenenti al gruppo di coerenza dal sito B.
2. Eliminare la relazione del gruppo di coerenza di SnapMirror utilizzando l'opzione force (forza).
3. Inserisci il comando SnapMirror breaker (snapmirror break -destination\_path svm:\_volume\_) Sui volumi costituenti del gruppo di coerenza per convertire volumi da DP a RW, per abilitare i/o dal sito B.

Devi inviare il comando SnapMirror BREAK per ogni relazione nel gruppo di coerenza. Ad esempio, se nel gruppo di coerenza sono presenti tre volumi, verrà inviato il comando per ogni volume.

4. Avviare i nodi del sito A per creare una relazione RTO zero dal sito B al sito A.

5. Rilasciare il gruppo di coerenza con informazioni sulla relazione solo sul sito A per conservare una copia Snapshot comune e annullare la mappatura delle LUN appartenenti al gruppo di coerenza.
6. Convertire i volumi sul sito A da RW a DP impostando una relazione a livello di volume utilizzando il criterio Sync o il criterio Async.
7. Eseguire il `snapmirror resync` per sincronizzare le relazioni.
8. Eliminare le relazioni di SnapMirror con il criterio di sincronizzazione sul sito A.
9. Rilasciare il criterio delle relazioni di SnapMirror con Sync utilizzando solo le informazioni sulla relazione, vero sul sito B.
10. Creare una relazione di gruppo di coerenza tra il sito B e il sito A.
11. Dal cluster di origine, sincronizzare nuovamente il gruppo di coerenza. Verificare che lo stato del gruppo di coerenza sia sincronizzato.
12. Eseguire nuovamente la scansione dei percorsi di i/o delle LUN dell'host per ripristinare tutti i percorsi alle LUN.

### Collegamento tra il sito A e il mediatore inattivo e il sito B inattivo

Quando si utilizza SM-BC, è possibile perdere la connettività tra il ONTAP Mediator o i cluster in cui si esegue il peering. È possibile diagnosticare il problema controllando la connessione, la disponibilità e lo stato di consenso delle diverse parti della relazione SM-BC e riprendendo con forza la connessione.

| Cosa controllare                   | Comando CLI                                                 | Indicatore                                                                         |
|------------------------------------|-------------------------------------------------------------|------------------------------------------------------------------------------------|
| Mediatore dal sito A.              | <code>snapmirror mediator show</code>                       | Lo stato della connessione sarà <code>unreachable</code>                           |
| Connettività del sito B.           | <code>cluster peer show</code>                              | La disponibilità sarà <code>unavailable</code>                                     |
| Stato di consenso del volume SM-BC | <code>volume show volume_name -fields smbc-consensus</code> | Il <code>sm-bc consensus</code> il campo indicherà <code>Awaiting-consensus</code> |

Per ulteriori informazioni sulla diagnosi e la risoluzione di questo problema, consultare l'articolo della Knowledge base ["Collegamento tra il sito A e Mediator Down e il sito B Down quando si utilizza SM-BC"](#).

### L'operazione di eliminazione di SM-BC SnapMirror non riesce quando fence è impostato sul volume di destinazione

#### Problema:

L'operazione di eliminazione di SnapMirror non riesce quando uno dei volumi di destinazione ha una fence di reindirizzamento impostata.

#### Soluzione

Eseguire le seguenti operazioni per riprovare il reindirizzamento e rimuovere la fence dal volume di destinazione.

- Risincronizzazione di SnapMirror
- Aggiornamento di SnapMirror

## **Operazione di spostamento del volume bloccata quando il sistema primario è inattivo**

### **Problema:**

Un'operazione di spostamento del volume rimane bloccata a tempo indeterminato nello stato di cutover rinviato quando il sito primario è inattivo in una relazione SM-BC. Quando il sito primario è inattivo, il sito secondario esegue un failover automatico non pianificato (AUFO). Quando è in corso un'operazione di spostamento del volume quando viene attivato l'AUFO, lo spostamento del volume si blocca.

### **Soluzione:**

Interrompere l'istanza di spostamento del volume bloccata e riavviare l'operazione di spostamento del volume.

## **La release di SnapMirror non riesce quando non è possibile eliminare la copia Snapshot**

### **Problema:**

L'operazione di rilascio di SnapMirror non riesce quando non è possibile eliminare la copia Snapshot.

### **Soluzione:**

La copia Snapshot contiene un tag transitorio. Utilizzare `snapshot delete` con il `-ignore-owners` Opzione per rimuovere la copia Snapshot transitoria.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners  
true -force true
```

Riprovare `snapmirror release` comando.

## **La copia Snapshot di riferimento per lo spostamento del volume viene visualizzata come la più recente**

### **Problema:**

Dopo aver eseguito un'operazione di spostamento del volume su un volume di gruppo di coerenza, la copia Snapshot di riferimento dello spostamento del volume potrebbe essere visualizzata come la più recente per la relazione SnapMirror.

È possibile visualizzare la copia Snapshot più recente con il seguente comando:

```
snapmirror show -fields newest-snapshot status -expand
```

### **Soluzione:**

Eseguire manualmente un `snapmirror resync` oppure attendere la successiva risincronizzazione automatica al termine dell'operazione di spostamento del volume.

# **Servizio mediatore per MetroCluster e SnapMirror Business Continuity**

## **Panoramica del mediatore ONTAP**

Il mediatore ONTAP offre diverse funzioni per le funzioni di ONTAP:

- Fornisce un archivio persistente e recintato per i metadati ha.

- Funge da proxy ping per la vivacità del controller.
- Fornisce una funzionalità di query sincrona sullo stato dei nodi per agevolare la determinazione del quorum.

Il mediatore ONTAP offre due servizi aggiuntivi di `systemctl`:

- **`ontap_mediator.service`**

Mantiene il server REST API per la gestione delle relazioni ONAP.

- **`mediator-scst.service`**

Controlla l'avvio e lo spegnimento del modulo iSCSI (SCST).

## Strumenti forniti all'amministratore di sistema

Strumenti forniti all'amministratore di sistema:

- **`/usr/local/bin/mediator_change_password`**

Imposta una nuova password API quando vengono forniti il nome utente e la password API correnti.

- **`/usr/local/bin/mediator_change_user`**

Imposta un nuovo nome utente API quando vengono forniti il nome utente e la password API correnti.

- **`/usr/local/bin/mediator_generate_support_bundle`**

Genera un file tgz locale contenente tutte le informazioni di supporto utili necessarie per la comunicazione con il supporto clienti NetApp. Ciò include la configurazione dell'applicazione, i registri e alcune informazioni di sistema. I bundle vengono generati sul disco locale e possono essere trasferiti manualmente, se necessario. Ubicazione dello storage: `/Opt/netapp/data/support_bundle/`

- **`/usr/local/bin/uninstall_ontap_mediator`**

Rimuove il pacchetto ONTAP Mediator e il modulo kernel SCST. Sono inclusi tutti i dati di configurazione, registri e mailbox.

- **`/usr/local/bin/mediator_unlock_user`**

Rilascia un blocco sull'account utente API se viene raggiunto il limite di tentativi di autenticazione. Questa funzione viene utilizzata per impedire la derivazione della password con forza bruta. Viene richiesto all'utente di inserire il nome utente e la password corretti.

- **`/usr/local/bin/mediator_add_user`**

(Solo supporto) utilizzato per aggiungere l'utente API al momento dell'installazione.

## Note speciali

ONTAP Mediator si affida a SCST per fornire iSCSI (vedere <http://scst.sourceforge.net/index.html>). Questo pacchetto è un modulo del kernel che viene compilato durante l'installazione specificamente per il kernel. Qualsiasi aggiornamento del kernel potrebbe richiedere la reinstallazione di SCST. In alternativa, disinstallare

e reinstallare il supporto ONTAP, quindi riconfigurare la relazione ONTAP.



Qualsiasi aggiornamento del kernel del sistema operativo del server deve essere coordinato con una finestra di manutenzione in ONTAP.

## Novità del mediatore ONTAP

Con ogni release vengono forniti nuovi miglioramenti al mediatore ONTAP. Ecco le novità.

### Miglioramenti

| Versione del mediatore ONTAP | Miglioramenti                                                                                                                                                                                                                                                 |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1,7                          | <ul style="list-style-type: none"><li>• Supporto per RHEL 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3</li><li>• Supporto per Rocky Linux 8 e 9</li></ul>                                                                                                     |
| 1.6                          | <ul style="list-style-type: none"><li>• Aggiornamenti di Python 3.9.</li><li>• Supporto per RHEL 8.4-8.8, 9.0-9.2, Rocky Linux 8 e 9.</li><li>• Supporto interrotto per tutte le release di RHEL 7.x / CentOS.</li></ul>                                      |
| 1.5                          | <ul style="list-style-type: none"><li>• Ottimizza la velocità per sistemi SMBC su larga scala.</li><li>• Firma del codice crittografico aggiunta al programma di installazione.</li><li>• Include avvisi di deprecazione per RHEL 7.x / CentOS 7.x.</li></ul> |
| 1.4                          | <ul style="list-style-type: none"><li>• Supporto per RHEL 8.4 e 8.5.</li><li>• Include SCST versione 3.6.0.</li><li>• Aggiunto supporto per Secure Boot (SB) del firmware basato su UEFI.</li></ul>                                                           |
| 1.3                          | <ul style="list-style-type: none"><li>• Supporto per RHEL/CentOS 8.2 e 8.3.</li><li>• Include SCST versione 3.5.0.</li></ul>                                                                                                                                  |
| 1.2                          | <ul style="list-style-type: none"><li>• Supporto per le cassette postali HTTPS.</li><li>• Per l'utilizzo con ONTAP 9.8+ MCC-IP AUSO e SM-BC ZRTO.</li><li>• Include SCST versione 3.4.0.</li></ul>                                                            |
| 1.1                          | <ul style="list-style-type: none"><li>• Supporto per RHEL/CentOS 7.6, 7.7, 8.0 e 8.1.</li><li>• Elimina le dipendenze Perl.</li><li>• Include SCST versione 3.4.0.</li></ul>                                                                                  |
| 1.0                          | <ul style="list-style-type: none"><li>• Supporto per cassette postali iSCSI.</li><li>• Per l'utilizzo con ONTAP 9.7+ MCC-IP AUSO.</li><li>• Supporto per RHEL/CentOS 7.6.</li></ul>                                                                           |

## Matrice di supporto del sistema operativo

| So per mediatore ONTAP | 1,7      | 1.6      | 1.5  | 1.4  | 1.3  | 1.2       | 1.1  | 1.0            |
|------------------------|----------|----------|------|------|------|-----------|------|----------------|
| 7.6                    | Obsoleto | Obsoleto | Sì   | Sì   | Sì   | Sì        | Sì   | Sì (solo RHEL) |
| 7.7                    | Obsoleto | Obsoleto | Sì   | Sì   | Sì   | Sì        | No   | No             |
| 7.8                    | Obsoleto | Obsoleto | Sì   | Sì   | Sì   | Sì        | No   | No             |
| 7.9                    | Obsoleto | Obsoleto | Sì   | Sì   | Sì   | Implicito | No   | No             |
| RHEL 8.0               | Obsoleto | Obsoleto | Sì   | Sì   | Sì   | Sì        | Sì   | No             |
| RHEL 8.1               | Obsoleto | Obsoleto | Sì   | Sì   | Sì   | Sì        | No   | No             |
| RHEL 8.2               | Obsoleto | Obsoleto | Sì   | Sì   | Sì   | No        | No   | No             |
| RHEL 8.3               | Obsoleto | Obsoleto | Sì   | Sì   | Sì   | No        | No   | No             |
| RHEL 8.4               | Obsoleto | Sì       | Sì   | Sì   | No   | No        | No   | No             |
| RHEL 8.5               | Sì       | Sì       | Sì   | Sì   | No   | No        | No   | No             |
| RHEL 8.6               | Sì       | Sì       | No   | No   | No   | No        | No   | No             |
| RHEL 8.7               | Sì       | Sì       | No   | No   | No   | No        | No   | No             |
| RHEL 8.8               | Sì       | Sì       | No   | No   | No   | No        | No   | No             |
| RHEL 9.0               | Sì       | Sì       | No   | No   | No   | No        | No   | No             |
| RHEL 9.1               | Sì       | Sì       | No   | No   | No   | No        | No   | No             |
| RHEL 9.2               | Sì       | Sì       | No   | No   | No   | No        | No   | No             |
| RHEL 9,3               | Sì       | No       | No   | No   | No   | No        | No   | No             |
| CentOS 8 e streaming   | No       | No       | No   | No   | No   | N/A.      | N/A. | N/A.           |
| Rocky Linux 8          | Sì       | Sì       | N/A. | N/A. | N/A. | N/A.      | N/A. | N/A.           |

|               |    |    |      |      |      |      |      |      |
|---------------|----|----|------|------|------|------|------|------|
| Rocky Linux 9 | Sì | Sì | N/A. | N/A. | N/A. | N/A. | N/A. | N/A. |
|---------------|----|----|------|------|------|------|------|------|

- Se non diversamente specificato, OS si riferisce alle release RedHat e CentOS.
- "No" significa che il sistema operativo e il mediatore ONTAP non sono compatibili.
- CentOS 8 è stato rimosso per tutte le release a causa della sua riramificazione. CentOS Stream non è stato considerato un sistema operativo di destinazione adatto per la produzione. Non è previsto alcun supporto.
- ONTAP Mediator 1.5 è stata l'ultima release supportata per i sistemi operativi delle filiali RHEL 7.x.
- ONTAP 1.6 aggiunge il supporto per Rocky Linux 8 e 9.

## Problemi risolti

| Data della modifica | Modificare l'ID | Descrizione                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 gennaio 2023     | 6567145         | <p>Sono state apportate le seguenti modifiche:</p> <ul style="list-style-type: none"> <li>• Supporto aggiunto per sistemi operativi aggiuntivi per ONTAP Mediator: RHEL 9.6, 8.7, 9.0 e 9.1.</li> <li>• Aggiunta della nuova versione 3.7.0 di SCST per sbloccare i problemi dei nuovi sistemi operativi supportati.</li> <li>• Supporto aggiunto per Rocky Linux: Rocky 8 e 9.</li> </ul> |
| 24 gennaio 2023     | 6621319         | Libreria SCST preinstallata consentita per le installazioni di ONTAP Mediator.                                                                                                                                                                                                                                                                                                             |
| 27 febbraio 2023    | 6623764         | Modifiche implementate per caricare sempre il modulo del kernel <code>scst_disk</code> al riavvio del servizio <code>mediator-scst</code> . Queste modifiche garantiscono che il servizio sia sempre pronto a creare nuove destinazioni iSCSI utilizzando la logica standard.                                                                                                              |
| 28 febbraio 2023    | 6625194         | Aggiunta di una nuova opzione al programma di installazione del mediatore ONTAP: <code>--skip-yum-dependencies</code>                                                                                                                                                                                                                                                                      |
| 24 marzo 2023       | 6652840         | Aggiornamento del programma di installazione di ONTAP Mediator in modo da poter reinstallare o riparare l'installazione di SCST.                                                                                                                                                                                                                                                           |
| 27 marzo 2023       | 6655179         | Risolto un problema di analisi che si verificava quando veniva attivata la raccolta di bundle di supporto con una password complessa.                                                                                                                                                                                                                                                      |
| 28 marzo 2023       | 6656739         | La logica di confronto SCST è stata modificata in modo da installare la versione corretta quando viene aggiornato ONTAP Mediator.                                                                                                                                                                                                                                                          |



## Installare o aggiornare

### Preparazione all'installazione o all'aggiornamento del servizio ONTAP Mediator

Per installare il servizio ONTAP Mediator, è necessario assicurarsi che tutti i prerequisiti siano soddisfatti, scaricare il pacchetto di installazione ed eseguire il programma di installazione sull'host. Questa procedura viene utilizzata per un'installazione o un aggiornamento di un'installazione esistente.

#### A proposito di questa attività

- A partire da ONTAP 9.7, è possibile utilizzare qualsiasi versione di ONTAP Mediator per monitorare una configurazione IP MetroCluster.
- A partire da ONTAP 9.8, è possibile utilizzare qualsiasi versione di ONTAP Mediator per monitorare una relazione SM-BC.

#### Prima di iniziare

È necessario soddisfare i seguenti prerequisiti.

| Versione del mediatore ONTAP | Versioni Linux supportate                                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1,7                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 8,5, 8,6, 8,7, 8,8, 8,9, 9,0, 9,1, 9,2 e 9,3</li><li>• Rocky Linux 8 e 9</li></ul>         |
| 1.6                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 8.4, 8.5, 8.6, 8.7, 8.8, 9.0, 9.1, 9.2</li><li>• Rocky Linux 8 e 9</li></ul>               |
| 1.5                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul> |
| 1.4                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul> |
| 1.3                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3</li><li>• CentOS: 7.6, 7.7, 7.8, 7.9</li></ul>           |
| 1.2                          | <ul style="list-style-type: none"><li>• Red Hat Enterprise Linux: 7.6, 7.7, 7.8, 8.1</li><li>• CentOS: 7.6, 7.7, 7.8</li></ul>                               |



La versione del kernel deve corrispondere alla versione del sistema operativo.

- installazione fisica a 64 bit o macchina virtuale
- 8 GB DI RAM
- 1 GB di spazio su disco (utilizzato per l'installazione delle applicazioni, i log dei server e il database)
- Utente: Accesso root

Tutti i pacchetti di librerie, ad eccezione del kernel, possono essere aggiornati in modo sicuro, ma potrebbero richiedere un riavvio per influire sull'applicazione ONTAP Mediator. Quando è necessario riavviare il sistema, si consiglia di utilizzare una finestra di servizio.

Se si installa `yum-utils` è possibile utilizzare `needs-restarting` comando.

Il core del kernel può essere aggiornato se viene aggiornato a una versione ancora supportata dalla matrice di versione di ONTAP Mediator. Il riavvio è obbligatorio, pertanto è necessaria una finestra di servizio.

Il modulo kernel SCST deve essere disinstallato prima del riavvio, quindi reinstallato dopo il riavvio.



L'aggiornamento a un kernel oltre la release del sistema operativo supportata per la release specifica di ONTAP Mediator non è supportato. (Questo probabilmente indica che il modulo SCST testato non viene compilato).

### Registrare una chiave di protezione quando UEFI Secure Boot è attivato

Se l'avvio protetto UEFI è attivato, per installare ONTAP Mediator è necessario registrare una chiave di protezione prima che il servizio ONTAP Mediator possa avviarsi. Per determinare se il sistema è abilitato per UEFI e l'avvio protetto è attivato, procedere come segue:

#### Fasi

1. Se `mokutil` non è installato, eseguire il seguente comando:

```
yum install mokutil
```

2. Per determinare se UEFI Secure Boot è attivato sul sistema, eseguire il comando seguente:

```
mokutil --sb-state
```

I risultati mostrano se l'avvio protetto UEFI è abilitato su questo sistema.



ONTAP Mediator 1.2.0 e le versioni precedenti non supportano questa modalità.

### Disattivare l'avvio protetto UEFI

È inoltre possibile scegliere di disattivare l'avvio protetto UEFI prima di installare ONTAP Mediator.

#### Fasi

1. Nelle impostazioni del BIOS della macchina fisica, disattivare l'opzione "UEFI Secure Boot" (Avvio protetto UEFI).
2. Nelle impostazioni VMware per la VM, disattivare l'opzione "Avvio sicuro" per vSphere 6.x o l'opzione "Avvio sicuro" per vSphere 7.x

### Aggiornare il sistema operativo host, quindi il mediatore ONTAP

Per aggiornare il sistema operativo host per ONTAP Mediator a una versione successiva, è necessario prima disinstallare ONTAP Mediator.

#### Prima di iniziare

Le procedure consigliate per l'installazione di Red Hat Enterprise Linux o Rocky Linux e dei repository associati sul vostro sistema sono elencate di seguito. I sistemi installati o configurati in modo diverso

potrebbero richiedere ulteriori passaggi.

- È necessario installare Red Hat Enterprise Linux o Rocky Linux secondo le Best practice di Red Hat. A causa della fine del ciclo di vita del supporto per le versioni di CentOS 8.x, si sconsiglia di utilizzare le versioni compatibili di CentOS 8.x.
- Durante l'installazione del servizio ONTAP Mediator su Red Hat Enterprise Linux o Rocky Linux, il sistema deve avere accesso al repository appropriato in modo che il programma di installazione possa accedere e installare tutte le dipendenze software richieste.
- Affinché il programma di installazione di yum trovi il software dipendente nei repository Red Hat Enterprise Linux, devi aver registrato il sistema durante l'installazione di Red Hat Enterprise Linux o in seguito utilizzando un abbonamento Red Hat valido.

Per informazioni su Red Hat Subscription Manager, consulta la documentazione di Red Hat.

- Le seguenti porte devono essere inutilizzate e disponibili per Mediator:
  - 31784
  - 3260
- Se si utilizza un firewall di terze parti: Fare riferimento a. ["Requisiti del firewall per ONTAP Mediator"](#)
- Se l'host Linux si trova in una posizione senza accesso a Internet, è necessario assicurarsi che i pacchetti richiesti siano disponibili in un repository locale.

Se si utilizza il protocollo LACP (link Aggregation Control Protocol) in un ambiente Linux, è necessario configurare correttamente il kernel e assicurarsi di `sysctl net.ipv4.conf.all.arp_ignore` è impostato su "2".

**Di cosa hai bisogno**

I seguenti pacchetti sono richiesti dal servizio di supporto ONTAP:

| Tutte le versioni RHEL/CentOS                                                                                                                                                                                                                                                                                  | Pacchetti aggiuntivi per RHEL 8.x / Rocky Linux 8                                                                                                                                                          | Pacchetti aggiuntivi per RHEL 9.x / Rocky Linux 9                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• openssl</li><li>• openssl-devel</li><li>• kernel-devel- (uname -r)</li><li>• gcc</li><li>• fare</li><li>• libselineutils</li><li>• patch</li><li>• bzip2</li><li>• perl-Data-Dumper</li><li>• perl-ExtUtils-MakeMaker</li><li>• efibootmgr</li><li>• mokutil</li></ul> | <ul style="list-style-type: none"><li>• python3-pip</li><li>• elfutils-libelf-devel</li><li>• policycoreutils-python-utils</li><li>• redhat-lsb-core</li><li>• python39</li><li>• python39-devel</li></ul> | <ul style="list-style-type: none"><li>• python3-pip</li><li>• elfutils-libelf-devel</li><li>• policycoreutils-python-utils</li><li>• python3</li><li>• python3-devel</li></ul> |

Il pacchetto di installazione di Mediator è un file tar compresso autoestraente che include:

- Un file RPM contenente tutte le dipendenze che non è possibile ottenere dal repository della release supportata.
- Uno script di installazione.

Si consiglia una certificazione SSL valida.

### A proposito di questa attività

Quando si aggiorna il sistema operativo host per ONTAP Mediator a una versione successiva (ad esempio, da 7.x a 8.x) utilizzando il tool leapp-upgrade, È necessario disinstallare ONTAP Mediator perché lo strumento cerca di rilevare nuove versioni degli RPM installati nei repository registrati con il sistema.

Poiché un file .rpm è stato installato come parte del programma di installazione di ONTAP Mediator, viene incluso nella ricerca. Tuttavia, poiché il file .rpm è stato decompresso come parte del programma di installazione e non scaricato da un repository registrato, non è possibile trovare un aggiornamento. In questo caso, il tool leapp-upgrade disinstalla il pacchetto.

Per conservare i file di log, che verranno utilizzati per il triage dei casi di supporto, è necessario eseguire il backup dei file prima di eseguire un aggiornamento del sistema operativo e ripristinarli dopo la reinstallazione del pacchetto ONTAP Mediator. Poiché il mediatore ONTAP viene reinstallato, tutti i cluster ONTAP ad esso connessi dovranno essere riconnessi dopo la nuova installazione.



Le seguenti operazioni devono essere eseguite nell'ordine indicato. Subito dopo aver reinstallato ONTAP Mediator, interrompere il servizio ontap\_mediator, sostituire i file di log e riavviare il servizio. In questo modo, i registri non andranno persi.

### Fasi

1. Eseguire il backup dei file di log.

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Esegui l'upgrade con il tool di aggiornamento leapp.

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
..<snip upgrade checks>..
..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

### 3. Reinstallare il mediatore ONTAP.



Eseguire il resto della procedura immediatamente dopo la reinstallazione di ONTAP Media per evitare la perdita dei file di log.

```
[rootmediator-host ~]# ontap-mediator-1.6.0/ontap-mediator-1.6.0

ONTAP Mediator: Self Extracting Installer

..<snip installation>..
[rootmediator-host ~]#
```

### 4. Arrestare il servizio ontap\_mediator.

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

### 5. Sostituire i file di log.

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

### 6. Avviare il servizio ontap\_mediator.

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

### 7. Ricollegare tutti i cluster ONTAP al mediatore ONTAP aggiornato

## Procedura per MetroCluster over IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
Status      Status
-----
-----
172.31.40.122
31784      siteA-node2      true      false
              siteA-node1      true      false
              siteB-node2      true      false
              siteB-node2      true      false

siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover.
It may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP      Port      Node      Configuration
Connection
Status      Status
-----
-----
172.31.40.122
31784      siteA-node2      true      true
              siteA-node1      true      true
              siteB-node2      true      true
              siteB-node2      true      true

siteA::>
```

## Procedura per la Business Continuity di SnapMirror

Per SnapMirror Business Continuity, se il certificato TLS è stato installato al di fuori della directory /opt/netapp, non sarà necessario reinstallarlo. Se si utilizza il certificato autofirmato generato per impostazione predefinita o si mette il certificato personalizzato nella directory /opt/netapp, eseguire il backup e il ripristino.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
172.31.49.237    peer2                unreachable      true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39

Job ID Name                      Owing
Vserver      Node                      State
-----
39    mediator remove    peer1    peer1-node1    Success
Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver      Serial Number  Certificate Name
Type
-----
peer1
4A790360081F41145E14C5D7CE721DC6C210007F
ONTAPMediatorCA
server-ca
Certificate Authority: ONTAP Mediator CA
Expiration Date: Mon Apr 17 10:27:54 2017

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer1::> security certificate install -type server-ca -vserver
peer1

Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for
future reference.
```

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

```
peer2::> security certificate delete -common-name ONTAPMediatorCA *  
1 entry was deleted.
```

```
peer2::> security certificate install -type server-ca -vserver peer2
```

```
  Please enter Certificate: Press <Enter> when done  
  ..<snip ONTAP Mediator CA public key>..
```

You should keep a copy of the CA-signed digital certificate for future reference.

The installed certificate's CA and serial number for reference:

CA: ONTAP Mediator CA

serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

```
peer1::> snapmirror mediator add -mediator-address 172.31.49.237  
-peer-cluster peer2 -username mediatoradmin
```

Notice: Enter the mediator password.

Enter the password:

Enter the password again:

Info: [Job: 43] 'mediator add' job queued

```
peer1::> job show -id 43
```

| Job                                    | ID | Name         | Owning<br>Vserver | Node        | State   |
|----------------------------------------|----|--------------|-------------------|-------------|---------|
| 43                                     |    | mediator add | peer1             | peer1-node2 | Success |
| Description: Creating a mediator entry |    |              |                   |             |         |

```
peer1::> snapmirror mediator show
```

| Mediator Address | Peer  | Cluster | Connection | Status | Quorum | Status |
|------------------|-------|---------|------------|--------|--------|--------|
| 172.31.49.237    | peer2 |         | connected  |        | true   |        |



```
peer1::>
```

### Abilitare l'accesso ai repository

È necessario abilitare l'accesso ai repository in modo che ONTAP Mediator possa accedere ai pacchetti richiesti durante il processo di installazione

#### Fasi

1. Determinare quali repository devono essere utilizzati, come mostrato nella tabella seguente:

| Se il sistema operativo in uso è... | È necessario fornire l'accesso a questi repository...                                                                      |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| RHEL 7.x                            | <ul style="list-style-type: none"><li>• rhel-7-server-optional-rpms</li></ul>                                              |
| RHEL 8.x                            | <ul style="list-style-type: none"><li>• rhel-8-for-x86_64-baseos-rpms</li><li>• rhel-8-for-x86_64-appstream-rpms</li></ul> |
| RHEL 9.x                            | <ul style="list-style-type: none"><li>• rhel-9-for-x86_64-baseos-rpms</li><li>• rhel-9-for-x86_64-appstream-rpms</li></ul> |
| CentOS 7.x                          | <ul style="list-style-type: none"><li>• C7.6.1810 - repository di base</li></ul>                                           |
| Rocky Linux 8                       | <ul style="list-style-type: none"><li>• appstream</li><li>• baseos</li></ul>                                               |
| Rocky Linux 9                       | <ul style="list-style-type: none"><li>• appstream</li><li>• baseos</li></ul>                                               |

2. Utilizzare una delle seguenti procedure per abilitare l'accesso ai repository elencati in precedenza, in modo che ONTAP Media possa accedere ai pacchetti richiesti durante il processo di installazione.

## Procedura per il sistema operativo RHEL 7.x.

Utilizzare questa procedura se il sistema operativo in uso è **RHEL 7.x** per consentire l'accesso ai repository:

### Fasi

1. Iscriviti al repository richiesto:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

Nell'esempio seguente viene illustrata l'esecuzione di questo comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-  
server-optional-rpms  
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. Eseguire `yum repolist` comando.

Nell'esempio riportato di seguito viene illustrata l'esecuzione di questo comando. Il repository "rhel-7-server-optional-rpms" dovrebbe apparire nell'elenco.

```
[root@localhost ~]# yum repolist  
Loaded plugins: product-id, search-disabled-repos, subscription-  
manager  
rhel-7-server-optional-rpms | 3.2 kB  00:00:00  
rhel-7-server-rpms | 3.5 kB  00:00:00  
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group  
| 26 kB  00:00:00  
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo  
| 2.5 MB  00:00:00  
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db  
| 8.3 MB  00:00:01  
repo id                                repo name  
status  
rhel-7-server-optional-rpms/7Server/x86_64  Red Hat Enterprise  
Linux 7 Server - Optional (RPMs)  19,447  
rhel-7-server-rpms/7Server/x86_64          Red Hat Enterprise  
Linux 7 Server (RPMs)              26,758  
repolist: 46,205  
[root@localhost ~]#
```

## Procedura per il sistema operativo RHEL 8.x.

Utilizzare questa procedura se il sistema operativo in uso è **RHEL 8.x** per abilitare l'accesso ai repository:

### Fasi

1. Iscriviti al repository richiesto:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

Nell'esempio seguente viene illustrata l'esecuzione di questo comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Eseguire `yum repolist` comando.

I repository appena sottoscritti dovrebbero apparire nell'elenco.

## Procedura per il sistema operativo RHEL 9.x.

Utilizzare questa procedura se il sistema operativo in uso è **RHEL 9.x** per consentire l'accesso ai repository:

### Fasi

1. Iscriviti al repository richiesto:

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms  
  
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

Nell'esempio seguente viene illustrata l'esecuzione di questo comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-  
x86_64-baseos-rpms  
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this  
system.  
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-  
x86_64-appstream-rpms  
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this  
system.
```

2. Eseguire `yum repolist` comando.

I repository appena sottoscritti dovrebbero apparire nell'elenco.

## Procedura per il sistema operativo CentOS 7.x.

Utilizzare questa procedura se il sistema operativo in uso è **CentOS 7.x** per consentire l'accesso ai repository:



I seguenti esempi mostrano un repository per CentOS 7.6 e potrebbero non funzionare per altre versioni di CentOS. Utilizza il repository di base per la tua versione di CentOS.

### Fasi

1. Aggiungere il repository di base C7.6.1810. Il repository dei vault di base di C7.6.1810 contiene il pacchetto "kernel-devel" necessario per il mediatore ONTAP.
2. Aggiungere le seguenti righe a /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Eseguire `yum repolist` comando.

Nell'esempio riportato di seguito viene illustrata l'esecuzione di questo comando. Il repository CentOS-7.6.1810 - base dovrebbe apparire nell'elenco.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: distro.ibiblio.org
* extras: distro.ibiblio.org
* updates: ewr.edge.kernel.org
C7.6.1810-base | 3.6 kB 00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz | 166 kB 00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db | 6.0 MB 00:00:04
repo id repo name status
C7.6.1810-base/x86_64 CentOS-7.6.1810 - Base 10,019
base/7/x86_64 CentOS-7 - Base 10,097
extras/7/x86_64 CentOS-7 - Extras 307
updates/7/x86_64 CentOS-7 - Updates 1,010
repolist: 21,433
[root@localhost ~]#
```

## Procedura per i sistemi operativi Rocky Linux 8 o 9

Utilizzare questa procedura se il sistema operativo in uso è **Rocky Linux 8** o **Rocky Linux 9** per consentire l'accesso ai repository:

### Fasi

1. Iscriviti ai repository richiesti:

```
dnf config-manager --set-enabled baseos  
  
dnf config-manager --set-enabled appstream
```

2. Eseguire una clean funzionamento:

```
dnf clean all
```

3. Verificare l'elenco dei repository:

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos  
[root@localhost ~]# dnf config-manager --set-enabled appstream  
[root@localhost ~]# dnf clean all  
[root@localhost ~]# dnf repolist  
repo id                                repo name  
appstream                              Rocky Linux 8 - AppStream  
baseos                                  Rocky Linux 8 - BaseOS  
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos  
[root@localhost ~]# dnf config-manager --set-enabled appstream  
[root@localhost ~]# dnf clean all  
[root@localhost ~]# dnf repolist  
repo id                                repo name  
appstream                              Rocky Linux 9 - AppStream  
baseos                                  Rocky Linux 9 - BaseOS  
[root@localhost ~]#
```

## Scarica il pacchetto di installazione di Mediator

Scarica il pacchetto di installazione di Mediator come parte del processo di installazione.

### Fasi

1. Scarica il pacchetto di installazione di Mediator dalla pagina del mediatore ONTAP.

["Pagina di download del mediatore ONTAP"](#)

2. Verificare che il pacchetto di installazione di Mediator si trovi nella directory di lavoro corrente:

```
ls
```

```
[root@mediator-host ~]#ls
ontap-mediator-1.7.0.tgz
```



Per le versioni 1.4 e precedenti di ONTAP Mediator, il programma di installazione è denominato `ontap-mediator`.

Se ci si trova in una posizione senza accesso a Internet, è necessario assicurarsi che il programma di installazione abbia accesso ai pacchetti richiesti.

3. Se necessario, spostare il pacchetto di installazione di Mediator dalla directory di download alla directory di installazione sull'host Linux Mediator.
4. Decomprimere il pacchetto di installazione:

```
tar xvfz ontap-mediator-1.7.0.tgz
```

```
[root@scs000099753 ~]# tar xvfz ontap-mediator-1.7.0.tgz
ontap-mediator-1.7.0/
ontap-mediator-1.7.0/ONTAP-Mediator-production.pub
ontap-mediator-1.7.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.7.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.7.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.7.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.7.0/ontap-mediator-1.7.0
ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig.tsr
ontap-mediator-1.7.0/ontap-mediator-1.7.0.tsr
ontap-mediator-1.7.0/ontap-mediator-1.7.0.sig
```

## Verificare la firma del codice del mediatore ONTAP

Prima di installare il pacchetto di installazione di ONTAP, verificare la firma del codice del mediatore.

### Prima di iniziare

Prima di verificare la firma del codice Mediator, il sistema deve soddisfare i seguenti requisiti.

- openssl versioni da 1.0.2 a 3.0 per la verifica di base
- openssl versione 1.1.0 o successiva per le operazioni TSA (Time Stamping Authority)
- Accesso a Internet pubblico per la verifica OCSP

I seguenti file sono inclusi nel pacchetto di download:

| File                              | Descrizione                                                                                                   |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------|
| ONTAP-Mediator-development.pub    | Chiave pubblica utilizzata per verificare la firma                                                            |
| csc-prod-chain-ONTAP-Mediator.pem | Catena di trust della CA per la certificazione pubblica                                                       |
| csc-prod-ONTAP-Mediator.pem       | Il certificato utilizzato per generare la chiave                                                              |
| ontap-mediator-1.7.0              | Il file eseguibile di installazione del prodotto per la versione 1.7.0                                        |
| ontap-mediator-1.7.0.sig          | SHA-256 ha eseguito l'hashing, quindi ha firmato RSA utilizzando la chiave csc-PROD, firma per l'installatore |
| ontap-mediator-1.7.0.sig.tsr      | La richiesta di revoca per l'utilizzo da parte di OCSCP per la firma dell'installatore                        |
| tsc-prod-ONTAP-Mediator.pem       | Il certificato pubblico per il TSR                                                                            |
| tsc-prod-chain-ONTAP-Mediator.pem | La catena CA del certificato pubblico per il TSR                                                              |

## Fasi

1. Eseguire il controllo della revoca su `csc-prod-ONTAP-Mediator.pem` Utilizzando il protocollo OCSP (Online Certificate Status Protocol).
  - a. Individuare l'URL OCSP utilizzato per registrare il certificato perché i certificati dello sviluppatore potrebbero non fornire un uri.

```
openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
```

- b. Generare una richiesta OCSP per il certificato.

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout req.der
```

- c. Connettersi a OCSP Manager per inviare la richiesta OCSP:

```
openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-chain-ONTAP-Mediator.pem
```



2. Verificare la catena di attendibilità del CSC e le date di scadenza rispetto all'host locale:

```
openssl verify
```



Il openssl La versione dal PERCORSO deve avere un valido cert.pem (non autofirmato).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. Verificare ontap-mediator-1.6.0.sig.tsr e ontap-mediator-1.7.0.tsr file che utilizzano i certificati associati:

```
openssl ts -verify
```



.tsr i file contengono la risposta di time stamp associata al programma di installazione e la firma del codice. L'elaborazione conferma che il timestamp ha una firma valida da TSA e che il file di input non è stato modificato. La verifica viene eseguita localmente sul computer. Indipendentemente, non è necessario accedere ai server TSA.

```
openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-
ONTAP-Mediator.pem
```

4. Verificare le firme rispetto alla chiave:

```
openssl dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
```

## Esempio di verifica della firma del codice del mediatore ONTAP (output della console)

```
[root@scspa2695423001 ontap-mediator-1.7.0]# pwd
/root/ontap-mediator-1.7.0
[root@scspa2695423001 ontap-mediator-1.7.0]# ls -l
total 63660
-r--r--r-- 1 root root      8582 Feb 19 15:02 csc-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root      2373 Feb 19 15:02 csc-prod-ONTAP-
Mediator.pem
-r-xr-xr-- 1 root root 65132818 Feb 20 15:17 ontap-mediator-1.7.0
-rw-r--r-- 1 root root      384 Feb 20 15:17 ontap-mediator-1.7.0.sig
-rw-r--r-- 1 root root      5437 Feb 20 15:17 ontap-mediator-
1.7.0.sig.tsr
-rw-r--r-- 1 root root      5436 Feb 20 15:17 ontap-mediator-1.7.0.tsr
-r--r--r-- 1 root root      625 Feb 19 15:02 ONTAP-Mediator-
production.pub
-r--r--r-- 1 root root      3323 Feb 19 15:02 tsa-prod-chain-ONTAP-
Mediator.pem
-r--r--r-- 1 root root      1740 Feb 19 15:02 tsa-prod-ONTAP-
Mediator.pem
[root@scspa2695423001 ontap-mediator-1.7.0]#
[root@scspa2695423001 ontap-mediator-1.7.0]#
/root/verify_ontap_mediator_signatures.sh
++ openssl version -d
++ cut -d '"' -f2
+ OPENSSLDIR=/etc/pki/tls
+ openssl version
OpenSSL 1.1.1k  FIPS 25 Mar 2021
++ openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
+ ocsp_uri=http://ocsp.entrust.net
+ echo http://ocsp.entrust.net
http://ocsp.entrust.net
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -reqout
req.der
+ openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem -url
http://ocsp.entrust.net -resp_text -respout resp.der -verify_other csc-
prod-chain-ONTAP-Mediator.pem
OCSP Response Data:
    OCSP Response Status: successful (0x0)
    Response Type: Basic OCSP Response
    Version: 1 (0x0)
    Responder Id: C = US, O = "Entrust, Inc.", CN = Entrust Extended
Validation Code Signing CA - EVCS2
```

Produced At: Feb 28 05:01:00 2023 GMT

Responses:

Certificate ID:

Hash Algorithm: sha1

Issuer Name Hash: 69FA640329AB84E27220FE0927647B8194B91F2A

Issuer Key Hash: CE894F8251AA15A28462CA312361D261F8FE78

Serial Number: 511A542B57522AEB7295A640DC6200E5

Cert Status: good

This Update: Feb 28 05:00:00 2023 GMT

Next Update: Mar 4 04:59:59 2023 GMT

Signature Algorithm: sha512WithRSAEncryption

3c:1d:49:b0:93:62:37:3e:c7:38:e3:9f:9f:62:82:73:ed:f4:  
ea:00:6b:f1:01:cd:79:57:92:f1:9d:5d:85:9b:60:59:f8:6c:  
e6:f4:50:51:f3:4c:8a:51:dd:50:68:16:8f:20:24:7e:39:b0:  
44:94:8d:b0:61:da:b9:08:36:74:2d:44:55:62:fb:92:be:4a:  
e7:6c:8c:49:dd:0c:fd:d8:ce:20:08:0d:0f:5a:29:a3:19:03:  
9f:d3:df:41:f4:89:0f:73:18:3f:ac:bb:a7:a3:96:7d:c5:70:  
4c:57:cd:17:17:c6:8a:60:d1:37:c9:2d:81:07:2a:d7:a6:02:  
ee:ce:88:16:22:db:e3:43:64:1e:9b:0d:4d:31:66:fa:ab:a5:  
52:99:94:4a:4a:d0:52:c5:34:f5:18:c7:15:5b:ce:74:c2:fc:  
61:ea:55:aa:f1:2f:82:a3:6a:95:8d:7e:2b:38:49:4f:bf:b1:  
68:7b:1b:24:8b:1f:4d:c5:77:f0:71:af:9c:34:c8:7a:82:50:  
09:a2:19:6e:c6:30:4f:da:a2:79:08:f9:d0:ff:85:d9:2a:84:  
cf:0c:aa:75:8f:72:c9:a7:a2:83:e8:8b:cf:ed:0c:69:75:b6:  
2a:7b:6b:58:99:01:d8:34:ad:e1:89:25:27:1b:fa:d9:6d:32:  
97:3a:0b:0a:8e:a3:9e:e3:f4:e0:d6:1a:c9:b5:14:8c:3e:54:  
3b:37:17:1a:93:44:84:8b:4a:87:97:1e:76:43:3e:d3:ec:8b:  
7e:56:4a:3f:01:31:c0:e5:58:fb:50:ce:6f:b1:e7:35:f9:b7:  
a3:ef:6b:3b:21:95:37:a6:5b:8f:f0:15:18:36:65:89:a1:9c:  
9b:69:00:b4:b1:65:6a:bc:11:2d:d4:9b:b4:97:cc:cb:7a:0c:  
16:11:c1:75:58:7e:13:ab:56:3c:3f:93:5b:95:24:c6:54:52:  
1f:86:a9:16:ce:d9:ea:8b:3a:f3:4f:c4:8f:ad:de:e8:3e:3c:  
d2:51:51:ad:33:7f:d8:c5:33:24:26:f1:2d:9d:0e:9f:55:d0:  
68:bf:af:bd:68:4a:40:08:bc:92:a0:62:54:7d:16:7b:36:29:  
15:b1:cd:58:8e:fb:4a:f2:3e:94:8b:fe:56:95:cc:24:32:af:  
5f:71:99:18:ed:0c:64:94:f7:54:48:87:48:d0:6d:b3:42:04:  
96:03:73:a2:8e:8a:6a:b2:af:ee:56:19:a1:c6:35:12:59:ad:  
19:6a:fe:e0:f1:27:cc:96:4e:f0:4f:fb:6a:bd:ce:05:2c:aa:  
79:7c:df:02:5c:ca:53:7d:60:12:88:7c:ce:15:c7:d4:02:27:  
c1:ab:cf:71:30:1e:14:ba

WARNING: no nonce in response

Response verify OK

csc-prod-ONTAP-Mediator.pem: good

This Update: Feb 28 05:00:00 2023 GMT

Next Update: Mar 4 04:59:59 2023 GMT

```

+ openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls csc-prod-ONTAP-Mediator.pem
csc-prod-ONTAP-Mediator.pem: OK
+ openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
/etc/pki/tls tsa-prod-ONTAP-Mediator.pem
tsa-prod-ONTAP-Mediator.pem: OK
+ openssl ts -verify -data ontap-mediator-1.7.0.sig -in ontap-mediator-
1.7.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl ts -verify -data ontap-mediator-1.7.0 -in ontap-mediator-
1.7.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
Using configuration from /etc/pki/tls/openssl.cnf
Verification: OK
+ openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.7.0.sig ontap-mediator-1.7.0
Verified OK
[root@scspa2695423001 ontap-mediator-1.7.0]#

```

## Installare il pacchetto di installazione di ONTAP Mediator

Per installare il servizio di supporto ONTAP, è necessario ottenere il pacchetto di installazione ed eseguire il programma di installazione sull'host.

### Fasi

1. Eseguire il programma di installazione e rispondere alle richieste come richiesto:

```
./ontap-mediator-1.7.0/ontap-mediator-1.7.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.5.0/ontap-mediator-1.7.0 -y
```

Il processo di installazione procede alla creazione degli account richiesti e all'installazione dei pacchetti richiesti. Se sull'host è installata una versione precedente di Mediator, viene richiesto di confermare l'aggiornamento.

2. A partire da ONTAP Mediator 1.4, il meccanismo di avvio sicuro è abilitato sui sistemi UEFI. Quando Secure Boot è attivato, è necessario eseguire ulteriori operazioni per registrare la chiave di sicurezza dopo l'installazione:

- Seguire le istruzioni nel file README per firmare il modulo del kernel SCST:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

- Individuare le chiavi richieste:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```



Dopo l'installazione, i file README e la posizione della chiave vengono forniti anche nell'output di sistema.

## Esempio di installazione di ONTAP Mediator 1,6 (uscita console)

```
[root@scs000099753 ~]# ./ontap-mediator-1.6.0/ontap-mediator-1.6.0 -y
ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
  Using openssl from the path: /usr/bin/openssl configured for
  CApath:/etc/pki/tls

+ Unpacking the ONTAP Mediator installer
ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Using default account names: netapp + mediatoradmin

Enter ONTAP Mediator user account (mediatoradmin) password:

Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode

+ Checking for default Linux firewall
success
success
success

#####
Preparing for installation of ONTAP Mediator packages.

+ Installing required packages.

Last metadata expiration check: 0:25:24 ago on Fri 21 Oct 2022 04:00:13
PM EDT.
Package openssl-1:1.1.1k-4.el8.x86_64 is already installed.
Package gcc-8.4.1-1.el8.x86_64 is already installed.
Package python36-3.6.8-2.module+el8.1.0+3334+5cb623d7.x86_64 is already
installed.
Package libselinux-utils-2.9-5.el8.x86_64 is already installed.
Package perl-Data-Dumper-2.167-399.el8.x86_64 is already installed.
Package efibootmgr-16-1.el8.x86_64 is already installed.
Package mokutil-1:0.3.0-11.el8.x86_64 is already installed.
```

Package python3-pip-9.0.3-19.el8.noarch is already installed.  
 Package polycoreutils-python-utils-2.9-14.el8.noarch is already installed.  
 Dependencies resolved.

| =====                                  |              |  |             |
|----------------------------------------|--------------|--|-------------|
| =====                                  |              |  |             |
| =====                                  |              |  |             |
| Package                                | Architecture |  |             |
| Version                                |              |  | Repository  |
| Size                                   |              |  |             |
| =====                                  |              |  |             |
| =====                                  |              |  |             |
| =====                                  |              |  |             |
| Installing:                            |              |  |             |
| bzip2                                  | x86_64       |  |             |
| 1.0.6-26.el8                           |              |  | rhel-8-for- |
| x86_64-baseos-rpms                     | 60 k         |  |             |
| elfutils-libelf-devel                  | x86_64       |  |             |
| 0.186-1.el8                            |              |  | rhel-8-for- |
| x86_64-baseos-rpms                     | 60 k         |  |             |
| kernel-devel                           | x86_64       |  |             |
| 4.18.0-348.el8                         |              |  | rhel-8-for- |
| x86_64-baseos-rpms                     | 20 M         |  |             |
| make                                   | x86_64       |  |             |
| 1:4.2.1-11.el8                         |              |  | rhel-8-for- |
| x86_64-baseos-rpms                     | 498 k        |  |             |
| openssl-devel                          | x86_64       |  |             |
| 1:1.1.1k-7.el8_6                       |              |  | rhel-8-for- |
| x86_64-baseos-rpms                     | 2.3 M        |  |             |
| patch                                  | x86_64       |  |             |
| 2.7.6-11.el8                           |              |  | rhel-8-for- |
| x86_64-baseos-rpms                     | 138 k        |  |             |
| perl-ExtUtils-MakeMaker                | noarch       |  |             |
| 1:7.34-1.el8                           |              |  | rhel-8-for- |
| x86_64-appstream-rpms                  | 301 k        |  |             |
| python36-devel                         | x86_64       |  |             |
| 3.6.8-38.module+el8.5.0+12207+5c5719bc |              |  | rhel-8-for- |
| x86_64-appstream-rpms                  | 17 k         |  |             |
| redhat-lsb-core                        | x86_64       |  |             |
| 4.1-47.el8                             |              |  | rhel-8-for- |
| x86_64-appstream-rpms                  | 45 k         |  |             |
| Upgrading:                             |              |  |             |
| cpp                                    | x86_64       |  |             |
| 8.5.0-10.1.el8_6                       |              |  | rhel-8-for- |
| x86_64-appstream-rpms                  | 10 M         |  |             |
| elfutils-libelf                        | x86_64       |  |             |

|                                        |       |        |             |
|----------------------------------------|-------|--------|-------------|
| 0.186-1.el8                            |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 229 k |        |             |
| elfutils-libs                          |       | x86_64 |             |
| 0.186-1.el8                            |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 295 k |        |             |
| gcc                                    |       | x86_64 |             |
| 8.5.0-10.1.el8_6                       |       |        | rhel-8-for- |
| x86_64-appstream-rpms                  | 23 M  |        |             |
| libgcc                                 |       | x86_64 |             |
| 8.5.0-10.1.el8_6                       |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 80 k  |        |             |
| libgomp                                |       | x86_64 |             |
| 8.5.0-10.1.el8_6                       |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 207 k |        |             |
| libsemanage                            |       | x86_64 |             |
| 2.9-8.el8                              |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 168 k |        |             |
| mokutil                                |       | x86_64 |             |
| 1:0.3.0-11.el8_6.1                     |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 46 k  |        |             |
| openssl                                |       | x86_64 |             |
| 1:1.1.1k-7.el8_6                       |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 709 k |        |             |
| openssl-libs                           |       | x86_64 |             |
| 1:1.1.1k-7.el8_6                       |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 1.5 M |        |             |
| platform-python-pip                    |       | noarch |             |
| 9.0.3-22.el8                           |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 1.6 M |        |             |
| policycoreutils                        |       | x86_64 |             |
| 2.9-19.el8                             |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 374 k |        |             |
| policycoreutils-python-utils           |       | noarch |             |
| 2.9-19.el8                             |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 253 k |        |             |
| python3-libsemanage                    |       | x86_64 |             |
| 2.9-8.el8                              |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 128 k |        |             |
| python3-pip                            |       | noarch |             |
| 9.0.3-22.el8                           |       |        | rhel-8-for- |
| x86_64-appstream-rpms                  | 20 k  |        |             |
| python3-policycoreutils                |       | noarch |             |
| 2.9-19.el8                             |       |        | rhel-8-for- |
| x86_64-baseos-rpms                     | 2.2 M |        |             |
| python36                               |       | x86_64 |             |
| 3.6.8-38.module+el8.5.0+12207+5c5719bc |       |        | rhel-8-for- |



```

x86_64-appstream-rpms                19 k
Installing dependencies:
  annobin                             x86_64
10.29-3.el8                           rhel-8-for-
x86_64-appstream-rpms                117 k
  at                                  x86_64
3.1.20-11.el8                         rhel-8-for-
x86_64-baseos-rpms                   81 k
  bc                                  x86_64
1.07.1-5.el8                         rhel-8-for-
x86_64-baseos-rpms                   129 k
  cups-client                        x86_64
1:2.2.6-38.el8                       rhel-8-for-
x86_64-appstream-rpms                169 k
  dwz                                x86_64
0.12-10.el8                          rhel-8-for-
x86_64-appstream-rpms                109 k
  ed                                  x86_64
1.14.2-4.el8                         rhel-8-for-
x86_64-baseos-rpms                   82 k
  efi-srpm-macros                    noarch
3-3.el8                              rhel-8-for-
x86_64-appstream-rpms                22 k
  esmtplib                           x86_64
1.2-15.el8                           EPEL-8
57 k
  glibc-srpm-macros                  noarch
1.4.2-7.el8                          rhel-8-for-
x86_64-appstream-rpms                9.4 k
  go-srpm-macros                     noarch
2-17.el8                             rhel-8-for-
x86_64-appstream-rpms                13 k
  keyutils-libs-devel                x86_64
1.5.10-6.el8                         rhel-8-for-
x86_64-baseos-rpms                   48 k
  krb5-devel                         x86_64
1.18.2-14.el8                       rhel-8-for-
x86_64-baseos-rpms                   560 k
  libcom_err-devel                   x86_64
1.45.6-2.el8                        rhel-8-for-
x86_64-baseos-rpms                   38 k
  libesmtplib                        x86_64
1.0.6-18.el8                        EPEL-8
70 k
  libkadm5                           x86_64
1.18.2-14.el8                       rhel-8-for-

```

|                       |       |        |             |
|-----------------------|-------|--------|-------------|
| x86_64-baseos-rpms    | 187 k |        |             |
| libblockfile          |       | x86_64 |             |
| 1.14-1.el8            |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 32 k  |        |             |
| libselenium-devel     |       | x86_64 |             |
| 2.9-5.el8             |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 200 k |        |             |
| libsepol-devel        |       | x86_64 |             |
| 2.9-3.el8             |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 87 k  |        |             |
| libverto-devel        |       | x86_64 |             |
| 0.3.0-5.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 18 k  |        |             |
| m4                    |       | x86_64 |             |
| 1.4.18-7.el8          |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 223 k |        |             |
| mailx                 |       | x86_64 |             |
| 12.5-29.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 257 k |        |             |
| ncurses-compat-libs   |       | x86_64 |             |
| 6.1-9.20180224.el8    |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 328 k |        |             |
| ocaml-srpm-macros     |       | noarch |             |
| 5-4.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 9.5 k |        |             |
| openblas-srpm-macros  |       | noarch |             |
| 2-2.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 8.0 k |        |             |
| pcre2-devel           |       | x86_64 |             |
| 10.32-2.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 605 k |        |             |
| pcre2-utf16           |       | x86_64 |             |
| 10.32-2.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 229 k |        |             |
| pcre2-utf32           |       | x86_64 |             |
| 10.32-2.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms    | 220 k |        |             |
| perl-CPAN-Meta-YAML   |       | noarch |             |
| 0.018-397.el8         |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 34 k  |        |             |
| perl-ExtUtils-Command |       | noarch |             |
| 1:7.34-1.el8          |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 19 k  |        |             |
| perl-ExtUtils-Install |       | noarch |             |
| 2.14-4.el8            |       |        | rhel-8-for- |
| x86_64-appstream-rpms | 46 k  |        |             |

|                        |       |        |             |
|------------------------|-------|--------|-------------|
| perl-ExtUtils-Manifest |       | noarch |             |
| 1.70-395.el8           |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 37 k  |        |             |
| perl-ExtUtils-ParseXS  |       | noarch |             |
| 1:3.35-2.el8           |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 83 k  |        |             |
| perl-JSON-PP           |       | noarch |             |
| 1:2.97.001-3.el8       |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 68 k  |        |             |
| perl-Math-BigInt       |       | noarch |             |
| 1:1.9998.11-7.el8      |       |        | rhel-8-for- |
| x86_64-baseos-rpms     | 196 k |        |             |
| perl-Math-Complex      |       | noarch |             |
| 1.59-421.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms     | 109 k |        |             |
| perl-Test-Harness      |       | noarch |             |
| 1:3.42-1.el8           |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 279 k |        |             |
| perl-devel             |       | x86_64 |             |
| 4:5.26.3-419.el8_4.1   |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 599 k |        |             |
| perl-srpm-macros       |       | noarch |             |
| 1-25.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 11 k  |        |             |
| perl-version           |       | x86_64 |             |
| 6:0.99.24-1.el8        |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 67 k  |        |             |
| platform-python-devel  |       | x86_64 |             |
| 3.6.8-41.el8           |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 249 k |        |             |
| python-rpm-macros      |       | noarch |             |
| 3-41.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 15 k  |        |             |
| python-srpm-macros     |       | noarch |             |
| 3-41.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 15 k  |        |             |
| python3-pyparsing      |       | noarch |             |
| 2.1.10-7.el8           |       |        | rhel-8-for- |
| x86_64-baseos-rpms     | 142 k |        |             |
| python3-rpm-generators |       | noarch |             |
| 5-7.el8                |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 25 k  |        |             |
| python3-rpm-macros     |       | noarch |             |
| 3-41.el8               |       |        | rhel-8-for- |
| x86_64-appstream-rpms  | 14 k  |        |             |
| qt5-srpm-macros        |       | noarch |             |

|                                      |       |        |             |
|--------------------------------------|-------|--------|-------------|
| 5.15.2-1.el8                         |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 11 k  |        |             |
| redhat-lsb-submod-security           |       | x86_64 |             |
| 4.1-47.el8                           |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 22 k  |        |             |
| redhat-rpm-config                    |       | noarch |             |
| 125-1.el8                            |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 87 k  |        |             |
| rust-srpm-macros                     |       | noarch |             |
| 5-2.el8                              |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 9.3 k |        |             |
| spax                                 |       | x86_64 |             |
| 1.5.3-13.el8                         |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 217 k |        |             |
| systemtap-sdt-devel                  |       | x86_64 |             |
| 4.6-4.el8                            |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 86 k  |        |             |
| time                                 |       | x86_64 |             |
| 1.9-3.el8                            |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 54 k  |        |             |
| unzip                                |       | x86_64 |             |
| 6.0-46.el8                           |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 196 k |        |             |
| util-linux-user                      |       | x86_64 |             |
| 2.32.1-28.el8                        |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 100 k |        |             |
| zip                                  |       | x86_64 |             |
| 3.0-23.el8                           |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 270 k |        |             |
| zlib-devel                           |       | x86_64 |             |
| 1.2.11-17.el8                        |       |        | rhel-8-for- |
| x86_64-baseos-rpms                   | 58 k  |        |             |
| Installing weak dependencies:        |       |        |             |
| perl-CPAN-Meta                       |       | noarch |             |
| 2.150010-396.el8                     |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 191 k |        |             |
| perl-CPAN-Meta-Requirements          |       | noarch |             |
| 2.140-396.el8                        |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 37 k  |        |             |
| perl-Encode-Locale                   |       | noarch |             |
| 1.05-10.module+el8.3.0+6498+9eecfe51 |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 22 k  |        |             |
| perl-Time-HiRes                      |       | x86_64 |             |
| 4:1.9758-2.el8                       |       |        | rhel-8-for- |
| x86_64-appstream-rpms                | 61 k  |        |             |

## Transaction Summary

Install 69 Packages

Upgrade 17 Packages

Total download size: 72 M

Is this ok [y/N]: y

Downloading Packages:

(1/86): perl-ExtUtils-Install-2.14-4.el8.noarch.rpm

735 kB/s | 46 kB 00:00

(2/86): libesmtplib-1.0.6-18.el8.x86\_64.rpm

1.0 MB/s | 70 kB 00:00

(3/86): esmtplib-1.2-15.el8.x86\_64.rpm

747 kB/s | 57 kB 00:00

(4/86): rust-srpm-macros-5-2.el8.noarch.rpm

308 kB/s | 9.3 kB 00:00

(5/86): perl-ExtUtils-Manifest-1.70-395.el8.noarch.rpm

781 kB/s | 37 kB 00:00

(6/86): perl-CPAN-Meta-2.150010-396.el8.noarch.rpm

2.7 MB/s | 191 kB 00:00

(7/86): ocaml-srpm-macros-5-4.el8.noarch.rpm

214 kB/s | 9.5 kB 00:00

(8/86): perl-JSON-PP-2.97.001-3.el8.noarch.rpm

1.2 MB/s | 68 kB 00:00

(9/86): perl-ExtUtils-MakeMaker-7.34-1.el8.noarch.rpm

5.8 MB/s | 301 kB 00:00

(10/86): ghc-srpm-macros-1.4.2-7.el8.noarch.rpm

317 kB/s | 9.4 kB 00:00

(11/86): perl-Test-Harness-3.42-1.el8.noarch.rpm

4.5 MB/s | 279 kB 00:00

(12/86): perl-ExtUtils-Command-7.34-1.el8.noarch.rpm

520 kB/s | 19 kB 00:00

...

15 MB/s | 1.5 MB 00:00

Total

35 MB/s | 72 MB 00:02

Running transaction check

Transaction check succeeded.

Running transaction test

```
Transaction test succeeded.
Running transaction
  Preparing      :
1/1
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/1
  Upgrading       : openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Running scriptlet: openssl-libs-1:1.1.1k-7.el8_6.x86_64
1/103
  Upgrading       : libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Running scriptlet: libgcc-8.5.0-10.1.el8_6.x86_64
2/103
  Upgrading       : elfutils-libelf-0.186-1.el8.x86_64
3/103
  Installing      : perl-version-6:0.99.24-1.el8.x86_64
4/103
  Installing      : perl-CPAN-Meta-Requirements-2.140-396.el8.noarch
5/103
  Upgrading       : libsemanage-2.9-8.el8.x86_64
6/103
  Installing      : zlib-devel-1.2.11-17.el8.x86_64
7/103
  Installing      : python-srpm-macros-3-41.el8.noarch
8/103
  Installing      : python-rpm-macros-3-41.el8.noarch
9/103
  Installing      : python3-rpm-macros-3-41.el8.noarch
10/103
  Installing      : perl-Time-HiRes-4:1.9758-2.el8.x86_64
11/103
  Installing      : perl-ExtUtils-ParseXS-1:3.35-2.el8.noarch
12/103
  Installing      : perl-Test-Harness-1:3.42-1.el8.noarch
13/103
  Upgrading       : python3-libsemanage-2.9-8.el8.x86_64
14/103
  Upgrading       : polycoreutils-2.9-19.el8.x86_64
15/103
  Running scriptlet: polycoreutils-2.9-19.el8.x86_64
15/103
  Upgrading       : python3-polycoreutils-2.9-19.el8.noarch
16/103
  Installing      : dwz-0.12-10.el8.x86_64
17/103
```

```

Installing      : ncurses-compat-libs-6.1-9.20180224.el8.x86_64
18/103
Installing      : libesmtplib-1.0.6-18.el8.x86_64
19/103
Installing      : mailx-12.5-29.el8.x86_64
20/103
Installing      : libkadm5-1.18.2-14.el8.x86_64
21/103
Upgrading       : libgomp-8.5.0-10.1.el8_6.x86_64
22/103
Running scriptlet: libgomp-8.5.0-10.1.el8_6.x86_64
22/103
Upgrading       : platform-python-pip-9.0.3-22.el8.noarch
23/103
Upgrading       : python3-pip-9.0.3-22.el8.noarch
24/103
Upgrading       : python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
Running scriptlet: python36-3.6.8-
38.module+el8.5.0+12207+5c5719bc.x86_64
25/103
Upgrading       : cpp-8.5.0-10.1.el8_6.x86_64
26/103
Running scriptlet: cpp-8.5.0-10.1.el8_6.x86_64
26/103
Upgrading       : gcc-8.5.0-10.1.el8_6.x86_64
27/103
Running scriptlet: gcc-8.5.0-10.1.el8_6.x86_64
27/103
Installing      : annobin-10.29-3.el8.x86_64
28/103
Installing      : unzip-6.0-46.el8.x86_64
29/103
Installing      : zip-3.0-23.el8.x86_64
30/103
Installing      : perl-Math-Complex-1.59-421.el8.noarch
31/103
Installing      : perl-Math-BigInt-1:1.9998.11-7.el8.noarch
32/103
Installing      : perl-JSON-PP-1:2.97.001-3.el8.noarch
33/103
Installing      : make-1:4.2.1-11.el8.x86_64
34/103
Running scriptlet: make-1:4.2.1-11.el8.x86_64
34/103

```

```

Installing      : libcom_err-devel-1.45.6-2.el8.x86_64
35/103
Installing      : util-linux-user-2.32.1-28.el8.x86_64
36/103
Installing      : libsepol-devel-2.9-3.el8.x86_64
37/103
Installing      : pcre2-utf32-10.32-2.el8.x86_64
38/103
Installing      : pcre2-utf16-10.32-2.el8.x86_64
39/103
Installing      : pcre2-devel-10.32-2.el8.x86_64
40/103
Installing      : libselinux-devel-2.9-5.el8.x86_64
41/103
Installing      : patch-2.7.6-11.el8.x86_64
42/103
Installing      : python3-pyparsing-2.1.10-7.el8.noarch
43/103
Installing      : systemtap-sdt-devel-4.6-4.el8.x86_64
44/103
Installing      : spax-1.5.3-13.el8.x86_64
45/103
Running scriptlet: spax-1.5.3-13.el8.x86_64
45/103
Installing      : m4-1.4.18-7.el8.x86_64
46/103
Running scriptlet: m4-1.4.18-7.el8.x86_64
46/103
Installing      : libverto-devel-0.3.0-5.el8.x86_64
47/103
Installing      : bc-1.07.1-5.el8.x86_64
48/103
Running scriptlet: bc-1.07.1-5.el8.x86_64
48/103
Installing      : at-3.1.20-11.el8.x86_64
49/103
Running scriptlet: at-3.1.20-11.el8.x86_64
49/103
Installing      : keyutils-libs-devel-1.5.10-6.el8.x86_64
50/103
Installing      : krb5-devel-1.18.2-14.el8.x86_64
51/103
Installing      : time-1.9-3.el8.x86_64
52/103
Running scriptlet: time-1.9-3.el8.x86_64
52/103

```



```

Upgrading      : polycoreutils-python-utils-2.9-19.el8.noarch
80/103
Installing     : elfutils-libelf-devel-0.186-1.el8.x86_64
81/103
Upgrading      : elfutils-libs-0.186-1.el8.x86_64
82/103
Upgrading      : mokutil-1:0.3.0-11.el8_6.1.x86_64
83/103
Upgrading      : openssl-1:1.1.1k-7.el8_6.x86_64
84/103
Installing     : kernel-devel-4.18.0-348.el8.x86_64
85/103
Running scriptlet: kernel-devel-4.18.0-348.el8.x86_64

...

85/103
Installing     : bzip2-1.0.6-26.el8.x86_64
86/103
Cleanup        : polycoreutils-python-utils-2.9-14.el8.noarch
87/103
Cleanup        : python3-polycoreutils-2.9-14.el8.noarch
88/103
Cleanup        : python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
Running scriptlet: python36-3.6.8-
2.module+el8.1.0+3334+5cb623d7.x86_64
89/103
Cleanup        : elfutils-libs-0.185-1.el8.x86_64
90/103
Cleanup        : openssl-1:1.1.1k-4.el8.x86_64
91/103
Cleanup        : python3-libsemanage-2.9-6.el8.x86_64
92/103
Running scriptlet: gcc-8.4.1-1.el8.x86_64
93/103
Cleanup        : gcc-8.4.1-1.el8.x86_64
93/103
Running scriptlet: polycoreutils-2.9-14.el8.x86_64
94/103
Cleanup        : polycoreutils-2.9-14.el8.x86_64
94/103
Cleanup        : mokutil-1:0.3.0-11.el8.x86_64
95/103

```

```

Cleanup      : python3-pip-9.0.3-19.el8.noarch
96/103
Cleanup      : platform-python-pip-9.0.3-19.el8.noarch
97/103
Cleanup      : openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
Running scriptlet: openssl-libs-1:1.1.1k-4.el8.x86_64
98/103
Cleanup      : libsemanage-2.9-6.el8.x86_64
99/103
Running scriptlet: cpp-8.4.1-1.el8.x86_64
100/103
Cleanup      : cpp-8.4.1-1.el8.x86_64
100/103
Cleanup      : libgcc-8.5.0-3.el8.x86_64
101/103
Running scriptlet: libgcc-8.5.0-3.el8.x86_64
101/103
Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
Cleanup      : libgomp-8.4.1-1.el8.x86_64
102/103
Running scriptlet: libgomp-8.4.1-1.el8.x86_64
102/103
Cleanup      : elfutils-libelf-0.185-1.el8.x86_64
103/103
Running scriptlet: elfutils-libelf-0.185-1.el8.x86_64
103/103
Verifying    : esmtp-1.2-15.el8.x86_64
1/103
Verifying    : libesmtp-1.0.6-18.el8.x86_64

...

Upgraded:
  cpp-8.5.0-10.1.el8_6.x86_64                                elfutils-
libelf-0.186-1.el8.x86_64      elfutils-libs-0.186-1.el8.x86_64
gcc-8.5.0-10.1.el8_6.x86_64
  libgcc-8.5.0-10.1.el8_6.x86_64                                libgomp-
8.5.0-10.1.el8_6.x86_64      libsemanage-2.9-8.el8.x86_64
mokutil-1:0.3.0-11.el8_6.1.x86_64
  openssl-1:1.1.1k-7.el8_6.x86_64                                openssl-
libs-1:1.1.1k-7.el8_6.x86_64      platform-python-pip-9.0.3-22.el8.noarch
policycoreutils-2.9-19.el8.x86_64
  policycoreutils-python-utils-2.9-19.el8.noarch                python3-
libsemanage-2.9-8.el8.x86_64      python3-pip-9.0.3-22.el8.noarch

```

```

python3-policycoreutils-2.9-19.el8.noarch
python36-3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
Installed:
annobin-10.29-3.el8.x86_64 at-
3.1.20-11.el8.x86_64 bc-1.07.1-5.el8.x86_64
bzip2-1.0.6-26.el8.x86_64
cups-client-1:2.2.6-38.el8.x86_64 dwz-0.12-
10.el8.x86_64
ed-1.14.2-4.el8.x86_64
efi-srpm-macros-3-3.el8.noarch elfutils-libelf-
devel-0.186-1.el8.x86_64
esmtplib-1.2-15.el8.x86_64
ghc-srpm-macros-1.4.2-7.el8.noarch go-srpm-macros-2-
17.el8.noarch
kernel-devel-4.18.0-348.el8.x86_64
keyutils-libs-devel-1.5.10-6.el8.x86_64 krb5-devel-1.18.2-
14.el8.x86_64
libcom_err-devel-1.45.6-2.el8.x86_64
libesmtplib-1.0.6-18.el8.x86_64 libkadm5-1.18.2-
14.el8.x86_64
libblockfile-1.14-1.el8.x86_64
libselinux-devel-2.9-5.el8.x86_64 libsepol-devel-2.9-
3.el8.x86_64
libverto-devel-0.3.0-5.el8.x86_64 m4-
1.4.18-7.el8.x86_64 mailx-12.5-
29.el8.x86_64
make-1:4.2.1-11.el8.x86_64
ncurses-compat-libs-6.1-9.20180224.el8.x86_64 ocaml-srpm-macros-
5-4.el8.noarch
openblas-srpm-macros-2-2.el8.noarch
openssl-devel-1:1.1.1k-7.el8_6.x86_64 patch-2.7.6-
11.el8.x86_64
pcre2-devel-10.32-2.el8.x86_64
pcre2-utf16-10.32-2.el8.x86_64 pcre2-utf32-10.32-
2.el8.x86_64
perl-CPAN-Meta-2.150010-396.el8.noarch
perl-CPAN-Meta-Requirements-2.140-396.el8.noarch perl-CPAN-Meta-
YAML-0.018-397.el8.noarch
perl-Encode-Locale-1.05-10.module+el8.3.0+6498+9eecfe51.noarch
perl-ExtUtils-Command-1:7.34-1.el8.noarch perl-ExtUtils-
Install-2.14-4.el8.noarch
perl-ExtUtils-MakeMaker-1:7.34-1.el8.noarch
perl-ExtUtils-Manifest-1.70-395.el8.noarch perl-ExtUtils-
ParseXS-1:3.35-2.el8.noarch
perl-JSON-PP-1:2.97.001-3.el8.noarch
perl-Math-BigInt-1:1.9998.11-7.el8.noarch perl-Math-Complex-

```

```

1.59-421.el8.noarch
perl-Test-Harness-1:3.42-1.el8.noarch
perl-Time-HiRes-4:1.9758-2.el8.x86_64 perl-devel-
4:5.26.3-419.el8_4.1.x86_64
perl-srpm-macros-1-25.el8.noarch
perl-version-6:0.99.24-1.el8.x86_64 platform-python-
devel-3.6.8-41.el8.x86_64
python-rpm-macros-3-41.el8.noarch
python-srpm-macros-3-41.el8.noarch python3-pyparsing-
2.1.10-7.el8.noarch
python3-rpm-generators-5-7.el8.noarch
python3-rpm-macros-3-41.el8.noarch python36-devel-
3.6.8-38.module+el8.5.0+12207+5c5719bc.x86_64
qt5-srpm-macros-5.15.2-1.el8.noarch
redhat-lsb-core-4.1-47.el8.x86_64 redhat-lsb-submod-
security-4.1-47.el8.x86_64
redhat-rpm-config-125-1.el8.noarch
rust-srpm-macros-5-2.el8.noarch spax-1.5.3-
13.el8.x86_64
systemtap-sdt-devel-4.6-4.el8.x86_64
time-1.9-3.el8.x86_64 unzip-6.0-
46.el8.x86_64
util-linux-user-2.32.1-28.el8.x86_64
zip-3.0-23.el8.x86_64 zlib-devel-1.2.11-
17.el8.x86_64

```

Complete!

OS package installations finished

+ Installing ONTAP Mediator. (Log: /tmp/ontap\_mediator.JixKGP/ontap-mediator-1.6.0/ontap-mediator-1.6.0/install\_20221021155929.log)

This step will take several minutes. Use the log file to view progress.

Sudoer config verified

ONTAP Mediator rsyslog and logging rotation enabled

+ Install successful. (Moving log to /opt/netapp/lib/ontap\_mediator/log/install\_20221021155929.log)

+ WARNING: This system supports UEFI

Secure Boot (SB) is currently disabled on this system.

If SB is enabled in the future, SCST will not work unless the following action is taken:

Using the keys in

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys follow instructions in

/opt/netapp/lib/ontap\_mediator/ontap\_mediator/SCST\_mod\_keys/README.module-signing

to sign the SCST kernel module. Note that reboot will be

needed.

SCST will not start automatically when Secure Boot is enabled and not configured properly.

+ Note: ONTAP Mediator uses a kernel module compiled specifically for the current

OS. Using 'yum update' to upgrade the kernel might cause service interruption.

```
For more information, see /opt/netapp/lib/ontap_mediator/README
[root@scs000099753 ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 8.5 (Ootpa)
[root@scs000099753 ~]#
```

## Verificare l'installazione

Una volta installato il mediatore ONTAP, verificare che i servizi del mediatore ONTAP siano in esecuzione.

### Fasi

1. Visualizza lo stato dei servizi di supporto ONTAP:

a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Verificare le porte utilizzate dal servizio di supporto ONTAP:

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

tcp        0      0 0.0.0.0:31784      0.0.0.0:*        LISTEN
tcp        0      0 0.0.0.0:3260      0.0.0.0:*        LISTEN
tcp6       0      0 :::3260          :::*             LISTEN
```

## Configurazione post-installazione

Una volta installato ed eseguito il servizio ONTAP Mediator, è necessario eseguire ulteriori attività di configurazione nel sistema di storage ONTAP per utilizzare le funzioni di Mediator:

- Per utilizzare il servizio ONTAP Mediator in una configurazione IP MetroCluster, vedere ["Configurazione del servizio ONTAP Mediator da una configurazione IP MetroCluster"](#).
- Per utilizzare SnapMirror Business Continuity, vedere ["Installare il servizio di supporto ONTAP e confermare la configurazione del cluster ONTAP"](#).

## Configurare i criteri di sicurezza di ONTAP Mediator

Il server ONTAP supporta diverse impostazioni di sicurezza configurabili. I valori predefiniti per tutte le impostazioni sono forniti in un file `low_space_threshold_mib: 10Read-only`:

```
/opt/netapp/lib/ontap_mediator/server_config/ontap_mediator.user_config.yaml
```

Tutti i valori inseriti in `ontap_mediator.user_config.yaml` Sovrascrive i valori predefiniti e viene mantenuto in tutti gli aggiornamenti di ONTAP Mediator.

Dopo la modifica `ontap_mediator.user_config.yaml`, Riavviare il servizio di supporto ONTAP:

```
systemctl restart ontap_mediator
```

### Modificare gli attributi del mediatore ONTAP

È possibile configurare i seguenti attributi:



Altri valori predefiniti in `ontap_mediator.config.yaml` non deve essere modificato.

- **Impostazioni utilizzate per installare certificati SSL di terze parti come sostituzioni dei certificati autofirmati predefiniti**

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
tor_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
tor_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
cert_valid_days: '1095' # Used to set the expiration
on client certs to 3 years
x509_passin_pwd: 'pass:ontap' # passphrase for the signed
client cert
```

- **Impostazioni che forniscono protezione contro gli attacchi di indovinare le password a forza bruta**

Per attivare la funzione, impostare un valore per `window_seconds` e `a.retry_limit`

Esempi:

- Fornire una finestra di 5 minuti per le ipotesi, quindi ripristinare il conteggio a zero errori:

```
authentication_lock_window_seconds: 300
```

- Bloccare l'account se si verificano cinque guasti entro il periodo di tempo previsto:

```
authentication_retry_limit: 5
```

- Riduci l'impatto degli attacchi di indovinare le password con la forza bruta impostando un ritardo che si verifica prima di rifiutare ogni tentativo, rallentando gli attacchi.

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0    # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null   # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null           # number of retries to
allow before locking API access, null = unlimited
```

- **Campi che controllano le regole di complessità delle password dell'account utente API del mediatore ONTAP**

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters
password_lowercase_chars: 1    # min. lowercase character
password_special_chars: 1      # min. non-letter, non-digit
password_nonletter_chars: 2     # min. non-letter characters (digits,
specials, anything)
```

- **Impostazione che controlla lo spazio libero richiesto su `/opt/netapp/lib/ontap_mediator` disco.**

Se lo spazio è inferiore alla soglia impostata, il servizio emetterà un avviso.

```
low_space_threshold_mib: 10
```

- **Impostazione che controlla `RESERVE_LOG_SPACE`.**

L'installazione predefinita del server ONTAP Mediator crea uno spazio su disco separato per i log. Il programma di installazione crea un nuovo file a dimensione fissa con un totale di 700 MB di spazio su disco da utilizzare esplicitamente per la registrazione di Mediator.

Per disattivare questa funzione e utilizzare lo spazio su disco predefinito, procedere come segue:

- a. Modificare il valore di `RESERVE_LOG_SPACE` da `"1"` a `"0"` nel seguente file:

```
/opt/netapp/lib/ontap_mediator/tools/mediator_env
```

- b. Riavviare Mediator:



- i. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

```
RESERVE_LOG_SPACE=0
```

- ii. `systemctl restart ontap_mediator`

Per riattivare la funzione, modificare il valore da "0" a "1" e riavviare il Mediator.



L'alternanza tra gli spazi su disco non elimina i registri esistenti. Viene eseguito il backup di tutti i registri precedenti, quindi viene spostato nello spazio su disco corrente dopo l'attivazione e il riavvio di Mediator.

## Gestire il servizio ONTAP mediator

Dopo aver installato il servizio ONTAP Mediator, è possibile modificare il nome utente o la password. È inoltre possibile disinstallare il servizio di supporto ONTAP.

### Modificare il nome utente

#### A proposito di queste attività

Questa operazione viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.

Se non si riesce a raggiungere questo comando, potrebbe essere necessario eseguire il comando utilizzando il percorso completo, come illustrato nell'esempio seguente:

```
/usr/local/bin/mediator_username
```

### Procedura

Modificare il nome utente scegliendo una delle seguenti opzioni:

- Eseguire il comando `mediator_change_user` e rispondere alle richieste come mostrato nell'esempio seguente:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
  Mediator API User Name: mediatoradmin
                        Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- Eseguire il seguente comando:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME= mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME= mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

## Modificare la password

### A proposito di questa attività

Questa attività viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.

Se non si riesce a raggiungere questo comando, potrebbe essere necessario eseguire il comando utilizzando il percorso completo, come illustrato nell'esempio seguente:

```
/usr/local/bin/mediator_change_password
```

### Procedura

Modificare la password scegliendo una delle seguenti opzioni:

- Eseguire `mediator_change_password` e rispondere ai prompt come mostrato nell'esempio seguente:

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
  Mediator API User Name: mediatoradmin
    Old Password:
    New Password:
    Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- Eseguire il seguente comando:

```
MEDIATOR_USERNAME= mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

L'esempio mostra che la password viene modificata da "mediator1" a "mediator2".

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
The password has been updated successfully.
[root@mediator-host ~]#
```

## Arrestare il servizio di supporto ONTAP

Per interrompere il servizio ONTAP Mediator, attenersi alla seguente procedura:

### Fasi

1. Arrestare il mediatore ONTAP.

```
systemctl stop ontap_mediator
```

2. Arrestare SCST.

```
systemctl stop mediator-scst
```

3. Disattivare il mediatore ONTAP e l'SCST.

```
systemctl disable ontap_mediator mediator-scst
```

## Riattivare il servizio di supporto ONTAP

Per riattivare il servizio ONTAP Mediator, attenersi alla seguente procedura:

### Fasi

1. Abilitare il mediatore ONTAP e l'SCST.

```
systemctl enable ontap_mediator mediator-scst
```

2. Avviare SCST.

```
systemctl start mediator-scst
```

3. Avviare il mediatore ONTAP.

```
systemctl start ontap_mediator
```

## Verificare che il mediatore ONTAP sia in buone condizioni

Una volta installato il mediatore ONTAP, verificare che i servizi del mediatore ONTAP siano in esecuzione.

### Fasi

1. Visualizza lo stato dei servizi di supporto ONTAP:

- a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
└─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
└─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst

Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
Main PID: 286662 (iscsi-scstd)
Tasks: 1 (limit: 49473)
Memory: 1.2M
CGroup: /system.slice/mediator-scst.service
└─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Verificare le porte utilizzate dal servizio di supporto ONTAP:

`netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'
```

```
tcp    0    0 0.0.0.0:31784    0.0.0.0:*        LISTEN
```

```
tcp    0    0 0.0.0.0:3260    0.0.0.0:*        LISTEN
```

```
tcp6   0    0 :::3260         :::*             LISTEN
```

## Disinstallare manualmente SCST per eseguire la manutenzione dell'host

Per disinstallare SCST, è necessario il pacchetto tar SCST utilizzato per la versione installata di ONTAP Mediator.

### Fasi

1. Scaricare il pacchetto SCST appropriato (come mostrato nella tabella seguente) e scaricarlo.

| Per questa versione ... | USA questo bundle tar... |
|-------------------------|--------------------------|
| ONTAP mediatore 1,7     | scst-3.7.0.tar.bz2       |
| Mediatore ONTAP 1.6     | scst-3.7.0.tar.bz2       |
| Mediatore ONTAP 1.5     | scst-3.6.0.tar.bz2       |
| Mediatore ONTAP 1.4     | scst-3.6.0.tar.bz2       |
| Mediatore ONTAP 1.3     | scst-3.5.0.tar.bz2       |
| Mediatore ONTAP 1.1     | scst-3.4.0.tar.bz2       |
| Mediatore ONTAP 1.0     | scst-3.3.0.tar.bz2       |

2. Eseguire i seguenti comandi nella directory "scst":

- a. `systemctl stop mediator-scst`
- b. `make scstadm_uninstall`
- c. `make iscsi_uninstall`
- d. `make usr_uninstall`
- e. `make scst_uninstall`
- f. `depmod`

## Installare manualmente SCST per eseguire la manutenzione dell'host

Per installare manualmente SCST, è necessario disporre del pacchetto tar SCST utilizzato per la versione installata di ONTAP Mediator (vedere la [tabella precedente](#)).

1. Eseguire i seguenti comandi nella directory "scst":

- a. `make 2release`
- b. `make scst_install`
- c. `make usr_install`
- d. `make iscsi_install`
- e. `make scstadm_install`
- f. `depmod`
- g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
- h. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/.`
- i. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

2. (Facoltativo) se l'opzione Secure Boot (Avvio protetto) è attivata, prima di riavviare il sistema, attenersi alla seguente procedura:

- a. Determinare ciascun nome di file per i moduli "scst\_vdisk", "scst" e "iscsi\_scst".

```
[root@localhost ~]# modinfo -n scst_vdisk
[root@localhost ~]# modinfo -n scst
[root@localhost ~]# modinfo -n iscsi_scst
```

- b. Determinare la release del kernel.

```
[root@localhost ~]# uname -r
```

- c. Firmare ogni file con il kernel.

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

- d. Installare la chiave corretta con il firmware UEFI.

Le istruzioni per l'installazione della chiave UEFI sono disponibili all'indirizzo:

`/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-  
signing`

La chiave UEFI generata si trova in:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.der
```

### 3. Eseguire un riavvio.

```
reboot
```

## Disinstallare il servizio di supporto ONTAP

### Prima di iniziare

Se necessario, è possibile rimuovere il servizio di supporto ONTAP. Il mediatore deve essere disconnesso da ONTAP prima di rimuovere il servizio.

### A proposito di questa attività

Questa attività viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.

Se non si riesce a raggiungere questo comando, potrebbe essere necessario eseguire il comando utilizzando il percorso completo, come illustrato nell'esempio seguente:

```
/usr/local/bin/uninstall_ontap_mediator
```

### Fase

#### 1. Disinstallare il servizio di supporto ONTAP:

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator

ONTAP Mediator: Self Extracting Uninstaller

+ Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
+ Remove successful.
[root@mediator-host ~]#
```

## Rigenerare un certificato autofirmato temporaneo

### A proposito di questa attività

- Questa attività viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.
- È possibile eseguire questa attività solo se i certificati autofirmati generati sono diventati obsoleti a causa di modifiche al nome host o all'indirizzo IP dell'host dopo l'installazione di ONTAP Mediator.
- Dopo che il certificato autofirmato temporaneo è stato sostituito da un certificato di terze parti attendibile, *non* utilizzare questa attività per rigenerare un certificato. L'assenza di un certificato autofirmato causerà l'errore di questa procedura.

### Fase

Per rigenerare un nuovo certificato autofirmato temporaneo per l'host corrente, attenersi alla seguente procedura:

#### 1. Riavviare ONTAP Mediator:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

## Gestire l'host del sistema operativo per ONTAP Mediator

Per ottenere performance ottimali, è necessario mantenere regolarmente il sistema operativo host per ONTAP Mediator.

### Riavviare l'host

Riavviare l'host quando i cluster sono integri. Mentre il mediatore ONTAP è offline, i cluster rischiano di non essere in grado di reagire correttamente ai guasti. Se è necessario riavviare il sistema, si consiglia di utilizzare una finestra di servizio.

Il mediatore ONTAP riprende automaticamente durante il riavvio e reinserisce le relazioni precedentemente configurate con i cluster ONTAP.



## Aggiornamenti dei pacchetti host

Qualsiasi libreria o pacchetto yum (ad eccezione del kernel) può essere aggiornato in modo sicuro, ma potrebbe richiedere un riavvio per avere effetto. Se è necessario riavviare il sistema, si consiglia di utilizzare una finestra di servizio.

Se si installa `yum-utils` utilizzare il `needs-restarting` comando per rilevare se qualsiasi modifica del pacchetto richiede un riavvio.

È necessario riavviare il sistema se una delle dipendenze del mediatore ONTAP viene aggiornata perché non avrà effetto immediato sui processi in esecuzione.

## Aggiornamenti minori del kernel per il sistema operativo host

SCST deve essere compilato per il kernel in uso. Per aggiornare il sistema operativo, è necessaria una finestra di manutenzione.

### Fasi

Per aggiornare il kernel del sistema operativo host, procedere come segue.

1. Arrestare il mediatore ONTAP
2. Disinstallare il pacchetto SCST. (SCST non fornisce un meccanismo di aggiornamento).
3. Aggiornare il sistema operativo e riavviare.
4. Reinstallare il pacchetto SCST.
5. Riattivare i servizi del mediatore ONTAP.

## L'host modifica il nome host o l'IP

### A proposito di questa attività

- Questa attività viene eseguita sull'host Linux su cui è installato il servizio ONTAP Mediator.
- È possibile eseguire questa attività solo se i certificati autofirmati generati sono diventati obsoleti a causa di modifiche al nome host o all'indirizzo IP dell'host dopo l'installazione di ONTAP Mediator.
- Dopo che il certificato autofirmato temporaneo è stato sostituito da un certificato di terze parti attendibile, *non* utilizzare questa attività per rigenerare un certificato. L'assenza di un certificato autofirmato causerà l'errore di questa procedura.

### Fase

Per rigenerare un nuovo certificato autofirmato temporaneo per l'host corrente, attenersi alla seguente procedura:

1. Riavviare ONTAP Mediator:

```
./make_self_signed_certs.sh overwrite
```

```

[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....
.....
.....++++
.....++++
e is 65537 (0x010001)
Generating a RSA private key
.....++++
.....
.....+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator

```

## Gestire i siti MetroCluster con Gestione di sistema

### Panoramica sulla gestione del sito MetroCluster con Gestione di sistema

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema come interfaccia semplificata per gestire una configurazione di un'installazione di MetroCluster.

Una configurazione MetroCluster consente a due cluster di eseguire il mirroring dei dati l'uno rispetto all'altro, in modo che, se un cluster non funziona, i dati non vadano persi.

In genere, un'organizzazione imposta i cluster in due ubicazioni geografiche separate. Un amministratore di ogni ubicazione imposta un cluster e lo configura. Quindi, uno degli amministratori può impostare il peering tra i cluster in modo che possano condividere i dati.

L'organizzazione può anche installare un mediatore ONTAP in una terza sede. Il servizio ONTAP Mediator monitora lo stato di ciascun cluster. Quando uno dei cluster rileva che non è in grado di comunicare con il cluster partner, interroga il monitor per determinare se l'errore è un problema con il sistema del cluster o con la

connessione di rete.

Se il problema riguarda la connessione di rete, l'amministratore di sistema esegue i metodi di risoluzione dei problemi per correggere l'errore e riconnettersi. Se il cluster partner non è attivo, l'altro cluster avvia un processo di switchover per controllare l'i/o dei dati per entrambi i cluster.

È inoltre possibile eseguire uno switchover per spegnere uno dei sistemi cluster per la manutenzione pianificata. Il cluster partner gestisce tutte le operazioni di i/o dei dati per entrambi i cluster fino a quando non viene attivato il cluster su cui è stata eseguita la manutenzione ed è stata eseguita un'operazione di switchback.

È possibile gestire le seguenti operazioni:

- ["Configurare un sito IP MetroCluster"](#)
- ["Impostare il peering di IP MetroCluster"](#)
- ["Configurare un sito IP MetroCluster"](#)
- ["Eseguire lo switchover e lo switchback di IP MetroCluster"](#)
- ["Risoluzione dei problemi relativi alle configurazioni di IP MetroCluster"](#)
- ["Upgrade di ONTAP su cluster MetroCluster"](#)

## Configurare un sito IP MetroCluster

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema per impostare una configurazione IP di un sito MetroCluster.

Un sito MetroCluster è costituito da due cluster. In genere, i cluster si trovano in posizioni geografiche diverse.

### Prima di iniziare

- Il sistema deve essere già installato e cablato come indicato nella ["Istruzioni per l'installazione e la configurazione"](#) fornito con il sistema.
- Le interfacce di rete del cluster devono essere configurate su ciascun nodo di ciascun cluster per la comunicazione all'interno del cluster.

### Assegnare un indirizzo IP di gestione dei nodi

#### Sistema Windows

Collegare il computer Windows alla stessa subnet dei controller. In questo modo, viene assegnato automaticamente un indirizzo IP di gestione dei nodi al sistema.

#### Fasi

1. Dal sistema Windows, aprire l'unità **Network** per rilevare i nodi.
2. Fare doppio clic sul nodo per avviare l'installazione guidata del cluster.

#### Altri sistemi

È necessario configurare l'indirizzo IP di gestione dei nodi per uno dei nodi nel cluster. È possibile utilizzare questo indirizzo IP di gestione dei nodi per avviare la configurazione guidata del cluster.

Vedere ["Creazione del cluster sul primo nodo"](#) Per informazioni sull'assegnazione di un indirizzo IP di gestione dei nodi.

## Inizializzare e configurare il cluster

Per inizializzare il cluster, impostare una password amministrativa per il cluster e le reti di gestione dei nodi e del cluster. È inoltre possibile configurare servizi come un server DNS per risolvere i nomi host e un server NTP per sincronizzare l'ora.

### Fasi

1. In un browser Web, immettere l'indirizzo IP di gestione dei nodi configurato: "<https://node-management-IP>"

System Manager rileva automaticamente i nodi rimanenti nel cluster.

2. Nella finestra **Initialize Storage System** (Inizializza sistema di storage), eseguire le seguenti operazioni:
  - a. Inserire i dati di configurazione della rete di gestione del cluster.
  - b. Inserire gli indirizzi IP di gestione dei nodi per tutti i nodi.
  - c. Fornire i dettagli del DNS (Domain Name Server).
  - d. Nella sezione **Altro**, selezionare la casella di controllo **Usa servizio ora (NTP)** per aggiungere i server di riferimento orario.

Quando si fa clic su **Submit** (Invia), attendere la creazione e la configurazione del cluster. Quindi, viene eseguito un processo di convalida.

### Quali sono le prossime novità?

Una volta configurati, inizializzati e configurati entrambi i cluster, eseguire la seguente procedura:

- "[Impostare il peering di IP MetroCluster](#)"

## Configurare ONTAP su un nuovo video del cluster



## Impostare il peering di IP MetroCluster

A partire da ONTAP 9.8, è possibile gestire una configurazione IP di un'operazione MetroCluster con Gestore di sistema. Dopo aver configurato due cluster, è possibile impostare il peering tra di essi.

### Prima di iniziare

Per configurare due cluster, è necessario completare la seguente procedura:

- ["Configurare un sito IP MetroCluster"](#)

Alcune fasi di questo processo vengono eseguite da diversi amministratori di sistema situati nei siti geografici di ciascun cluster. Ai fini della spiegazione di questo processo, i cluster sono denominati "cluster del sito A" e "cluster del sito B".

### Esecuzione del processo di peering dal sito A.

Questo processo viene eseguito da un amministratore di sistema presso il sito A.

#### Fasi

1. Accedere al sito Di Un cluster.
2. In System Manager, selezionare **Dashboard** dalla colonna di navigazione a sinistra per visualizzare la panoramica del cluster.  
  
La dashboard mostra i dettagli del cluster (sito A). Nella sezione **MetroCluster**, a sinistra viene visualizzato un cluster.
3. Fare clic su **Attach Partner Cluster**.
4. Inserire i dettagli delle interfacce di rete che consentono ai nodi del cluster del sito A di comunicare con i nodi del cluster del sito B.
5. Fare clic su **Salva e continua**.
6. Nella finestra **Attach Partner Cluster**, selezionare **i do not have a passphrase**, che consente di generare una passphrase.
7. Copiare la passphrase generata e condividerla con l'amministratore di sistema nel sito B.
8. Selezionare **Chiudi**.

### Esecuzione del processo di peering dal sito B.

Questo processo viene eseguito da un amministratore di sistema presso il sito B.

#### Fasi

1. Accedere al cluster del sito B.
2. In System Manager, selezionare **Dashboard** per visualizzare la panoramica del cluster.  
  
La dashboard mostra i dettagli del cluster (sito B). Nella sezione MetroCluster, il cluster del sito B viene visualizzato a sinistra.
3. Fare clic su **Attach Partner Cluster** per avviare il processo di peering.
4. Inserire i dettagli delle interfacce di rete che consentono ai nodi del cluster del sito B di comunicare con i nodi del cluster del sito A.

5. Fare clic su **Salva e continua**.
6. Nella finestra **Attach Partner Cluster**, selezionare **ho una passphrase**, che consente di immettere la passphrase ricevuta dall'amministratore di sistema presso il sito A.
7. Selezionare **Peer** per completare il processo di peering.

#### Quali sono le prossime novità?

Una volta completato correttamente il processo di peering, i cluster vengono configurati. Vedere ["Configurare un sito IP MetroCluster"](#).

## Configurare un sito IP MetroCluster

A partire da ONTAP 9.8, è possibile gestire una configurazione IP di un'operazione MetroCluster con Gestore di sistema. Dopo aver configurato due cluster e aver eseguito il peering, è possibile configurare ciascun cluster.

#### Prima di iniziare

Le seguenti procedure dovrebbero essere state completate:

- ["Configurare un sito IP MetroCluster"](#)
- ["Impostare il peering di IP MetroCluster"](#)

## Configurare la connessione tra cluster

#### Fasi

1. Accedere a System Manager da uno dei siti e selezionare **Dashboard**.

Nella sezione **MetroCluster**, la figura mostra i due cluster configurati e peered per i siti MetroCluster. Il cluster da cui si sta lavorando (cluster locale) viene visualizzato a sinistra.

2. Fare clic su **Configura MetroCluster**. Da questa finestra è possibile eseguire le seguenti operazioni:
  - a. Vengono visualizzati i nodi per ciascun cluster nella configurazione MetroCluster. Utilizzare gli elenchi a discesa per selezionare i nodi del cluster locale che saranno partner di disaster recovery con i nodi del cluster remoto.
  - b. Fare clic sulla casella di controllo se si desidera configurare un servizio ONTAP Mediator. Vedere [Configurare il servizio ONTAP Mediator](#).
  - c. Se entrambi i cluster dispongono di una licenza per attivare la crittografia, viene visualizzata la sezione **Encryption**.

Per attivare la crittografia, immettere una passphrase.

- d. Fare clic sulla casella di controllo se si desidera configurare MetroCluster con una rete condivisa Layer 3.



I nodi partner ha e gli switch di rete che si connettono ai nodi devono avere una configurazione corrispondente.

3. Fare clic su **Salva** per configurare i siti MetroCluster.

Nella sezione **MetroCluster** della dashboard, il grafico mostra un segno di spunta sul collegamento tra i due cluster, a indicare che la connessione è in buone condizioni.


## Configurare il servizio ONTAP Mediator

Il servizio di supporto ONTAP viene in genere installato in una posizione geografica separata da entrambe le posizioni dei cluster. I cluster comunicano regolarmente con il servizio per indicare che sono attivi e in esecuzione. Se uno dei cluster nella configurazione MetroCluster rileva che la comunicazione con il cluster partner non è attiva, verifica con il mediatore ONTAP se il cluster partner stesso non è attivo.

### Prima di iniziare

Entrambi i cluster dei siti MetroCluster devono essere in fase di peering.

### Fasi

1. In Gestione sistema in ONTAP 9.8, selezionare **Cluster > Impostazioni**.
2. Nella sezione **Mediator**, fare clic su .
3. Nella finestra **Configure Mediator** (Configura Mediator), fare clic su **Add+** (Aggiungi+).
4. Inserire i dettagli di configurazione per il mediatore ONTAP.

È possibile immettere i seguenti dettagli durante la configurazione di un ONTAP Mediator con Gestione di sistema.

- L'indirizzo IP del mediatore.
- Il nome utente.
- La password.

## Gestire il Mediator con System Manager

Tramite System Manager, è possibile eseguire attività di gestione del Mediator.




### A proposito di queste attività

A partire da ONTAP 9.8, è possibile utilizzare Gestione sistema come interfaccia semplificata per gestire una configurazione IP a quattro nodi di una configurazione MetroCluster, che può includere un ONTAP Mediator installato in una terza posizione.

A partire da ONTAP 9.14.1, è possibile utilizzare System Manager per eseguire queste operazioni anche per una configurazione IP a otto nodi di un sito MetroCluster. Anche se con System Manager non è possibile configurare o espandere un sistema a otto nodi, se è già stato configurato un sistema IP MetroCluster a otto nodi, è possibile eseguire queste operazioni.

Eseguire le seguenti attività per gestire il Mediator.

| Per eseguire questa attività...  | Intraprendere queste azioni...                                                                  |
|----------------------------------|-------------------------------------------------------------------------------------------------|
| Configurare il servizio Mediator | Eseguire le operazioni descritte in " <a href="#">Configurare il servizio ONTAP Mediator</a> ". |

|                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Attivazione o disattivazione del MAUSO (Mediator-Assisted Automatic Switchover) | <ol style="list-style-type: none"> <li>1. In System Manager, fare clic su <b>Dashboard</b>.</li> <li>2. Scorrere fino alla sezione MetroCluster.</li> <li>3. Fare clic su  Accanto al nome del sito MetroCluster.</li> <li>4. Selezionare <b>Abilita</b> o <b>Disabilita</b>.</li> <li>5. Immettere il nome utente e la password dell'amministratore, quindi fare clic su <b>Abilita</b> o <b>Disabilita</b>.</li> </ol> <div>  <p>È possibile attivare o disattivare il Mediator quando è possibile raggiungerlo ed entrambi i siti sono in modalità "normale". Il mediatore è ancora raggiungibile quando MAUSO è attivato o disattivato se il sistema MetroCluster è in buone condizioni.</p> </div> |
| Rimuovere il mediatore dalla configurazione MetroCluster                        | <ol style="list-style-type: none"> <li>1. In System Manager, fare clic su <b>Dashboard</b>.</li> <li>2. Scorrere fino alla sezione MetroCluster.</li> <li>3. Fare clic su  Accanto al nome del sito MetroCluster.</li> <li>4. Selezionare <b>Rimuovi mediatore</b>.</li> <li>5. Immettere il nome utente e la password dell'amministratore, quindi fare clic su <b>Rimuovi</b>.</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                               |
| Controllare lo stato del mediatore                                              | Eseguire le operazioni descritte in <a href="#">"Risoluzione dei problemi relativi alle configurazioni di IP MetroCluster"</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Eseguire uno switchover e uno switchback                                        | Eseguire le operazioni descritte in <a href="#">"Eseguire lo switchover e lo switchback di IP MetroCluster"</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Eseguire lo switchover e lo switchback di IP MetroCluster

È possibile passare al controllo da un sito IP MetroCluster all'altro per eseguire la manutenzione o il ripristino da un problema.



Le procedure di switchover e switchback sono supportate solo per le configurazioni IP MetroCluster.

### Panoramica dello switchover e dello switchback

Lo switchover può avvenire in due casi:

- **Uno switchover pianificato**

Questo switchover viene avviato da un amministratore di sistema che utilizza System Manager. Lo switchover pianificato consente a un amministratore di sistema di un cluster locale di passare al controllo in modo che i servizi dati del cluster remoto vengano gestiti dal cluster locale. Quindi, un amministratore di sistema nella posizione remota del cluster può eseguire la manutenzione sul cluster remoto.

- **Uno switchover non pianificato**



In alcuni casi, quando un cluster MetroCluster non funziona o le connessioni tra i cluster non sono attive, ONTAP avvia automaticamente una procedura di switchover in modo che il cluster ancora in esecuzione gestisca le responsabilità di gestione dei dati del cluster inattivo.

In altri casi, quando ONTAP non è in grado di determinare lo stato di uno dei cluster, l'amministratore di sistema del sito che sta lavorando avvia la procedura di switchover per assumere il controllo delle responsabilità di gestione dei dati dell'altro sito.

Per qualsiasi tipo di procedura di switchover, la funzionalità di servizio dei dati viene restituita al cluster utilizzando un processo *switchback*.

Vengono eseguiti diversi processi di switchover e switchback per ONTAP 9.7 e 9.8:

- [Utilizzare Gestione sistema in ONTAP 9.7 per lo switchover e lo switchback](#)
- [Utilizzare Gestione sistema in ONTAP 9.8 per lo switchover e lo switchback](#)

## Utilizzare Gestione sistema in ONTAP 9.7 per lo switchover e lo switchback

### Fasi

1. Accedere a Gestore di sistema in ONTAP 9.7.
2. Fare clic su **(Torna alla versione classica)**.
3. Fare clic su **Configurazione > MetroCluster**.


System Manager verifica se è possibile uno switchover negoziato.

4. Una volta completato il processo di convalida, eseguire una delle seguenti operazioni secondarie:
  - a. Se la convalida non riesce, ma il sito B è attivo, si è verificato un errore. Ad esempio, potrebbe essersi verificato un problema con un sottosistema oppure il mirroring della NVRAM potrebbe non essere sincronizzato.
    - i. Risolvere il problema che causa l'errore, fare clic su **Chiudi**, quindi ricominciare dalla fase 2.
    - ii. Arrestare i nodi del sito B, fare clic su **Close** (Chiudi), quindi eseguire le operazioni descritte in ["Esecuzione di uno switchover non pianificato"](#).
  - b. Se la convalida non riesce e il sito B è inattivo, molto probabilmente si è verificato un problema di connessione. Verificare che il sito B sia effettivamente inattivo, quindi eseguire le operazioni descritte in ["Esecuzione di uno switchover non pianificato"](#).
5. Fare clic su **Switchover from Site B to Site A** (passa da sito B a sito A) per avviare il processo di switchover.
6. Fare clic su **passa alla nuova esperienza**.

## Utilizzare Gestione sistema in ONTAP 9.8 per lo switchover e lo switchback

### Eseguire uno switchover pianificato (ONTAP 9.8)

### Fasi

1. Accedere a Gestore di sistema in ONTAP 9.8.
2. Selezionare **Dashboard**. Nella sezione **MetroCluster**, i due cluster vengono visualizzati con una connessione.
3. Nel cluster locale (mostrato a sinistra), fare clic su  E selezionare **Switchover remote data Services to the local site**.

Una volta convalidata la richiesta di switchover, il controllo viene trasferito dal sito remoto al sito locale, che esegue le richieste di servizio dati per entrambi i cluster.

Il cluster remoto viene riavviato, ma i componenti dello storage non sono attivi e il cluster non risponde alle richieste di dati. È ora disponibile per la manutenzione pianificata.



Il cluster remoto non deve essere utilizzato per la manutenzione dei dati fino a quando non viene eseguito uno switchback.

### Eseguire uno switchover non pianificato (ONTAP 9.8)

ONTAP potrebbe avviare automaticamente uno switchover non pianificato. Se ONTAP non è in grado di determinare se è necessario uno switchback, l'amministratore di sistema del sito MetroCluster ancora in esecuzione avvia lo switchover seguendo questa procedura:

#### Fasi

1. Accedere a Gestore di sistema in ONTAP 9.8.
2. Selezionare **Dashboard**.

Nella sezione **MetroCluster**, la connessione tra i due cluster viene visualizzata con una "X", il che significa che non è possibile rilevare una connessione. Le connessioni o il cluster non sono attivi.

3. Nel cluster locale (mostrato a sinistra), fare clic su  E selezionare **Switchover remote data Services to the local site**.

Se lo switchover non riesce e viene visualizzato un errore, fare clic sul collegamento "View details" (Visualizza dettagli) nel messaggio di errore e confermare lo switchover non pianificato.

Una volta convalidata la richiesta di switchover, il controllo viene trasferito dal sito remoto al sito locale, che esegue le richieste di servizio dati per entrambi i cluster.

Il cluster deve essere riparato prima di essere nuovamente messo in linea.



Una volta che il cluster remoto viene nuovamente messo in linea, non deve essere utilizzato per la manutenzione dei dati fino a quando non viene eseguito uno switchback.

### Eseguire uno switchback (ONTAP 9.8)

#### Prima di iniziare

Che il cluster remoto sia stato inattivo a causa di manutenzione pianificata o a causa di un disastro, ora dovrebbe essere attivo e in attesa dello switchback.

#### Fasi

1. Nel cluster locale, accedere a Gestione sistema in ONTAP 9.8.
2. Selezionare **Dashboard**.

Nella sezione **MetroCluster**, vengono visualizzati i due cluster.

3. Nel cluster locale (mostrato a sinistra), fare clic su  E selezionare **Take back control**.

I dati vengono prima *gariti*, per garantire la sincronizzazione e il mirroring dei dati tra entrambi i cluster.

4. Una volta completata la riparazione dei dati, fare clic su  E selezionare **inizia switchback**.

Una volta completato lo switchback, entrambi i cluster sono attivi e servono le richieste di dati. Inoltre, i dati vengono sottoposti a mirroring e sincronizzati tra i cluster.

## Modificare l'indirizzo, la netmask e il gateway in un IP MetroCluster

A partire da ONTAP 9.10.1, è possibile modificare le seguenti proprietà di un'interfaccia IP MetroCluster: Indirizzo IP, maschera e gateway. È possibile utilizzare qualsiasi combinazione di parametri per l'aggiornamento.

Potrebbe essere necessario aggiornare queste proprietà, ad esempio, se viene rilevato un indirizzo IP duplicato o se un gateway deve essere modificato in caso di rete di livello 3 a causa di modifiche alla configurazione del router. È possibile modificare solo un'interfaccia alla volta. L'interfaccia verrà rallentata fino a quando le altre interfacce non saranno aggiornate e le connessioni non verranno ristabilite.



È necessario apportare le modifiche a ciascuna porta. Analogamente, anche gli switch di rete devono aggiornare la configurazione. Ad esempio, se il gateway viene aggiornato, idealmente viene modificato su entrambi i nodi di una coppia ha, poiché sono identici. Inoltre, anche lo switch connesso a tali nodi deve aggiornare il gateway.

### Fase

Aggiornare l'indirizzo IP, la netmask e il gateway per ogni nodo e interfaccia.

## Risoluzione dei problemi relativi alle configurazioni di IP MetroCluster

A partire da ONTAP 9.8, Gestione sistema monitora lo stato delle configurazioni di IP MetroCluster e aiuta a identificare e correggere i problemi che potrebbero verificarsi.

### Panoramica della verifica dello stato di salute di MetroCluster

System Manager verifica periodicamente lo stato della configurazione di IP MetroCluster. Quando si visualizza la sezione MetroCluster nella dashboard, di solito viene visualizzato il messaggio "i sistemi MetroCluster sono integri".

Tuttavia, quando si verifica un problema, il messaggio mostra il numero di eventi. È possibile fare clic sul messaggio e visualizzare i risultati del controllo dello stato di salute dei seguenti componenti:

- Nodo
- Interfaccia di rete
- Tier (storage)
- Cluster
- Connessione
- Volume
- Replica della configurazione

La colonna **Status** (Stato) identifica i componenti che presentano problemi e la colonna **Details** (Dettagli) suggerisce come risolvere il problema.

## Risoluzione dei problemi di MetroCluster

### Fasi

1. In System Manager, selezionare **Dashboard**.
2. Nella sezione **MetroCluster**, osservare il messaggio.
  - a. Se il messaggio indica che la configurazione di MetroCluster è in buone condizioni e che le connessioni tra i cluster e il mediatore ONTAP sono in buone condizioni (visualizzate con segni di spunta), non si verificano problemi per la correzione.
  - b. Se il messaggio elenca il numero di eventi o le connessioni sono scollegate (indicate con una "X"), passare alla fase successiva.
3. Fare clic sul messaggio che mostra il numero di eventi.

Viene visualizzato il report sullo stato di salute di MetroCluster.

4. Risolvere i problemi visualizzati nel report utilizzando i suggerimenti nella colonna **Dettagli**.
5. Una volta risolti tutti i problemi, fare clic su **Controlla lo stato di salute di MetroCluster**.



La verifica dello stato di salute di MetroCluster utilizza una quantità elevata di risorse, pertanto si consiglia di eseguire tutte le attività di risoluzione dei problemi prima di eseguire il controllo.

Il controllo dello stato di salute di MetroCluster viene eseguito in background. È possibile lavorare su altre attività mentre si attende il completamento.

## Protezione dei dati mediante backup su nastro

### Panoramica del backup su nastro dei volumi FlexVol

ONTAP supporta il backup e il ripristino su nastro attraverso il protocollo di gestione dei dati di rete (NDMP). NDMP consente di eseguire il backup dei dati nei sistemi storage direttamente su nastro, con un utilizzo efficiente della larghezza di banda della rete. ONTAP supporta motori di dump e SMTape per il backup su nastro.

È possibile eseguire un dump o un backup o ripristino SMTape utilizzando applicazioni di backup conformi a NDMP. È supportata solo la versione 4 di NDMP.

#### Backup su nastro con dump

Dump è un backup basato su copia Snapshot in cui viene eseguito il backup dei dati del file system su nastro. Il motore di dump ONTAP esegue il backup su nastro di file, directory e le informazioni dell'elenco di controllo di accesso (ACL) applicabili. È possibile eseguire il backup di un intero volume, di un intero qtree o di un sottoalbero che non sia un intero volume o un intero qtree. Dump supporta backup baseline, differenziali e incrementali.

#### Backup su nastro con SMTape

SMTape è una soluzione di disaster recovery basata su copia Snapshot di ONTAP che esegue il backup di blocchi di dati su nastro. È possibile utilizzare SMTape per eseguire backup dei volumi su nastri. Tuttavia, non è possibile eseguire un backup a livello di qtree o sottostruttura. SMTape supporta backup baseline,

differenziali e incrementali.

A partire da ONTAP 9.13.1, il backup su nastro con SMTape supporta [Continuità aziendale di SnapMirror](#).

## Workflow di backup e ripristino su nastro

È possibile eseguire operazioni di backup e ripristino su nastro utilizzando un'applicazione di backup abilitata per NDMP.

### A proposito di questa attività

Il flusso di lavoro di backup e ripristino su nastro offre una panoramica delle attività coinvolte nell'esecuzione delle operazioni di backup e ripristino su nastro. Per informazioni dettagliate sull'esecuzione di un'operazione di backup e ripristino, consultare la documentazione dell'applicazione di backup.

### Fasi

1. Configurare una libreria di nastri scegliendo una topologia a nastro supportata da NDMP.
2. Abilitare i servizi NDMP sul sistema storage.

È possibile attivare i servizi NDMP a livello di nodo o di SVM (Storage Virtual Machine). Questo dipende dalla modalità NDMP in cui si sceglie di eseguire l'operazione di backup e ripristino su nastro.

3. Utilizza le opzioni NDMP per gestire NDMP sul tuo sistema storage.

È possibile utilizzare le opzioni NDMP a livello di nodo o SVM. Questo dipende dalla modalità NDMP in cui si sceglie di eseguire l'operazione di backup e ripristino su nastro.

È possibile modificare le opzioni NDMP a livello di nodo utilizzando `system services ndmp modify` E a livello di SVM utilizzando `vserver services ndmp modify` comando. Per ulteriori informazioni su questi comandi, consulta le pagine man.

4. Eseguire un'operazione di backup o ripristino su nastro utilizzando un'applicazione di backup abilitata per NDMP.

ONTAP supporta motori di dump e SMTape per backup e ripristino su nastro.

Per ulteriori informazioni sull'utilizzo dell'applicazione di backup (denominata anche *applicazioni di gestione dei dati* o *DMA*) per eseguire operazioni di backup o ripristino, consultare la documentazione dell'applicazione di backup.

### Informazioni correlate

[Topologie comuni di backup su nastro NDMP](#)

[Comprendere il motore di dump per i volumi FlexVol](#)

## Casi di utilizzo per la scelta di un motore di backup su nastro

ONTAP supporta due motori di backup: SMTape e dump. È necessario conoscere i casi di utilizzo dei motori di backup SMTape e dump per scegliere il motore di backup per eseguire le operazioni di backup e ripristino su nastro.

Il dump può essere utilizzato nei seguenti casi:

- Direct Access Recovery (DAR) di file e directory
- Backup di un sottoinsieme di sottodirectory o file in un percorso specifico
- Esclusione di file e directory specifici durante i backup
- Conservazione del backup per lunghi periodi di tempo

SMTape può essere utilizzato nei seguenti casi:

- Soluzione di disaster recovery
- Preservando i risparmi di deduplica e le impostazioni di deduplica sui dati di cui è stato eseguito il backup durante un'operazione di ripristino
- Backup di grandi volumi

## Gestire le unità a nastro

### Panoramica sulla gestione delle unità a nastro

Prima di eseguire un'operazione di backup o ripristino su nastro, è possibile verificare le connessioni della libreria di nastri e visualizzare le informazioni sul disco a nastro. È possibile utilizzare un'unità a nastro non qualificata emulando questa unità a nastro in un'unità a nastro qualificata. Oltre a visualizzare gli alias esistenti, è anche possibile assegnare e rimuovere gli alias del nastro.

Quando si esegue il backup dei dati su nastro, i dati vengono memorizzati in file su nastro. I contrassegni dei file separano i file del nastro e non hanno nomi. Specificare un file nastro in base alla posizione sul nastro. Si scrive un file su nastro utilizzando un dispositivo a nastro. Quando si legge il file su nastro, è necessario specificare un dispositivo con lo stesso tipo di compressione utilizzato per scrivere il file su nastro.

### Comandi per la gestione delle unità a nastro, dei media changer e delle operazioni del disco a nastro

Sono disponibili comandi per visualizzare le informazioni relative alle unità a nastro e ai media changer in un cluster, portare un'unità a nastro online e portarla fuori linea, modificare la posizione della cartuccia dell'unità a nastro, impostare e cancellare il nome alias dell'unità a nastro e reimpostare un'unità a nastro. È inoltre possibile visualizzare e ripristinare le statistiche del disco a nastro.

| Se si desidera...                                                               | Utilizzare questo comando...          |
|---------------------------------------------------------------------------------|---------------------------------------|
| Portare online un'unità a nastro                                                | <code>storage tape online</code>      |
| Cancellare un nome alias per l'unità a nastro o il caricatore di supporti       | <code>storage tape alias clear</code> |
| Attivare o disattivare un'operazione di traccia su nastro per un'unità a nastro | <code>storage tape trace</code>       |
| Modificare la posizione della cartuccia del disco a nastro                      | <code>storage tape position</code>    |

| Se si desidera...                                                                                                                  | Utilizzare questo comando...                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ripristinare un'unità a nastro                                                                                                     | <pre>storage tape reset</pre> <div>  <p>Questo comando è disponibile solo a livello di privilegi avanzati.</p> </div> |
| Impostare un nome alias per l'unità a nastro o il caricatore di supporti                                                           | <pre>storage tape alias set</pre>                                                                                                                                                                      |
| Portare un'unità a nastro offline                                                                                                  | <pre>storage tape offline</pre>                                                                                                                                                                        |
| Visualizza informazioni su tutte le unità a nastro e i media changer                                                               | <pre>storage tape show</pre>                                                                                                                                                                           |
| Visualizzare le informazioni sulle unità a nastro collegate al cluster                                                             | <ul style="list-style-type: none"> <li>• <pre>storage tape show-tape-drive</pre></li> <li>• <pre>system node hardware tape drive show</pre></li> </ul>                                                 |
| Consente di visualizzare informazioni sui media changer collegati al cluster                                                       | <pre>storage tape show-media-changer</pre>                                                                                                                                                             |
| Visualizzare le informazioni sugli errori relativi alle unità a nastro collegate al cluster                                        | <pre>storage tape show-errors</pre>                                                                                                                                                                    |
| Visualizza tutte le unità a nastro qualificate e supportate da ONTAP collegate a ciascun nodo del cluster                          | <pre>storage tape show-supported-status</pre>                                                                                                                                                          |
| Visualizzare gli alias di tutte le unità a nastro e i media changer collegati a ciascun nodo del cluster                           | <pre>storage tape alias show</pre>                                                                                                                                                                     |
| Azzerare le statistiche di lettura di un'unità a nastro                                                                            | <pre>storage stats tape zero tape_name</pre> <p>Devi usare questo comando al nodeshell.</p>                                                                                                            |
| Visualizza le unità a nastro supportate da ONTAP                                                                                   | <pre>storage show tape supported [-v]</pre> <p>Devi usare questo comando al nodeshell. È possibile utilizzare <code>-v</code> per visualizzare ulteriori dettagli su ciascuna unità a nastro.</p>      |
| Visualizzare le statistiche dei dispositivi a nastro per comprendere le prestazioni dei nastri e verificare il modello di utilizzo | <pre>storage stats tape tape_name</pre> <p>Devi usare questo comando al nodeshell.</p>                                                                                                                 |

Per ulteriori informazioni su questi comandi, consulta le pagine man.

## Utilizzare un'unità a nastro non qualificata

È possibile utilizzare un'unità a nastro non qualificata su un sistema storage se è in grado di emulare un'unità a nastro qualificata. Viene quindi trattato come un'unità a nastro qualificata. Per utilizzare un'unità a nastro non qualificata, è necessario prima determinare se emula una delle unità a nastro qualificate.

### A proposito di questa attività

Un'unità a nastro non qualificata è collegata al sistema di storage, ma non è supportata o riconosciuta da ONTAP.

### Fasi

1. Visualizzare le unità a nastro non qualificate collegate a un sistema di storage utilizzando `storage tape show-supported-status` comando.

Il seguente comando visualizza le unità a nastro collegate al sistema di storage e lo stato di supporto e qualifica di ciascuna unità a nastro. Vengono inoltre elencate le unità a nastro non qualificate.

`tape_drive_vendor_name` È un'unità a nastro non qualificata collegata al sistema di storage, ma non supportata da ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1
```

| Node: Node1               | Is        |                         |
|---------------------------|-----------|-------------------------|
| Tape Drive                | Supported | Support Status          |
| -----                     | -----     | -----                   |
| "tape_drive_vendor_name"  | false     | Nonqualified tape drive |
| Hewlett-Packard C1533A    | true      | Qualified               |
| Hewlett-Packard C1553A    | true      | Qualified               |
| Hewlett-Packard Ultrium 1 | true      | Qualified               |
| Sony SDX-300C             | true      | Qualified               |
| Sony SDX-500C             | true      | Qualified               |
| StorageTek T9840C         | true      | Dynamically Qualified   |
| StorageTek T9840D         | true      | Dynamically Qualified   |
| Tandberg LTO-2 HH         | true      | Dynamically Qualified   |

2. Emulare l'unità a nastro qualificata.

["Download NetApp: File di configurazione dei dispositivi su nastro"](#)

### Informazioni correlate

[Quali sono le unità a nastro qualificate](#)

### Assegnare alias nastro

Per una facile identificazione del dispositivo, è possibile assegnare alias del nastro a un'unità a nastro o a un caricatore di supporti. Gli alias forniscono una corrispondenza tra i nomi logici dei dispositivi di backup e un nome assegnato in modo permanente all'unità



a nastro o al caricatore di supporti.

### Fasi

1. Assegnare un alias a un'unità a nastro o a un caricatore di supporti utilizzando `storage tape alias set` comando.

Per ulteriori informazioni su questo comando, vedere le pagine `man`.

È possibile visualizzare le informazioni sul numero di serie (SN) delle unità a nastro utilizzando `system node hardware tape drive show` e informazioni sulle librerie di nastri utilizzando `system node hardware tape library show` comandi.

Il seguente comando imposta un nome alias su un'unità a nastro con numero di serie SN[123456]L4 collegato al nodo, cluster1-01:

```
cluster-01::> storage tape alias set -node cluster-01 -name st3  
-mapping SN[123456]L4
```

Il seguente comando imposta un nome alias su un media changer con numero di serie SN[65432] collegato al nodo, cluster1-01:

```
cluster-01::> storage tape alias set -node cluster-01 -name mc1  
-mapping SN[65432]
```

### Informazioni correlate

[Che cos'è l'aliasing su nastro](#)

[Rimozione degli alias del nastro](#)

### Rimuovere gli alias del nastro

È possibile rimuovere gli alias utilizzando `storage tape alias clear` comando quando gli alias persistenti non sono più necessari per un'unità a nastro o un dispositivo di sostituzione del supporto.

### Fasi

1. Rimuovere un alias da un'unità a nastro o da un caricatore di supporti utilizzando `storage tape alias clear` comando.

Per ulteriori informazioni su questo comando, vedere le pagine `man`.

Il seguente comando rimuove gli alias di tutte le unità a nastro specificando l'ambito dell'operazione di cancellazione alias in `tape`:

```
cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
```

## Al termine

Se si esegue un'operazione di backup o ripristino su nastro utilizzando NDMP, dopo aver rimosso un alias da un'unità a nastro o da un caricatore di supporti, è necessario assegnare un nuovo nome alias all'unità a nastro o al caricatore di supporti per continuare l'accesso al dispositivo a nastro.

## Informazioni correlate

[Che cos'è l'aliasing su nastro](#)

[Assegnazione degli alias del nastro](#)

## Attivazione o disattivazione delle prenotazioni su nastro

È possibile controllare il modo in cui ONTAP gestisce le prenotazioni dei dispositivi a nastro utilizzando `tape.reservations` opzione. Per impostazione predefinita, la prenotazione su nastro è disattivata.

### A proposito di questa attività

L'attivazione dell'opzione di riserva dei nastri può causare problemi se le unità a nastro, i media Changer, i bridge o le librerie non funzionano correttamente. Se i comandi su nastro indicano che il dispositivo è riservato quando nessun altro sistema di storage sta utilizzando il dispositivo, questa opzione deve essere disattivata.

### Fasi

1. Per utilizzare il meccanismo SCSI Reserve/Release o SCSI Persistent Reservations o per disattivare le prenotazioni su nastro, immettere il seguente comando nella shell del cluster shell:

```
options -option-name tape.reservations -option-value {scsi | persistent | off}
```

`scsi` Seleziona il meccanismo SCSI Reserve/Release.

`persistent` Seleziona le prenotazioni persistenti SCSI.

`off` disattiva le prenotazioni su nastro.

## Informazioni correlate

[Quali sono le prenotazioni su nastro](#)

## Comandi per la verifica delle connessioni della libreria di nastri

È possibile visualizzare informazioni sul percorso di connessione tra un sistema di storage e una configurazione della libreria di nastri collegata al sistema di storage. È possibile utilizzare queste informazioni per verificare il percorso di connessione alla configurazione della libreria di nastri o per la risoluzione dei problemi relativi ai percorsi di connessione.

È possibile visualizzare i seguenti dettagli della libreria di nastri per verificare le connessioni della libreria di nastri dopo l'aggiunta o la creazione di una nuova libreria di nastri o dopo il ripristino di un percorso guasto in un accesso a percorso singolo o multipath a una libreria di nastri. È inoltre possibile utilizzare queste informazioni durante la risoluzione di errori relativi al percorso o in caso di errore nell'accesso a una libreria di nastri.

- Nodo a cui è collegata la libreria di nastri

- ID dispositivo
- Percorso NDMP
- Nome della libreria di nastri
- Porta di destinazione e ID porta iniziatore
- Accesso a percorso singolo o multipath a una libreria di nastri per ogni porta di destinazione o FC Initiator
- Dettagli sull'integrità dei dati relativi al percorso, ad esempio "Path Errors" e "Path Qual"
- Gruppi LUN e conteggi LUN

| Se si desidera...                                                                                | Utilizzare questo comando...                             |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| Consente di visualizzare informazioni su una libreria di nastri in un cluster                    | <code>system node hardware tape library show</code>      |
| Visualizzare le informazioni sul percorso di una libreria di nastri                              | <code>storage tape library path show</code>              |
| Visualizzare le informazioni sul percorso di una libreria di nastri per ogni porta di iniziatore | <code>storage tape library path show-by-initiator</code> |
| Visualizzare le informazioni di connettività tra una libreria di nastri di storage e il cluster  | <code>storage tape library config show</code>            |

Per ulteriori informazioni su questi comandi, consulta le pagine man.

## Informazioni sulle unità a nastro

### Panoramica delle unità a nastro qualificate

È necessario utilizzare un'unità a nastro qualificata che sia stata testata e che funzioni correttamente su un sistema di storage. È possibile seguire l'aliasing del nastro e abilitare anche le prenotazioni su nastro per garantire che un solo sistema storage acceda a un'unità a nastro in qualsiasi momento.

Un'unità a nastro qualificata è un'unità a nastro che è stata testata e che funziona correttamente sui sistemi di storage. È possibile qualificare le unità a nastro per le release ONTAP esistenti utilizzando il file di configurazione del nastro.

### Formato del file di configurazione del nastro

Il formato del file di configurazione del nastro è costituito da campi quali ID vendor, ID prodotto e dettagli sui tipi di compressione per un'unità a nastro. Questo file è inoltre costituito da campi facoltativi per l'abilitazione della funzione di caricamento automatico di un'unità a nastro e la modifica dei valori di timeout dei comandi di un'unità a nastro.

Nella tabella seguente viene visualizzato il formato del file di configurazione del nastro:

| Elemento                | Dimensione     | Descrizione                                                                                                                                                                                    |
|-------------------------|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vendor_id (stringa)     | fino a 8 byte  | L'ID del vendor come riportato da SCSI Inquiry comando.                                                                                                                                        |
| product_id(stringa)     | fino a 16 byte | L'ID del prodotto riportato da SCSI Inquiry comando.                                                                                                                                           |
| id_match_size(numero)   |                | Il numero di byte dell'ID prodotto da utilizzare per la corrispondenza per rilevare l'unità a nastro da identificare, iniziando dal primo carattere dell'ID prodotto nei dati della richiesta. |
| vendor_pretty (stringa) | fino a 16 byte | Se questo parametro è presente, viene specificato dalla stringa visualizzata dal comando, storage tape show -device -names; In caso contrario, viene visualizzato INQ_VENDOR_ID.               |
| product_pretty(stringa) | fino a 16 byte | Se questo parametro è presente, viene specificato dalla stringa visualizzata dal comando, storage tape show -device -names; In caso contrario, viene visualizzato INQ_PRODUCT_ID.              |




Il vendor\_pretty e. product\_pretty i campi sono facoltativi, ma se uno di questi campi ha un valore, anche l'altro deve avere un valore.

La seguente tabella illustra la descrizione, il codice di densità e l'algoritmo di compressione per i vari tipi di compressione, ad esempio l, m, h, e. a:

| Elemento                 | Dimensione     | Descrizione                                                                                                                               |
|--------------------------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| `{l                      | m              | h                                                                                                                                         |
| a}_description=(string)` | fino a 24 byte | La stringa da stampare per il comando nodeshell, sysconfig -t, che descrive le caratteristiche della particolare impostazione di densità. |
| `{l                      | m              | h                                                                                                                                         |

| Elemento                  | Dimensione | Descrizione                                                                                                                                                                                  |
|---------------------------|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| a}_density=(hex codes)`   |            | Il codice di densità da impostare nel descrittore di blocco di pagina di modalità SCSI corrispondente al codice di densità desiderato per l, m, h o a.                                       |
| `{l                       | m          | h                                                                                                                                                                                            |
| a}_algorithm=(hex codes)` |            | L'algoritmo di compressione da impostare nella pagina SCSI Compression Mode (modalità di compressione SCSI) corrispondente al codice di densità e alla caratteristica di densità desiderata. |

La seguente tabella descrive i campi opzionali disponibili nel file di configurazione del nastro:

| Campo                     | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| autoload=(Boolean yes/no) | Questo campo è impostato su <code>yes</code> se l'unità a nastro dispone di una funzione di caricamento automatico, ovvero dopo l'inserimento della cartuccia a nastro, l'unità a nastro diventa pronta senza eseguire un SCSI <code>load</code> (unità di avvio/arresto). L'impostazione predefinita per questo campo è <code>no</code> .                                                                                                                                                                                                     |
| cmd_timeout_0x            | <p>Singolo valore di timeout. È necessario utilizzare questo campo solo se si desidera specificare un valore di timeout diverso da quello utilizzato per impostazione predefinita dal driver del nastro. Il file di esempio elenca i valori di timeout dei comandi SCSI predefiniti utilizzati dall'unità a nastro. Il valore di timeout può essere espresso in minuti (m), secondi (s) o millisecondi (ms).</p> <div>  Non modificare questo campo. </div> |

È possibile scaricare e visualizzare il file di configurazione del nastro dal NetApp Support Site.

#### Esempio di un formato di file di configurazione del nastro

Il formato del file di configurazione del nastro per l'unità a nastro HP LTO5 ULTRIUM è il seguente:

```
vendor_id="HP"
```

```
product_id="Ultrium 5-SCSI"
```

```
id_match_size=9
```

```
vendor_pretty="Hewlett-Packard"

product_pretty="LTO-5"

l_description="LTO-3(ro)/4 4/800 GB"

l_density=0x00

l_algorithm=0x00

m_description="lto-3(ro)/4 8/1600 GB cmp"

m_density=0x00

m_algorithm=0x01

h_description="LTO-5 1600 GB"

h_density=0x58

h_algorithm=0x00

a_description="lto-5 3200gb cmp"

a_density=0x58

a_algorithm=0x01

autoload="sì"
```

### Informazioni correlate

["NetApp Tools: File di configurazione dei dispositivi su nastro"](#)

### In che modo il sistema storage qualifica dinamicamente una nuova unità a nastro

Il sistema storage qualifica dinamicamente un'unità a nastro associando l'ID del vendor e l'ID del prodotto alle informazioni contenute nella tabella di qualificazione del nastro.

Quando si collega un'unità a nastro al sistema di storage, viene eseguita la ricerca di una corrispondenza tra l'ID del vendor e l'ID del prodotto tra le informazioni ottenute durante il rilevamento del nastro e le informazioni contenute nella tabella di qualificazione del nastro interno. Se il sistema storage rileva una corrispondenza, contrassegna l'unità a nastro come qualificata e può accedere all'unità a nastro. Se il sistema di storage non riesce a trovare una corrispondenza, l'unità a nastro rimane nello stato non qualificato e non viene effettuato l'accesso.

### Panoramica dei dispositivi a nastro

#### Panoramica dei dispositivi a nastro

Un dispositivo a nastro è una rappresentazione di un'unità a nastro. Si tratta di una combinazione specifica di tipo di rewind e funzionalità di compressione di un'unità a nastro.

Viene creato un dispositivo a nastro per ogni combinazione di tipo di rewind e funzionalità di compressione. Pertanto, un'unità a nastro o una libreria a nastro possono essere associati a diversi dispositivi a nastro. È necessario specificare un dispositivo a nastro per spostare, scrivere o leggere i nastri.

Quando si installa un'unità a nastro o una libreria di nastri su un sistema di storage, ONTAP crea dispositivi a nastro associati all'unità a nastro o alla libreria di nastri.

ONTAP rileva le unità a nastro e le librerie a nastro e assegna loro numeri logici e dispositivi a nastro. ONTAP rileva le librerie e le unità a nastro Fibre Channel, SAS e SCSI parallele quando sono collegate alle porte di interfaccia. ONTAP rileva questi dischi quando le interfacce sono attivate.

#### Formato del nome del dispositivo a nastro

A ciascuna periferica a nastro è associato un nome che viene visualizzato in un formato definito. Il formato include informazioni sul tipo di dispositivo, sul tipo di riavvolgimento, sull'alias e sul tipo di compressione.

Il formato del nome di un dispositivo a nastro è il seguente:

```
rewind_type st alias_number compression_type
```

`rewind_type` è il tipo di riavvolgimento.

Il seguente elenco descrive i diversi valori del tipo di riavvolgimento:

- **r**

ONTAP riavvolge il nastro al termine della scrittura del file.

- **nr**

ONTAP non riavvolge il nastro al termine della scrittura del file. È necessario utilizzare questo tipo di riavvolgimento quando si desidera scrivere più file su nastro sullo stesso nastro.

- **ur**

Questo è il tipo di riavvolgimento di scaricamento/ricarica. Quando si utilizza questo tipo di riavvolgimento, la libreria di nastri scarica il nastro quando raggiunge la fine di un file di nastro, quindi carica il nastro successivo, se presente.

È necessario utilizzare questo tipo di riavvolgimento solo nei seguenti casi:

- L'unità a nastro associata a questo dispositivo si trova in una libreria di nastri o in un caricatore di supporti che si trova in modalità di libreria.
- L'unità a nastro associata a questo dispositivo è collegata a un sistema di storage.
- Nella sequenza di nastri della libreria definita per questa unità a nastro sono disponibili nastri sufficienti per l'operazione che si sta eseguendo.



Se si registra un nastro utilizzando un dispositivo senza riavvolgimento, è necessario riavvolgere il nastro prima di leggerlo.

`st` è la designazione standard per un'unità a nastro.

`alias_number` È l'alias assegnato da ONTAP all'unità a nastro. Quando ONTAP rileva una nuova unità a nastro, ONTAP assegna un alias all'unità a nastro.

`compression_type` è un codice specifico del disco per la densità dei dati sul nastro e il tipo di compressione.

L'elenco seguente descrive i vari valori per `compression_type`:

- **a**  
Compressione massima
- **h**  
Compressione elevata
- **m**  
Compressione media
- **l**  
Compressione bassa

## Esempi

`nrst0a` specifica un dispositivo no-rewind sull'unità a nastro 0 utilizzando la compressione più elevata.

### Esempio di un elenco di dispositivi a nastro

L'esempio seguente mostra i dispositivi a nastro associati a HP Ultrium 2-SCSI:

```
Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l - rewind device,          format is: HP (200GB)
nrst0l - no rewind device,       format is: HP (200GB)
urst0l - unload/reload device,   format is: HP (200GB)
rst0m - rewind device,          format is: HP (200GB)
nrst0m - no rewind device,       format is: HP (200GB)
urst0m - unload/reload device,   format is: HP (200GB)
rst0h - rewind device,          format is: HP (200GB)
nrst0h - no rewind device,       format is: HP (200GB)
urst0h - unload/reload device,   format is: HP (200GB)
rst0a - rewind device,          format is: HP (400GB w/comp)
nrst0a - no rewind device,       format is: HP (400GB w/comp)
urst0a - unload/reload device,   format is: HP (400GB w/comp)
```

L'elenco seguente descrive le abbreviazioni dell'esempio precedente:

- GB—Gigabyte; questa è la capacità del nastro.
- w/comp—con compressione; indica la capacità del nastro con compressione.



## Numero supportato di dispositivi a nastro simultanei

ONTAP supporta un massimo di 64 connessioni simultanee a unità a nastro, 16 media changer e 16 dispositivi bridge o router per ciascun sistema storage (per nodo) in qualsiasi combinazione di collegamenti Fibre Channel, SCSI o SAS.

I dischi a nastro o i media changer possono essere dispositivi in librerie di nastri fisiche o virtuali o dispositivi standalone.



Sebbene un sistema storage sia in grado di rilevare 64 connessioni a unità a nastro, il numero massimo di sessioni di backup e ripristino che possono essere eseguite contemporaneamente dipende dai limiti di scalabilità del motore di backup.

## Informazioni correlate

[Limiti di scalabilità per sessioni di dump backup e ripristino](#)

## Aliasing del nastro

### Panoramica dell'aliasing su nastro

L'aliasing semplifica il processo di identificazione dei dispositivi. L'aliasing associa un nome di percorso fisico (PPN) o un numero di serie (SN) di un nastro o di un media changer a un nome alias persistente ma modificabile.

La seguente tabella descrive in che modo l'aliasing del nastro consente di garantire che un'unità a nastro (o una libreria di nastri o un caricatore di supporti) sia sempre associata a un singolo alias:

| Scenario                                                              | Riassegnazione dell'alias                                                |
|-----------------------------------------------------------------------|--------------------------------------------------------------------------|
| Al riavvio del sistema                                                | L'alias precedente viene riassegnato automaticamente all'unità a nastro. |
| Quando un dispositivo a nastro si sposta su un'altra porta            | L'alias può essere regolato in modo da puntare al nuovo indirizzo.       |
| Quando più di un sistema utilizza un particolare dispositivo a nastro | L'utente può impostare lo stesso alias per tutti i sistemi.              |



Quando si esegue l'aggiornamento da Data ONTAP 8.1.x a Data ONTAP 8.2.x, la funzione di alias del nastro di Data ONTAP 8.2.x modifica i nomi degli alias del nastro esistenti. In tal caso, potrebbe essere necessario aggiornare i nomi alias del nastro nell'applicazione di backup.

L'assegnazione degli alias del nastro fornisce una corrispondenza tra i nomi logici dei dispositivi di backup (ad esempio, st0 o mc1) e un nome assegnato in modo permanente a una porta, un'unità a nastro o un dispositivo di sostituzione del supporto.



st0 e st00 sono nomi logici diversi.



I nomi logici e i numeri di serie vengono utilizzati solo per accedere a una periferica. Una volta effettuato l'accesso alla periferica, vengono visualizzati tutti i messaggi di errore utilizzando il nome del percorso fisico.

Sono disponibili due tipi di nomi per l'aliasing: Nome del percorso fisico e numero di serie.

#### Quali sono i nomi dei percorsi fisici

I nomi dei percorsi fisici (PPN) sono le sequenze di indirizzi numerici che ONTAP assegna alle unità a nastro e alle librerie a nastro in base all'adattatore o allo switch SCSI-2/3 (posizione specifica) che sono collegati al sistema di storage. Le PPN sono anche note come nomi elettrici.

Le PPN dei dispositivi direct-attached utilizzano il seguente formato: `host_adapter.device_id_lun`



Il valore del LUN viene visualizzato solo per i dispositivi a nastro e a media unità di sostituzione i cui valori LUN non sono pari a zero, ovvero se il valore del LUN è pari a zero `lun` Parte della PPN non viene visualizzata.

Ad esempio, il codice PPN 8.6 indica che il numero dell'adattatore host è 8, l'ID del dispositivo è 6 e il numero dell'unità logica (LUN) è 0.

I dispositivi a nastro SAS sono anche dispositivi a collegamento diretto. Ad esempio, il codice PPN 5c.4 indica che in un sistema storage l'HBA SAS è collegato nello slot 5, il nastro SAS è collegato alla porta C dell'HBA SAS e l'ID dispositivo è 4.

Le PPN dei dispositivi collegati a switch Fibre Channel utilizzano il seguente formato: `switch:port_id.device_id_lun`

Ad esempio, PPN MY\_SWITCH:5.3L2 indica che l'unità a nastro collegata alla porta 5 di uno switch chiamato MY\_SWITCH è impostata con l'ID dispositivo 3 e dispone del LUN 2.

Il LUN (Logical Unit Number) è determinato dal disco. Le librerie e le unità a nastro Fibre Channel, SCSI e i dischi dispongono di PPN.

Le PPN delle unità a nastro e delle librerie non cambiano a meno che il nome dello switch non venga modificato, l'unità a nastro o la libreria non venga spostata o l'unità a nastro o la libreria non venga riconfigurata. Le PPN rimangono invariate dopo il riavvio. Ad esempio, se un'unità a nastro denominata MY\_SWITCH:5.3L2 viene rimossa e una nuova unità a nastro con lo stesso ID dispositivo e LUN viene collegata alla porta 5 dello switch MY\_SWITCH, la nuova unità a nastro sarà accessibile utilizzando MY\_SWITCH:5.3L2.

#### Quali sono i numeri di serie

Un numero di serie (SN) è un identificatore univoco per un'unità a nastro o un dispositivo di sostituzione del supporto. ONTAP genera alias in base al numero di serie anziché al numero di serie.

Poiché SN è un identificatore univoco per un'unità a nastro o un caricatore di supporti, l'alias rimane lo stesso indipendentemente dai percorsi di connessione multipli all'unità a nastro o al caricatore di supporti. Ciò consente ai sistemi storage di tenere traccia dello stesso disco a nastro o del caricatore di supporti in una configurazione di libreria di nastri.

Il numero di serie di un'unità a nastro o di un caricatore di supporti non cambia anche se si rinomina lo switch Fibre Channel a cui è collegato l'unità a nastro o il caricatore di supporti. Tuttavia, in una libreria di nastri se si sostituisce un'unità a nastro esistente con una nuova, ONTAP genera nuovi alias a causa della modifica del numero di serie dell'unità a nastro. Inoltre, se si sposta un'unità a nastro esistente in un nuovo slot di una libreria di nastri o si rimappano le LUN dell'unità a nastro, ONTAP genera un nuovo alias per tale unità a nastro.



È necessario aggiornare le applicazioni di backup con gli alias appena generati.

Il numero di serie di un dispositivo a nastro utilizza il seguente formato: SN [xxxxxxxxxx] L [X]

x È un carattere alfanumerico e Lx È il LUN del dispositivo a nastro. Se il LUN è 0, il valore Lx parte della stringa non viene visualizzata.

Ogni SN è composto da un massimo di 32 caratteri; il formato per il SN non è sensibile al maiuscolo/minuscolo.

### **Considerazioni per la configurazione dell'accesso su nastro multipath**

È possibile configurare due percorsi dal sistema di storage per accedere alle unità a nastro in una libreria di nastri. In caso di guasto di un percorso, il sistema di storage può utilizzare gli altri percorsi per accedere alle unità a nastro senza dover riparare immediatamente il percorso guasto. In questo modo è possibile riavviare le operazioni su nastro.

Quando si configura l'accesso su nastro multipath dal sistema storage, è necessario prendere in considerazione quanto segue:

- Nelle librerie su nastro che supportano la mappatura LUN, per l'accesso multipath a un gruppo LUN, la mappatura LUN deve essere simmetrica su ciascun percorso.

Le unità a nastro e i media changer vengono assegnati ai gruppi LUN (set di LUN che condividono lo stesso set di percorsi iniziatori) in una libreria di nastri. Tutte le unità a nastro di un gruppo LUN devono essere disponibili per le operazioni di backup e ripristino su tutti i percorsi multipli.

- È possibile configurare un massimo di due percorsi dal sistema di storage per accedere alle unità a nastro in una libreria di nastri.
- L'accesso su nastro multipath supporta il bilanciamento del carico. Il bilanciamento del carico è disattivato per impostazione predefinita.

Nell'esempio seguente, il sistema di storage accede al gruppo LUN 0 attraverso due percorsi iniziatori: 0b e 0d. In entrambi i percorsi, il gruppo LUN ha lo stesso numero LUN, 0, e numero LUN, 5. Il sistema storage accede al gruppo LUN 1 attraverso un solo percorso iniziatore, 3d.

```
STSW-3070-2_cluster::> storage tape library config show
```

| Node                   | LUN Group | LUN Count | Library Name  | Library |
|------------------------|-----------|-----------|---------------|---------|
| Target Port Initiator  |           |           |               |         |
| STSW-3070-2_cluster-01 | 0         | 5         | IBM 3573-TL_1 |         |
| 510a09800000412d       | 0b        |           |               |         |
| 0d                     |           |           |               |         |
|                        | 1         | 2         | IBM 3573-TL_2 |         |
| 50050763124b4d6f       | 3d        |           |               |         |

3 entries were displayed

Per ulteriori informazioni, consulta le pagine man.

### Come aggiungere unità nastro e librerie ai sistemi storage

È possibile aggiungere dischi a nastro e librerie al sistema di storage in modo dinamico (senza interrompere la linea del sistema).

Quando si aggiunge un nuovo media changer, il sistema storage rileva la sua presenza e la aggiunge alla configurazione. Se nelle informazioni alias si fa già riferimento al caricatore di supporti, non vengono creati nuovi nomi logici. Se non si fa riferimento alla libreria, il sistema di storage crea un nuovo alias per il dispositivo di modifica del supporto.

Nella configurazione di una libreria di nastri, è necessario configurare un'unità a nastro o un caricatore di supporti sul LUN 0 di una porta di destinazione affinché ONTAP rilevi tutti i caricatori di supporti e le unità a nastro sulla porta di destinazione.

### Quali sono le prenotazioni su nastro

Più sistemi storage possono condividere l'accesso a unità nastro, media changer, bridge o librerie di nastri. Le prenotazioni su nastro garantiscono che un solo sistema storage acceda a un dispositivo in qualsiasi momento, attivando il meccanismo SCSI Reserve/Release o SCSI Persistent Reservations per tutte le unità nastro, i media changer, i bridge e le librerie di nastri.



Tutti i sistemi che condividono i dispositivi in una libreria, indipendentemente dal fatto che gli switch siano coinvolti o meno, devono utilizzare lo stesso metodo di prenotazione.

Il meccanismo SCSI Reserve/Release per riservare i dispositivi funziona bene in condizioni normali. Tuttavia, durante le procedure di ripristino degli errori dell'interfaccia, le riserve possono andare perse. In questo caso, gli iniziatori diversi dal proprietario riservato possono accedere al dispositivo.

Le prenotazioni effettuate con le prenotazioni persistenti SCSI non sono influenzate dai meccanismi di recupero degli errori, come la reimpostazione del loop o la reimpostazione della destinazione; tuttavia, non tutti

i dispositivi implementano correttamente le prenotazioni persistenti SCSI.

## Trasferire i dati utilizzando ndmpcopy

### Trasferire i dati utilizzando la panoramica di ndmpcopy

Il `ndmpcopy` Il comando `nodeshell` trasferisce i dati tra sistemi storage che supportano NDMP v4. È possibile eseguire trasferimenti di dati completi e incrementali. È possibile trasferire volumi completi o parziali, `qtree`, `directory` o singoli file.

#### A proposito di questa attività

Utilizzando ONTAP 8.x e le versioni precedenti, i trasferimenti incrementali sono limitati a un massimo di due livelli (uno completo e fino a due backup incrementali).


A partire da ONTAP 9.0 e versioni successive, i trasferimenti incrementali sono limitati a un massimo di nove livelli (un backup completo e fino a nove backup incrementali).

Puoi correre `ndmpcopy` alla riga di comando `nodeshell` dei sistemi storage di origine e di destinazione, o a un sistema storage che non è né l'origine né la destinazione del trasferimento dei dati. Puoi anche correre `ndmpcopy` su un singolo sistema storage che sia l'origine e la destinazione del trasferimento dei dati.

È possibile utilizzare gli indirizzi IPv4 o IPv6 dei sistemi di storage di origine e di destinazione in `ndmpcopy` comando. Il formato del percorso è `/vserver_name/volume_name \[path\]`.

#### Fasi

1. Abilitare il servizio NDMP sui sistemi storage di origine e di destinazione:

| Se si esegue il trasferimento dei dati all'origine o alla destinazione in... | Utilizzare il seguente comando...                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modalità NDMP con ambito SVM                                                 | <div><pre>vserver services ndmp on</pre></div> <div><p>Per l'autenticazione NDMP nella SVM amministrativa, l'account utente è <code>admin</code> e il ruolo dell'utente è <code>admin</code> oppure <code>backup</code>. Nel SVM dei dati, l'account utente è <code>vsadmin</code> e il ruolo dell'utente è <code>vsadmin</code> oppure <code>vsadmin-backup</code> ruolo.</p></div> |
| Modalità NDMP con ambito nodo                                                | <pre>system services ndmp on</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                      |

2. Trasferire i dati all'interno di un sistema storage o tra sistemi storage utilizzando `ndmpcopy` comando al `nodeshell`:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```



I nomi DNS non sono supportati in ndmcopy. Specificare l'indirizzo IP dell'origine e della destinazione. L'indirizzo loopback (127.0.0.1) non è supportato per l'indirizzo IP di origine o di destinazione.

- Il ndmcopy il comando determina la modalità degli indirizzi per le connessioni di controllo come segue:
  - La modalità indirizzo per la connessione di controllo corrisponde all'indirizzo IP fornito.
  - È possibile eseguire l'override di queste regole utilizzando `-mcs` e. `-mcd` opzioni.
- Se l'origine o la destinazione è il sistema ONTAP, a seconda della modalità NDMP (con ambito nodo o SVM), utilizzare un indirizzo IP che consenta l'accesso al volume di destinazione.
- `source_path` e `destination_path` sono i nomi dei percorsi assoluti fino al livello granulare di volume, qtree, directory o file.
- `-mcs` specifica la modalità di indirizzamento preferita per la connessione di controllo al sistema di storage di origine.

`inet` Indica una modalità di indirizzo IPv4 e. `inet6` Indica una modalità di indirizzo IPv6.

- `-mcd` specifica la modalità di indirizzamento preferita per la connessione di controllo al sistema di storage di destinazione.

`inet` Indica una modalità di indirizzo IPv4 e. `inet6` Indica una modalità di indirizzo IPv6.

- `-md` specifica la modalità di indirizzamento preferita per i trasferimenti di dati tra i sistemi di storage di origine e di destinazione.

`inet` Indica una modalità di indirizzo IPv4 e. `inet6` Indica una modalità di indirizzo IPv6.

Se non si utilizza `-md` in ndmcopy la modalità di indirizzamento per la connessione dati viene determinata come segue:

- Se uno degli indirizzi specificati per le connessioni di controllo è un indirizzo IPv6, la modalità di indirizzo per la connessione dati è IPv6.
- Se entrambi gli indirizzi specificati per le connessioni di controllo sono indirizzi IPv4, il ndmcopy Command prima tenta una modalità di indirizzo IPv6 per la connessione dati.

In caso di esito negativo, il comando utilizza una modalità di indirizzo IPv4.



Un indirizzo IPv6, se specificato, deve essere racchiuso tra parentesi quadre.

Questo comando di esempio migra i dati da un percorso di origine (`source_path`) su un percorso di destinazione (`destination_path`).

```
> ndmcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
  -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
  192.0.2.131:/<dst_svm>/<dst_vol>
```

+

Questo comando di esempio imposta esplicitamente le connessioni di controllo e la connessione dati in modo che utilizzino la modalità di indirizzo IPv6:


```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfd7:7e78]:/<dst_svm>/<dst_vol>
```

## Opzioni per il comando ndmpcopy

È necessario conoscere le opzioni disponibili per ndmpcopy comando nodeshell per trasferire correttamente i dati.

La seguente tabella elenca le opzioni disponibili. Per ulteriori informazioni, consultare ndmpcopy pagine man disponibili attraverso il nodeshell.

| Opzione                                                                                                                                                                                                                                        | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -sa username:[password]                                                                                                                                                                                                                        | <p>Questa opzione consente di impostare il nome utente e la password per l'autenticazione di origine per la connessione al sistema di storage di origine. Si tratta di un'opzione obbligatoria.</p> <p>Per un utente senza privilegi di amministratore, è necessario specificare la password specifica NDMP generata dal sistema dell'utente. La password generata dal sistema è obbligatoria per gli utenti admin e non admin.</p> |
| -da username:[password]                                                                                                                                                                                                                        | <p>Questa opzione consente di impostare il nome utente e la password di autenticazione di destinazione per la connessione al sistema di storage di destinazione. Si tratta di un'opzione obbligatoria.</p>                                                                                                                                                                                                                          |
| -st {md5                                                                                                                                                                                                                                       | text}                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Questa opzione consente di impostare il tipo di autenticazione di origine da utilizzare durante la connessione al sistema di storage di origine. Si tratta di un'opzione obbligatoria, pertanto l'utente deve fornire text oppure md5 opzione. | -dt {md5                                                                                                                                                                                                                                                                                                                                                                                                                            |
| text}                                                                                                                                                                                                                                          | <p>Questa opzione consente di impostare il tipo di autenticazione di destinazione da utilizzare durante la connessione al sistema di storage di destinazione.</p>                                                                                                                                                                                                                                                                   |

| Opzione  | Descrizione                                                                                                                                                                                                                                                                                                                                                                                         |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -l       | Questa opzione imposta il livello di dump utilizzato per il trasferimento sul valore specificato di level. Valid Values are 0, 1, a. 9, dove 0 indica un trasferimento completo e. 1 a. 9 specifica un trasferimento incrementale. L'impostazione predefinita è 0.                                                                                                                                  |
| -d       | Questa opzione consente la generazione di messaggi di log di debug ndmpcopy. I file di log di debug ndmpcopy si trovano in /mroot/etc/log volume root. I nomi dei file di log di debug ndmpcopy si trovano in ndmpcopy.yyyymmdd formato.                                                                                                                                                            |
| -f       | Questa opzione attiva la modalità forzata. Questa modalità consente di sovrascrivere i file di sistema in /etc Nella directory principale del volume 7-Mode.                                                                                                                                                                                                                                        |
| -h       | Questa opzione consente di stampare il messaggio della guida.                                                                                                                                                                                                                                                                                                                                       |
| -p       | <p>Questa opzione richiede di inserire la password per l'autorizzazione di origine e destinazione. Questa password sovrascrive la password specificata per -sa e. -da opzioni.</p> <div>  <p>È possibile utilizzare questa opzione solo quando il comando è in esecuzione in una console interattiva.</p> </div> |
| -exclude | Questa opzione esclude i file o le directory specificati dal percorso specificato per il trasferimento dei dati. Il valore può essere un elenco separato da virgole di nomi di directory o file come .pst oppure .txt.                                                                                                                                                                              |

## NDMP per volumi FlexVol

### Informazioni su NDMP per FlexVol Volumes

Il protocollo NDMP (Network Data Management Protocol) è un protocollo standardizzato per il controllo di backup, ripristino e altri tipi di trasferimento di dati tra dispositivi di storage primari e secondari, come sistemi storage e librerie su nastro.

Attivando il supporto NDMP su un sistema storage, è possibile consentire a tale sistema di comunicare con applicazioni di backup collegate in rete abilitate NDMP (denominate anche *applicazioni di gestione dati* o *DMA*), server di dati e server a nastro che partecipano alle operazioni di backup o ripristino. Tutte le comunicazioni di rete avvengono tramite rete TCPIP o TCP/IPv6. NDMP offre inoltre un controllo di basso livello di unità nastro e media Changer.



È possibile eseguire operazioni di backup e ripristino su nastro in modalità NDMP con ambito nodo o NDMP con ambito SVM (Storage Virtual Machine).

È necessario conoscere le considerazioni da tenere in considerazione durante l'utilizzo di NDMP, l'elenco delle variabili di ambiente e le topologie di backup su nastro NDMP supportate. È inoltre possibile attivare o disattivare la funzionalità DAR avanzata. I due metodi di autenticazione supportati da ONTAP per l'autenticazione dell'accesso NDMP a un sistema storage sono: Testo normale e sfida.

#### **Informazioni correlate**

[Variabili di ambiente supportate da ONTAP](#)

#### **Informazioni sulle modalità operative NDMP**

Puoi scegliere di eseguire le operazioni di backup e ripristino su nastro a livello di nodo o di Storage Virtual Machine (SVM). Per eseguire queste operazioni con successo a livello di SVM, il servizio NDMP deve essere attivato su SVM.

Se si esegue l'aggiornamento da Data ONTAP 8.2 a Data ONTAP 8.3, la modalità operativa NDMP utilizzata nel 8.2 continuerà a essere mantenuta dopo l'aggiornamento da 8.2 a 8.3.

Se si installa un nuovo cluster con Data ONTAP 8.2 o versione successiva, NDMP si trova nella modalità NDMP con ambito SVM per impostazione predefinita. Per eseguire operazioni di backup e ripristino su nastro in modalità NDMP con ambito nodo, è necessario attivare esplicitamente la modalità NDMP con ambito nodo.

#### **Informazioni correlate**

[Comandi per la gestione della modalità NDMP con ambito nodo](#)

[Gestione della modalità NDMP con ambito nodo per volumi FlexVol](#)

[Gestione della modalità NDMP con ambito SVM per volumi FlexVol](#)

#### **Qual è la modalità NDMP con ambito nodo**

Nella modalità NDMP con ambito nodo, è possibile eseguire operazioni di backup e ripristino su nastro a livello di nodo. La modalità operativa NDMP utilizzata in Data ONTAP 8.2 continuerà a essere mantenuta dopo l'aggiornamento dalla versione 8.2 alla 8.3.

Nella modalità NDMP con ambito nodo, è possibile eseguire operazioni di backup e ripristino su nastro su un nodo proprietario del volume. Per eseguire queste operazioni, è necessario stabilire connessioni di controllo NDMP su un LIF ospitato sul nodo proprietario dei dispositivi a nastro o volume.



Questa modalità è obsoleta e verrà rimossa in una release futura.

#### **Informazioni correlate**

[Gestione della modalità NDMP con ambito nodo per volumi FlexVol](#)

#### **Qual è la modalità NDMP con ambito SVM**

Se il servizio NDMP è attivato su SVM, è possibile eseguire correttamente operazioni di backup e ripristino su nastro a livello di SVM (Storage Virtual Machine). Se l'applicazione di backup supporta l'estensione CAB, è possibile eseguire il backup e il ripristino di tutti i

volumi ospitati su diversi nodi nella SVM di un cluster.

È possibile stabilire una connessione di controllo NDMP su diversi tipi di LIF. Nella modalità NDMP con ambito SVM, queste LIF appartengono a SVM di dati o SVM di amministrazione. La connessione può essere stabilita su una LIF solo se il servizio NDMP è attivato sulla SVM proprietaria di questa LIF.

Una LIF dei dati appartiene alla SVM dei dati e la LIF di intercluster, la LIF di gestione dei nodi e la LIF di gestione dei cluster appartengono alla SVM amministrativa.

Nella modalità NDMP con ambito SVM, la disponibilità di volumi e dispositivi a nastro per le operazioni di backup e ripristino dipende dal tipo di LIF da cui viene stabilita la connessione di controllo NDMP e dallo stato dell'estensione CAB. Se l'applicazione di backup supporta l'estensione CAB e un volume e il dispositivo a nastro condividono la stessa affinità, l'applicazione di backup può eseguire un'operazione di backup o ripristino locale invece di un'operazione di backup o ripristino a tre vie.

### Informazioni correlate

[Gestione della modalità NDMP con ambito SVM per volumi FlexVol](#)

### Considerazioni sull'utilizzo di NDMP

Quando si avvia il servizio NDMP sul sistema storage, è necessario tenere conto di una serie di considerazioni.

- Ogni nodo supporta un massimo di 16 backup, ripristini o combinazioni simultanei dei due utilizzando le unità a nastro collegate.
- I servizi NDMP possono generare dati di cronologia dei file su richiesta delle applicazioni di backup NDMP.

La cronologia dei file viene utilizzata dalle applicazioni di backup per consentire il ripristino ottimizzato di set secondari selezionati di dati da un'immagine di backup. La generazione e l'elaborazione della cronologia dei file potrebbero richiedere molto tempo e richiedere un'elevata quantità di CPU sia per il sistema di storage che per l'applicazione di backup.



SMTape non supporta la cronologia dei file.

Se la protezione dei dati è configurata per il disaster recovery, dove verrà ripristinata l'intera immagine di backup, è possibile disattivare la generazione della cronologia dei file per ridurre i tempi di backup. Consultare la documentazione dell'applicazione di backup per determinare se è possibile disattivare la generazione della cronologia dei file NDMP.

- Il criterio firewall per NDMP è attivato per impostazione predefinita su tutti i tipi di LIF.
- In modalità NDMP con ambito nodo, il backup di un volume FlexVol richiede l'utilizzo dell'applicazione di backup per avviare un backup su un nodo proprietario del volume.

Tuttavia, non è possibile eseguire il backup di un volume root del nodo.

- È possibile eseguire il backup NDMP da qualsiasi LIF consentito dalle policy firewall.

Se si utilizza una LIF dati, è necessario selezionare una LIF non configurata per il failover. Se si verifica un errore di LIF dei dati durante un'operazione NDMP, l'operazione NDMP non riesce e deve essere rieseguita.

- Nella modalità NDMP con ambito nodo e nella modalità NDMP con ambito SVM (Storage Virtual Machine) senza supporto DELL'estensione CAB, la connessione dati NDMP utilizza lo stesso LIF della connessione

di controllo NDMP.

- Durante la migrazione LIF, le operazioni di backup e ripristino in corso vengono interrotte.

È necessario avviare le operazioni di backup e ripristino dopo la migrazione LIF.

- Il percorso di backup NDMP è del formato `/vserver_name/volume_name/path_name`.

`path_name` È opzionale e specifica il percorso della directory, del file o della copia Snapshot.

- Quando si esegue il backup su nastro di una destinazione SnapMirror utilizzando il motore di dump, viene eseguito il backup solo dei dati nel volume.

Tuttavia, se viene eseguito il backup su nastro di una destinazione SnapMirror utilizzando SMTape, viene eseguito anche il backup dei metadati. Il backup delle relazioni SnapMirror e dei metadati associati non viene eseguito su nastro. Pertanto, durante il ripristino, vengono ripristinati solo i dati su quel volume, ma le relazioni SnapMirror associate non vengono ripristinate.

## Informazioni correlate

[Qual è la funzione di Cluster Aware Backup Extension](#)

["Concetti di ONTAP"](#)

["Amministrazione del sistema"](#)

## Variabile di ambiente

### Panoramica delle variabili d'ambiente

Le variabili di ambiente vengono utilizzate per comunicare informazioni su un'operazione di backup o ripristino tra un'applicazione di backup abilitata per NDMP e un sistema di storage.

Ad esempio, se un utente specifica che un'applicazione di backup deve eseguire il backup `/vserver1/vol1/dir1`, l'applicazione di backup imposta la variabile di ambiente `DEL FILE SYSTEM` su `/vserver1/vol1/dir1`. Analogamente, se un utente specifica che un backup deve essere un backup di livello 1, l'applicazione di backup imposta la variabile di ambiente `LEVEL` su 1 (uno).



L'impostazione e l'esame delle variabili di ambiente sono in genere trasparenti per gli amministratori del backup, ovvero l'applicazione di backup le imposta automaticamente.

Un amministratore del backup specifica raramente le variabili di ambiente; tuttavia, è possibile modificare il valore di una variabile di ambiente rispetto a quello impostato dall'applicazione di backup per caratterizzare o risolvere un problema funzionale o di performance. Ad esempio, un amministratore potrebbe voler disattivare temporaneamente la generazione della cronologia dei file per determinare se l'elaborazione delle informazioni della cronologia dei file da parte dell'applicazione di backup contribuisce a problemi di performance o di funzionamento.

Molte applicazioni di backup offrono un mezzo per eseguire l'override o modificare le variabili di ambiente o per specificare variabili di ambiente aggiuntive. Per informazioni, consultare la documentazione dell'applicazione di backup.

## Variabili di ambiente supportate da ONTAP

Le variabili di ambiente vengono utilizzate per comunicare informazioni su un'operazione di backup o ripristino tra un'applicazione di backup abilitata per NDMP e un sistema di storage. ONTAP supporta le variabili di ambiente, che hanno un valore predefinito associato. Tuttavia, è possibile modificare manualmente questi valori predefiniti.

Se si modificano manualmente i valori impostati dall'applicazione di backup, l'applicazione potrebbe comportarsi in modo imprevedibile. Questo perché le operazioni di backup o ripristino potrebbero non eseguire le operazioni previste dall'applicazione di backup. Tuttavia, in alcuni casi, una modifica prudente potrebbe aiutare a identificare o a risolvere i problemi.

Le tabelle seguenti elencano le variabili di ambiente il cui comportamento è comune a dump e SMTape e quelle che sono supportate solo per dump e SMTape. Queste tabelle contengono anche descrizioni del funzionamento delle variabili di ambiente supportate da ONTAP se utilizzate:



Nella maggior parte dei casi, le variabili che hanno il valore, Y accetta anche T e N accetta anche F.

### Variabili di ambiente supportate per dump e SMTape

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                         |
|-----------------------|---------------|-------------|-----------------------------------------------------------------------------------------------------|
| DEBUG                 | Y oppure N    | N           | Specifica che le informazioni di debug vengono stampate.                                            |
| FILESYSTEM            | string        | none        | Specifica il nome del percorso della directory principale dei dati di cui viene eseguito il backup. |

| Variabile di ambiente | Valori validi      | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|--------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NDMP_VERSION          | return_only        | none        | <p>Non modificare la variabile NDMP_VERSION. Creata dall'operazione di backup, la variabile NDMP_VERSION restituisce la versione NDMP.</p> <p>ONTAP imposta la variabile NDMP_VERSION durante un backup per uso interno e per passare a un'applicazione di backup a scopo informativo. La versione NDMP di una sessione NDMP non è impostata con questa variabile.</p> |
| PATHNAME_SEPARATOR    | return_value       | none        | <p>Specifica il carattere di separazione del nome del percorso.</p> <p>Questo carattere dipende dal file system di cui viene eseguito il backup. Per ONTAP, il carattere "/" è assegnato a questa variabile. Il server NDMP imposta questa variabile prima di avviare un'operazione di backup su nastro.</p>                                                           |
| TIPO                  | dump oppure smtape | dump        | Specifica il tipo di backup supportato per eseguire operazioni di backup e ripristino su nastro.                                                                                                                                                                                                                                                                       |
| DETTAGLIATO           | Y oppure N         | N           | Aumenta i messaggi di log durante l'esecuzione di un'operazione di backup o ripristino su nastro.                                                                                                                                                                                                                                                                      |

**Variabili di ambiente supportate per il dump**

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------|---------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ACL_START             | return_only   | none        | <p>Creata dall'operazione di backup, la variabile ACL_START è un valore di offset utilizzato da un ripristino ad accesso diretto o da un'operazione di backup NDMP ripristinabile.</p> <p>Il valore di offset è l'offset di byte nel file dump in cui iniziano i dati ACL (Pass V) e vengono restituiti alla fine di un backup. Per un'operazione di ripristino ad accesso diretto che ripristini correttamente i dati di cui è stato eseguito il backup, il valore ACL_START deve essere passato all'operazione di ripristino all'inizio.</p> <p>Un'operazione di backup NDMP avviabile utilizza il valore ACL_START per comunicare con l'applicazione di backup in cui inizia la parte non avviabile del flusso di backup.</p> |

| Variabile di ambiente | Valori validi                 | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|-------------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BASE_DATE             | 0, -1, o. DUMP_DATE<br>valore | -1          | <p>Specifica la data di inizio dei backup incrementali.</p> <p>Quando è impostato su -1, L'identificatore incrementale BASE_DATE è disattivato. Quando è impostato su 0 su un backup di livello 0, sono attivati backup incrementali. Dopo il backup iniziale, il valore della variabile DUMP_DATE del backup incrementale precedente viene assegnato alla variabile BASE_DATE.</p> <p>Queste variabili sono un'alternativa ai backup incrementali basati SU LIVELLO/AGGIORNAME NTO.</p> |
| DIRETTO               | Y oppure N                    | N           | <p>Specifica che un ripristino deve avanzare rapidamente direttamente nella posizione sul nastro in cui risiedono i dati del file, invece di eseguire la scansione dell'intero nastro.</p> <p>Affinché il ripristino dell'accesso diretto funzioni, l'applicazione di backup deve fornire informazioni di posizionamento. Se questa variabile è impostata su Y, l'applicazione di backup specifica i nomi dei file o delle directory e le informazioni di posizionamento.</p>            |

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|---------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOME_DMP              | string        | none        | <p>Specifica il nome di un backup di una sottostruttura multipla.</p> <p>Questa variabile è obbligatoria per i backup di più sottostruttura.</p>                                                                                                                                                                                                                                                                                                                                                      |
| DUMP_DATE             | return_value  | none        | <p>Questa variabile non viene modificata direttamente. Viene creato dal backup se la variabile BASE_DATE è impostata su un valore diverso da -1.</p> <p>La variabile DUMP_DATE viene derivata antepoendo il valore di livello a 32 bit a un valore di tempo a 32 bit calcolato dal software dump. Il livello viene incrementato dall'ultimo valore di livello passato alla variabile BASE_DATE. Il valore risultante viene utilizzato come valore BASE_DATE in un backup incrementale successivo.</p> |





| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|---------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ENHANCED_DAR_ENABLED  | Y oppure N    | N           | <p>Specifica se la funzionalità DAR avanzata è attivata. La funzionalità DAR avanzata supporta directory DAR e DAR di file con flussi NT. Offre miglioramenti delle performance.</p> <p>Il DAR avanzato durante il ripristino è possibile solo se vengono soddisfatte le seguenti condizioni:</p> <ul style="list-style-type: none"> <li>• ONTAP supporta DAR avanzato.</li> <li>• La cronologia del file viene attivata (HIST=Y) durante il backup.</li> <li>• Il <code>ndmpd.offset_map.enable</code> l'opzione è impostata su on.</li> <li>• LA variabile <code>ENHANCED_DAR_ENABLED</code> è impostata su Y durante il ripristino.</li> </ul> |

| Variabile di ambiente | Valori validi  | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|----------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESCLUDI               | pattern_string | none        | <p>Specifica i file o le directory che vengono esclusi durante il backup dei dati.</p> <p>L'elenco exclude è un elenco separato da virgole di nomi di file o directory. Se il nome di un file o di una directory corrisponde a uno dei nomi nell'elenco, viene escluso dal backup.</p> <p>Le seguenti regole si applicano quando si specificano i nomi nell'elenco di esclusione:</p> <ul style="list-style-type: none"> <li>• È necessario utilizzare il nome esatto del file o della directory.</li> <li>• L'asterisco (*), un carattere jolly, deve essere il primo o l'ultimo carattere della stringa.</li> </ul> <p>Ogni stringa può contenere fino a due asterischi.</p> <ul style="list-style-type: none"> <li>• Una virgola nel nome di un file o di una directory deve essere preceduta da una barra rovesciata.</li> <li>• L'elenco di esclusione può contenere fino a 32 nomi.</li> </ul> |
|                       |                |             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------|---------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESTRARRE              | Y, N, o. E    | N           | <p>Specifica che le sottostruttura di un set di dati di cui è stato eseguito il backup devono essere ripristinate.</p> <p>L'applicazione di backup specifica i nomi delle sottostrutture da estrarre. Se un file specificato corrisponde a una directory di cui è stato eseguito il backup, la directory viene estratta in modo ricorrente.</p> <p>Per rinominare un file, una directory o un qtree durante il ripristino senza utilizzare DAR, è necessario impostare la variabile di ambiente DI ESTRAZIONE su E.</p> |
| ESTRAI_ACL            | Y oppure N    | Y           | <p>Specifica che gli ACL del file di cui è stato eseguito il backup vengono ripristinati durante un'operazione di ripristino.</p> <p>L'impostazione predefinita prevede il ripristino degli ACL durante il ripristino dei dati, ad eccezione dei DAR (DIRECT=Y).</p>                                                                                                                                                                                                                                                    |

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|---------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FORZA                 | Y oppure N    | N           | <p>Determina se l'operazione di ripristino deve controllare lo spazio del volume e la disponibilità di inode sul volume di destinazione.</p> <p>Impostare questa variabile su Y consente all'operazione di ripristino di ignorare i controlli dello spazio del volume e della disponibilità di inode sul percorso di destinazione.</p> <p>Se sul volume di destinazione non è disponibile spazio di volume o inode sufficienti, l'operazione di ripristino ripristina la quantità di dati consentita dallo spazio di volume di destinazione e dalla disponibilità di inode. L'operazione di ripristino si interrompe quando lo spazio del volume o gli inode non sono disponibili.</p> |

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|---------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HIST                  | Y oppure N    | N           | <p>Specifica che le informazioni sulla cronologia del file vengono inviate all'applicazione di backup.</p> <p>La maggior parte delle applicazioni di backup commerciali imposta la variabile HIST su Y. Se si desidera aumentare la velocità di un'operazione di backup o risolvere un problema con la raccolta della cronologia dei file, è possibile impostare questa variabile su N.</p> <div>  <p>Non impostare la variabile HIST su Y se l'applicazione di backup non supporta la cronologia dei file.</p> </div> |


| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|---------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGNORE_CTIME          | Y oppure N    | N           | <p>Specifica che non viene eseguito il backup incrementale di un file se è stato modificato solo il relativo valore ctime rispetto al backup incrementale precedente.</p> <p>Alcune applicazioni, come il software antivirus, modificano il valore ctime di un file all'interno dell'inode, anche se il file o i relativi attributi non sono stati modificati. Di conseguenza, un backup incrementale potrebbe eseguire il backup dei file che non sono stati modificati. Il</p> <p>IGNORE_CTIME la variabile deve essere specificata solo se i backup incrementali richiedono una quantità di tempo o spazio inaccettabile a causa della modifica del valore ctime.</p> <div>  <p>Il NDMP dump set di comandi IGNORE_CTIME a. false per impostazione predefinita. Impostarlo su true può causare la seguente perdita di dati:</p> <ol style="list-style-type: none"> <li>Se IGNORE_CTIME viene impostato su true con un</li> </ol> </div> |

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|---------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGNORE_QTREE          | Y oppure N    | N           | Specifica che l'operazione di ripristino non ripristina le informazioni qtree dai qtree di cui è stato eseguito il backup.                                                                                                                                                                                                                                                                                                          |
| LIVELLO               | 0-31          | 0           | <p>Specifica il livello di backup.</p> <p>Il livello 0 copia l'intero set di dati. I livelli di backup incrementali, specificati da valori superiori a 0, copiano tutti i file (nuovi o modificati) dall'ultimo backup incrementale. Ad esempio, un livello 1 esegue il backup di file nuovi o modificati dal backup di livello 0, un livello 2 esegue il backup di file nuovi o modificati dal backup di livello 1 e così via.</p> |
| ELENCO                | Y oppure N    | N           | Elenca i nomi dei file di cui è stato eseguito il backup e i numeri di inode senza ripristinare effettivamente i dati.                                                                                                                                                                                                                                                                                                              |
| LIST_QTREE            | Y oppure N    | N           | Elenca i qtree di cui è stato eseguito il backup senza ripristinare effettivamente i dati.                                                                                                                                                                                                                                                                                                                                          |

uente  
 elimina  
 zione  
 dei file,  
 che  
 vengon  
 o  
 spostati  
 tra i  
 qtree di  
 origine  
 durante  
 il  
 ripristin  
 o  
 increm  
 entale.

| Variabile di ambiente        | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|---------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOMI_SOTTOSTRUTTURA_MULTIPLI | string        | none        | <p>Specifica che il backup è un backup a più sottostruttura.</p> <p>Nella stringa sono specificate più sottostruttura, ovvero un elenco di nomi di sottostruttura separati da una nuova riga e con terminazione nulla. I sottostruttura sono specificati dai nomi dei percorsi relativi alla directory root comune, che deve essere specificata come ultimo elemento dell'elenco.</p> <p>Se si utilizza questa variabile, è necessario utilizzare anche la variabile DMP_NAME.</p> |
| NDMP_UNICODE_FH              | Y oppure N    | N           | <p>Specifica che un nome Unicode è incluso in aggiunta al nome NFS del file nelle informazioni sulla cronologia del file.</p> <p>Questa opzione non viene utilizzata dalla maggior parte delle applicazioni di backup e non deve essere impostata a meno che l'applicazione di backup non riceva questi nomi di file aggiuntivi. È necessario impostare anche la variabile HIST.</p>                                                                                               |
| NO_ACL                       | Y oppure N    | N           | <p>Specifica che gli ACL non devono essere copiati durante il backup dei dati.</p>                                                                                                                                                                                                                                                                                                                                                                                                 |



| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|---------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| STRUTTURA_NON_QUOTA   | Y oppure N    | N           | <p>Specifica che i file e le directory nei qtree devono essere ignorati durante il backup dei dati.</p> <p>Quando è impostato su Y, Gli elementi in qtree nel set di dati specificato dalla variabile DI FILESYSTEM non vengono sottoposti a backup. Questa variabile ha un effetto solo se la variabile DI FILESYSTEM specifica un intero volume. La variabile NON_QUOTA_TREE funziona solo su un backup di livello 0 e non funziona se viene specificata la variabile MULTI_SUBTREE_NAMES.</p> <div>  <p>I file o le directory specificati per essere esclusi per il backup non sono esclusi se si imposta NON_QUOTA_TREE su Y simultaneamente.</p> </div> |
| NOWRITE               | Y oppure N    | N           | <p>Specifica che l'operazione di ripristino non deve scrivere i dati sul disco.</p> <p>Questa variabile viene utilizzata per il debug.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------|---------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RICORRENTE            | Y oppure N    | Y           | <p>Specifica che le voci della directory durante un ripristino DAR devono essere espanse.</p> <p>Le variabili di ambiente DIRECT e ENHANCED_DAR_ENABLED devono essere attivate (impostate su Y). Se la variabile RICORRENTE è disattivata (impostare su N), solo le autorizzazioni e gli ACL per tutte le directory nel percorso di origine originale vengono ripristinati dal nastro, non dal contenuto delle directory. Se la variabile RICORRENTE è impostata su N Oppure la variabile RECOVER_FULL_PATHS è impostata su Y, il percorso di ripristino deve terminare con il percorso originale.</p> <div>  <p>Se la variabile RICORRENTE è disattivata e se sono presenti più percorsi di ripristino, tutti i percorsi di ripristino devono essere contenuti entro il più lungo dei percorsi di ripristino. In caso contrario, viene visualizzato un messaggio di errore.</p> </div> |

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|---------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| RECOVERY_FULL_PATHS   | Y oppure N    | N           | <p>Specifica che il percorso di ripristino completo avrà le relative autorizzazioni e gli ACL ripristinati dopo il DAR.</p> <p>DIRECT e ENHANCED_DAR_ENABLED devono essere attivati (impostare su Y). Se RECOVER_FULL_PATHS è impostato su Y, il percorso di ripristino deve terminare con il percorso originale. Se nel volume di destinazione sono già presenti directory, le relative autorizzazioni e gli ACL non verranno ripristinati dal nastro.</p> |
| AGGIORNARE            | Y oppure N    | Y           | <p>Aggiorna le informazioni sui metadati per abilitare il backup incrementale basato SUL LIVELLO.</p>                                                                                                                                                                                                                                                                                                                                                       |

#### Variabili di ambiente supportate per SMTape

| Variabile di ambiente | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|---------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BASE_DATE             | DUMP_DATE     | -1          | <p>Specifica la data di inizio dei backup incrementali.</p> <div> <p><code>`BASE_DATE`</code> È una rappresentazione e stringa degli identificatori Snapshot di riferimento. Utilizzando il <code>`BASE_DATE`</code> Stringa, SMTape individua la copia Snapshot di riferimento.</p> <p><code>`BASE_DATE`</code> non è richiesto per i backup di riferimento. Per un backup incrementale, il valore di <code>`DUMP_DATE`</code> la variabile rispetto alla linea di base precedente o al backup incrementale viene assegnata a <code>`BASE_DATE`</code> variabile.</p> <p>L'applicazione di backup assegna DUMP_DATE Valore di una precedente linea di base SMTape o backup incrementale.</p> </div> |

| Variabile di ambiente | Valori validi                                          | Predefinito | Descrizione                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------|--------------------------------------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DUMP_DATE             | return_value                                           | none        | <p>Al termine di un backup SMTape, DUMP_DATE contiene un identificatore di stringa che identifica la copia Snapshot utilizzata per tale backup. Questa copia Snapshot può essere utilizzata come copia Snapshot di riferimento per un backup incrementale successivo.</p> <p>Il valore risultante di DUMP_DATE viene utilizzato come valore BASE_DATE per i backup incrementali successivi.</p> |
| SMTAPE_BACKUP_SET_ID  | string                                                 | none        | <p>Identifica la sequenza di backup incrementali associata al backup di riferimento.</p> <p>L'ID set di backup è un ID univoco a 128 bit generato durante un backup di base.</p> <p>L'applicazione di backup assegna questo ID come input a SMTAPE_BACKUP_SET_ID variabile durante un backup incrementale.</p>                                                                                  |
| NOME_SNAPSHOT_SMTAPE  | Qualsiasi copia Snapshot valida disponibile nel volume | Invalid     | <p>Quando la variabile SMTAPE_SNAPSHOT_NAME viene impostata su una copia Snapshot, viene eseguito il backup su nastro della copia Snapshot e delle copie Snapshot precedenti.</p> <p>Per il backup incrementale, questa variabile specifica la copia Snapshot incrementale. La variabile BASE_DATE fornisce la copia Snapshot di riferimento.</p>                                               |

| Variabile di ambiente      | Valori validi | Predefinito | Descrizione                                                                                                                                                                                                                                                                                            |
|----------------------------|---------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SMTAPE_DELETE_SNA<br>PSHOT | Y oppure N    | N           | Per una copia Snapshot creata automaticamente da SMTape, quando la variabile SMTAPE_DELETE_SNA PSHOT è impostata su Y, Quindi, una volta completata l'operazione di backup, SMTape elimina questa copia Snapshot. Tuttavia, una copia Snapshot creata dall'applicazione di backup non verrà eliminata. |
| SMTAPE_BREAK_MIRR<br>OR    | Y oppure N    | N           | Quando la variabile SMTAPE_BREAK_MIRR OR è impostata su Y, il volume di tipo DP viene modificato in a. RW dopo un ripristino riuscito.                                                                                                                                                                 |

### Topologie comuni di backup su nastro NDMP

NDMP supporta una serie di topologie e configurazioni tra applicazioni di backup e sistemi storage o altri server NDMP che forniscono servizi dati (file system) e su nastro.

#### Storage system-to-local-tape

Nella configurazione più semplice, un'applicazione di backup esegue il backup dei dati da un sistema storage a un sottosistema a nastro collegato al sistema storage. La connessione di controllo NDMP esiste attraverso il confine di rete. La connessione dati NDMP esistente nel sistema di storage tra i servizi dati e quelli su nastro viene chiamata configurazione locale NDMP.

#### Storage system-to-tape collegato a un altro sistema storage

Un'applicazione di backup può anche eseguire il backup dei dati da un sistema storage a una libreria di nastri (un dispositivo di sostituzione con una o più unità nastro) collegato a un altro sistema storage. In questo caso, la connessione dati NDMP tra i servizi dati e su nastro viene fornita da una connessione di rete TCP o TCP/IPv6. Questa configurazione è denominata configurazione del sistema di storage a tre vie NDMP.

#### Libreria di nastri collegata dal sistema di storage alla rete

Le librerie a nastro abilitate per NDMP offrono una variante della configurazione a tre vie. In questo caso, la libreria a nastro si collega direttamente alla rete TCP/IP e comunica con l'applicazione di backup e il sistema di storage attraverso un server NDMP interno.

## Storage system-to-data server-to-tape o data server-to-storage system-to-tape

NDMP supporta anche configurazioni a tre vie tra sistema storage e server dati e tra server dati, anche se queste varianti sono meno diffuse. Lo storage system-to-server consente di eseguire il backup dei dati del sistema di storage su una libreria a nastro collegata all'host dell'applicazione di backup o su un altro sistema di server dati. La configurazione da server a sistema storage consente di eseguire il backup dei dati del server in una libreria di nastri collegata al sistema storage.

## Metodi di autenticazione NDMP supportati

È possibile specificare un metodo di autenticazione per consentire le richieste di connessione NDMP. ONTAP supporta due metodi per autenticare l'accesso NDMP a un sistema storage: Testo normale e sfida.

Nella modalità NDMP con ambito nodo, sia challenge che plaintext sono attivati per impostazione predefinita. Tuttavia, non è possibile disattivare la sfida. È possibile attivare e disattivare il testo non crittografato. Nel metodo di autenticazione non crittografato, la password di accesso viene trasmessa come testo non crittografato.

Nella modalità NDMP con ambito SVM (Storage Virtual Machine), per impostazione predefinita il metodo di autenticazione è un problema. A differenza della modalità NDMP con ambito di nodo, in questa modalità è possibile attivare e disattivare sia i metodi di autenticazione a testo normale che quelli di verifica.

## Informazioni correlate

[Autenticazione dell'utente in una modalità NDMP con ambito nodo](#)

[Autenticazione dell'utente in modalità NDMP con ambito SVM](#)

## Estensioni NDMP supportate da ONTAP

NDMP v4 offre un meccanismo per la creazione di estensioni del protocollo NDMP v4 senza modificare il protocollo NDMP v4 principale. È necessario conoscere le estensioni NDMP v4 supportate da ONTAP.

ONTAP supporta le seguenti estensioni NDMP v4:

- Backup cluster-aware (CAB)



Questa estensione è supportata solo nella modalità NDMP con ambito SVM.

- Connection Address Extension (CAE) per il supporto IPv6
- Classe di estensione 0x2050

Questa estensione supporta operazioni di backup avviabili e Snapshot Management Extensions.



Il NDMP\_SNAP\_RECOVER Message, che fa parte delle Snapshot Management Extensions, viene utilizzato per avviare un'operazione di recovery e trasferire i dati ripristinati da una copia Snapshot locale a una posizione del file system locale. In ONTAP, questo messaggio consente il ripristino solo di volumi e file regolari.

Il NDMP\_SNAP\_DIR\_LIST Message (messaggio) consente di sfogliare le copie Snapshot di un volume. Se si verifica un'operazione senza interruzioni mentre è in corso un'operazione di esplorazione, l'applicazione di backup deve riavviare l'operazione di esplorazione.

## Estensione di backup NDMP riavviabile per un dump supportato da ONTAP

È possibile utilizzare la funzionalità RBE (Restrictable Backup Extension) di NDMP per riavviare un backup da un checkpoint noto nel flusso di dati prima dell'errore.

## Qual è la funzionalità DAR migliorata

È possibile utilizzare la funzionalità DAR (Direct Access Recovery) avanzata per le directory DAR e DAR di file e flussi NT. Per impostazione predefinita, la funzionalità DAR avanzata è attivata.

L'attivazione della funzionalità DAR avanzata potrebbe influire sulle prestazioni di backup, poiché è necessario creare e scrivere una mappa di offset su nastro. È possibile attivare o disattivare il DAR avanzato sia nelle modalità NDMP con ambito nodo che in quelle NDMP con ambito SVM (Storage Virtual Machine).

## Limiti di scalabilità per le sessioni NDMP

È necessario conoscere il numero massimo di sessioni NDMP che è possibile stabilire simultaneamente su sistemi storage con capacità di memoria di sistema diverse. Questo numero massimo dipende dalla memoria di sistema di un sistema di storage.

I limiti indicati nella seguente tabella si riferiscono al server NDMP. I limiti indicati nella sezione "Limiti di scalabilità per le sessioni di backup e ripristino dump" si riferiscono alla sessione di dump e ripristino.

### Limiti di scalabilità per sessioni di dump backup e ripristino

| Memoria di sistema di un sistema storage        | Numero massimo di sessioni NDMP |
|-------------------------------------------------|---------------------------------|
| Meno di 16 GB                                   | 8                               |
| Superiore o uguale a 16 GB ma inferiore a 24 GB | 20                              |
| Maggiore o uguale a 24 GB                       | 36                              |

È possibile ottenere la memoria di sistema del sistema di storage utilizzando `sysconfig -a` comando (disponibile attraverso il nodeshell). Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine `man`.



## Informazioni su NDMP per FlexGroup Volumes

A partire da ONTAP 9.7, NDMP è supportato sui volumi FlexGroup.

A partire da ONTAP 9.7, il comando `ndmpcopy` è supportato per il trasferimento dei dati tra volumi FlexVol e FlexGroup.

Se si ripristina ONTAP 9.7 a una versione precedente, le informazioni di trasferimento incrementale dei trasferimenti precedenti non vengono conservate e, di conseguenza, è necessario eseguire una copia di riferimento dopo il ripristino.

A partire da ONTAP 9.8, le seguenti funzionalità NDMP sono supportate su FlexGroup Volumes:

- Il messaggio NDMP\_SNAP\_RECOVER nella classe di estensione 0x2050 può essere utilizzato per il ripristino di singoli file in un volume FlexGroup.
- NDMP Restartable Backup Extension (RBE) è supportato per i volumi FlexGroup.
- Le variabili di ambiente EXCLUDE e MULTI\_SUBTREE\_NAMES sono supportate per i volumi FlexGroup.

## Informazioni su NDMP con volumi SnapLock

La creazione di più copie di dati regolamentati offre scenari di recovery ridondanti e, utilizzando il dump e il ripristino NDMP, è possibile preservare le caratteristiche WORM (write once, Read Many) dei file di origine su un volume SnapLock.

Gli attributi WORM sui file di un volume SnapLock vengono conservati durante il backup, il ripristino e la copia dei dati; tuttavia, gli attributi WORM vengono applicati solo quando si esegue il ripristino su un volume SnapLock. Se un backup da un volume SnapLock viene ripristinato in un volume diverso da un volume SnapLock, gli attributi WORM vengono conservati ma ignorati e non applicati da ONTAP.

## Gestire la modalità NDMP con ambito nodo per i volumi FlexVol

### Gestire la modalità NDMP con ambito nodo per la panoramica dei volumi FlexVol

È possibile gestire NDMP a livello di nodo utilizzando le opzioni e i comandi NDMP. È possibile modificare le opzioni NDMP utilizzando `options` comando. Per accedere a un sistema di storage ed eseguire operazioni di backup e ripristino su nastro, è necessario utilizzare credenziali specifiche di NDMP.

Per ulteriori informazioni su `options` vedere le pagine `man`.

### Informazioni correlate

[Comandi per la gestione della modalità NDMP con ambito nodo](#)

[Qual è la modalità NDMP con ambito nodo](#)

### Comandi per la gestione della modalità NDMP con ambito nodo

È possibile utilizzare `system services ndmp` Comandi per gestire NDMP a livello di nodo. Alcuni di questi comandi sono deprecati e verranno rimossi in una release futura.

È possibile utilizzare i seguenti comandi NDMP solo a livello di privilegi avanzati:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

| Se si desidera...                                             | Utilizzare questo comando...                              |
|---------------------------------------------------------------|-----------------------------------------------------------|
| Abilitare il servizio NDMP                                    | <code>system services ndmp on*</code>                     |
| Disattiva servizio NDMP                                       | <code>system services ndmp off*</code>                    |
| Visualizzare la configurazione NDMP                           | <code>system services ndmp show*</code>                   |
| Modificare la configurazione NDMP                             | <code>system services ndmp modify*</code>                 |
| Visualizza la versione NDMP predefinita                       | <code>system services ndmp version*</code>                |
| Visualizzare la configurazione del servizio NDMP              | <code>system services ndmp service show</code>            |
| Modificare la configurazione del servizio NDMP                | <code>system services ndmp service modify</code>          |
| Visualizza tutte le sessioni NDMP                             | <code>system services ndmp status</code>                  |
| Visualizza informazioni dettagliate su tutte le sessioni NDMP | <code>system services ndmp probe</code>                   |
| Terminare la sessione NDMP specificata                        | <code>system services ndmp kill</code>                    |
| Terminare tutte le sessioni NDMP                              | <code>system services ndmp kill-all</code>                |
| Modificare la password NDMP                                   | <code>system services ndmp password*</code>               |
| Attiva la modalità NDMP con ambito nodo                       | <code>system services ndmp node-scope-mode on*</code>     |
| Disattiva la modalità NDMP con ambito nodo                    | <code>system services ndmp node-scope-mode off*</code>    |
| Visualizza lo stato della modalità NDMP con ambito nodo       | <code>system services ndmp node-scope-mode status*</code> |
| Terminare con forza tutte le sessioni NDMP                    | <code>system services ndmp service terminate</code>       |

| Se si desidera...                                              | Utilizzare questo comando...                    |
|----------------------------------------------------------------|-------------------------------------------------|
| Avviare il daemon del servizio NDMP                            | <code>system services ndmp service start</code> |
| Arrestare il daemon del servizio NDMP                          | <code>system services ndmp service stop</code>  |
| Avviare la registrazione per la sessione NDMP specificata      | <code>system services ndmp log start*</code>    |
| Interrompere la registrazione per la sessione NDMP specificata | <code>system services ndmp log stop*</code>     |

- Questi comandi sono deprecati e verranno rimossi in una release futura.

Per ulteriori informazioni su questi comandi, consultare le pagine man del `system services ndmp` comandi.

### Autenticazione dell'utente in una modalità NDMP con ambito nodo

Nella modalità NDMP con ambito nodo, è necessario utilizzare credenziali specifiche NDMP per accedere a un sistema di storage per eseguire operazioni di backup e ripristino su nastro.

L'ID utente predefinito è "root". Prima di utilizzare NDMP su un nodo, è necessario assicurarsi di modificare la password NDMP predefinita associata all'utente NDMP. È inoltre possibile modificare l'ID utente NDMP predefinito.

#### Informazioni correlate

[Comandi per la gestione della modalità NDMP con ambito nodo](#)

### Gestire la modalità NDMP con ambito SVM per i volumi FlexVol

#### Gestire la modalità NDMP con ambito SVM per la panoramica dei volumi FlexVol

È possibile gestire NDMP per SVM utilizzando le opzioni e i comandi NDMP. È possibile modificare le opzioni NDMP utilizzando `vserver services ndmp modify` comando. Nella modalità NDMP con ambito SVM, l'autenticazione dell'utente è integrata con il meccanismo di controllo degli accessi basato sui ruoli.

È possibile aggiungere NDMP nell'elenco dei protocolli consentiti o non consentiti utilizzando `vserver modify` comando. Per impostazione predefinita, NDMP si trova nell'elenco dei protocolli consentiti. Se NDMP viene aggiunto all'elenco dei protocolli non consentiti, non è possibile stabilire sessioni NDMP.

È possibile controllare il tipo di LIF su cui viene stabilita una connessione dati NDMP utilizzando `-preferred -interface-role` opzione. Durante una connessione dati NDMP, NDMP sceglie un indirizzo IP appartenente al tipo LIF specificato da questa opzione. Se gli indirizzi IP non appartengono a nessuno di questi tipi LIF, non è possibile stabilire la connessione dati NDMP. Per ulteriori informazioni su `-preferred -interface-role` vedere le pagine man.

Per ulteriori informazioni su `vserver services ndmp modify` vedere le pagine man.

## Informazioni correlate

[Comandi per la gestione della modalità NDMP con ambito SVM](#)

[Qual è la funzione di Cluster Aware Backup Extension](#)

["Concetti di ONTAP"](#)

[Qual è la modalità NDMP con ambito SVM](#)

["Amministrazione del sistema"](#)

## Comandi per la gestione della modalità NDMP con ambito SVM

È possibile utilizzare `vserver services ndmp` Comandi per la gestione di NDMP su ciascuna macchina virtuale di storage (SVM, in precedenza noto come Vserver).

| Se si desidera...                                             | Utilizzare questo comando...                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Abilitare il servizio NDMP                                    | <code>vserver services ndmp on</code> <div><p>Il servizio NDMP deve essere sempre attivato su tutti i nodi di un cluster. È possibile attivare il servizio NDMP su un nodo utilizzando <code>system services ndmp on</code> comando. Per impostazione predefinita, il servizio NDMP è sempre attivato su un nodo.</p></div> |
| Disattiva servizio NDMP                                       | <code>vserver services ndmp off</code>                                                                                                                                                                                                                                                                                                                                                                       |
| Visualizzare la configurazione NDMP                           | <code>vserver services ndmp show</code>                                                                                                                                                                                                                                                                                                                                                                      |
| Modificare la configurazione NDMP                             | <code>vserver services ndmp modify</code>                                                                                                                                                                                                                                                                                                                                                                    |
| Visualizza la versione NDMP predefinita                       | <code>vserver services ndmp version</code>                                                                                                                                                                                                                                                                                                                                                                   |
| Visualizza tutte le sessioni NDMP                             | <code>vserver services ndmp status</code>                                                                                                                                                                                                                                                                                                                                                                    |
| Visualizza informazioni dettagliate su tutte le sessioni NDMP | <code>vserver services ndmp probe</code>                                                                                                                                                                                                                                                                                                                                                                     |
| Terminare una sessione NDMP specificata                       | <code>vserver services ndmp kill</code>                                                                                                                                                                                                                                                                                                                                                                      |
| Terminare tutte le sessioni NDMP                              | <code>vserver services ndmp kill-all</code>                                                                                                                                                                                                                                                                                                                                                                  |
| Generare la password NDMP                                     | <code>vserver services ndmp generate-password</code>                                                                                                                                                                                                                                                                                                                                                         |

| Se si desidera...                                              | Utilizzare questo comando...                                                                                               |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Visualizza lo stato dell'interno NDMP                          | <code>vserver services ndmp extensions show</code><br><br>Questo comando è disponibile a livello di privilegio avanzato.   |
| Modifica (attiva o disattiva) lo stato dell'interno NDMP       | <code>vserver services ndmp extensions modify</code><br><br>Questo comando è disponibile a livello di privilegio avanzato. |
| Avviare la registrazione per la sessione NDMP specificata      | <code>vserver services ndmp log start</code><br><br>Questo comando è disponibile a livello di privilegio avanzato.         |
| Interrompere la registrazione per la sessione NDMP specificata | <code>vserver services ndmp log stop</code><br><br>Questo comando è disponibile a livello di privilegio avanzato.          |

Per ulteriori informazioni su questi comandi, consultare le pagine man del `vserver services ndmp` comandi.

### Qual è la funzione di Cluster Aware Backup Extension

CAB (Cluster Aware Backup) è un'estensione del protocollo NDMP v4. Questa estensione consente al server NDMP di stabilire una connessione dati su un nodo proprietario di un volume. Ciò consente inoltre all'applicazione di backup di determinare se i volumi e i dispositivi a nastro si trovano sullo stesso nodo di un cluster.

Per consentire al server NDMP di identificare il nodo proprietario di un volume e di stabilire una connessione dati su tale nodo, l'applicazione di backup deve supportare l'estensione CAB. CAB Extension richiede che l'applicazione di backup informi il server NDMP del volume di cui eseguire il backup o il ripristino prima di stabilire la connessione dati. Questo consente al server NDMP di determinare il nodo che ospita il volume e di stabilire in modo appropriato la connessione dati.

Con l'estensione CAB supportata dall'applicazione di backup, il server NDMP fornisce informazioni di affinità su volumi e dispositivi a nastro. Utilizzando queste informazioni di affinità, l'applicazione di backup può eseguire un backup locale invece di un backup a tre vie se un volume e un dispositivo a nastro si trovano sullo stesso nodo di un cluster.

### Disponibilità di volumi e dispositivi a nastro per il backup e il ripristino su diversi tipi di LIF

È possibile configurare un'applicazione di backup per stabilire una connessione di controllo NDMP su qualsiasi tipo di LIF in un cluster. Nella modalità NDMP con ambito SVM (Storage Virtual Machine), è possibile determinare la disponibilità di volumi e dispositivi a nastro per le operazioni di backup e ripristino in base a questi tipi di LIF e allo stato dell'estensione CAB.

Le seguenti tabelle mostrano la disponibilità di volumi e dispositivi a nastro per i tipi LIF di connessione di controllo NDMP e lo stato dell'estensione CAB:

**Disponibilità di volumi e dispositivi a nastro quando L'estensione CAB non è supportata dall'applicazione di backup**

| <b>Tipo LIF connessione di controllo NDMP</b> | <b>Volumi disponibili per il backup o il ripristino</b>                                | <b>Dispositivi a nastro disponibili per il backup o il ripristino</b>         |
|-----------------------------------------------|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|
| LIF di gestione dei nodi                      | Tutti i volumi ospitati da un nodo                                                     | Dispositivi a nastro collegati al nodo che ospita la LIF di gestione dei nodi |
| LIF dati                                      | Solo i volumi che appartengono alla SVM ospitati da un nodo che ospita la LIF dei dati | Nessuno                                                                       |
| LIF gestione cluster                          | Tutti i volumi ospitati da un nodo che ospita la LIF di gestione del cluster           | Nessuno                                                                       |
| LIF intercluster                              | Tutti i volumi ospitati da un nodo che ospita la LIF dell'intercluster                 | Dispositivi a nastro collegati al nodo che ospita la LIF dell'intercluster    |

**Disponibilità di volumi e dispositivi a nastro quando L'estensione CAB è supportata dall'applicazione di backup**

| <b>Tipo LIF connessione di controllo NDMP</b> | <b>Volumi disponibili per il backup o il ripristino</b>             | <b>Dispositivi a nastro disponibili per il backup o il ripristino</b>         |
|-----------------------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------|
| LIF di gestione dei nodi                      | Tutti i volumi ospitati da un nodo                                  | Dispositivi a nastro collegati al nodo che ospita la LIF di gestione dei nodi |
| LIF dati                                      | Tutti i volumi che appartengono alla SVM che ospita la LIF dei dati | Nessuno                                                                       |
| LIF gestione cluster                          | Tutti i volumi nel cluster                                          | Tutti i dispositivi a nastro nel cluster                                      |
| LIF intercluster                              | Tutti i volumi nel cluster                                          | Tutti i dispositivi a nastro nel cluster                                      |

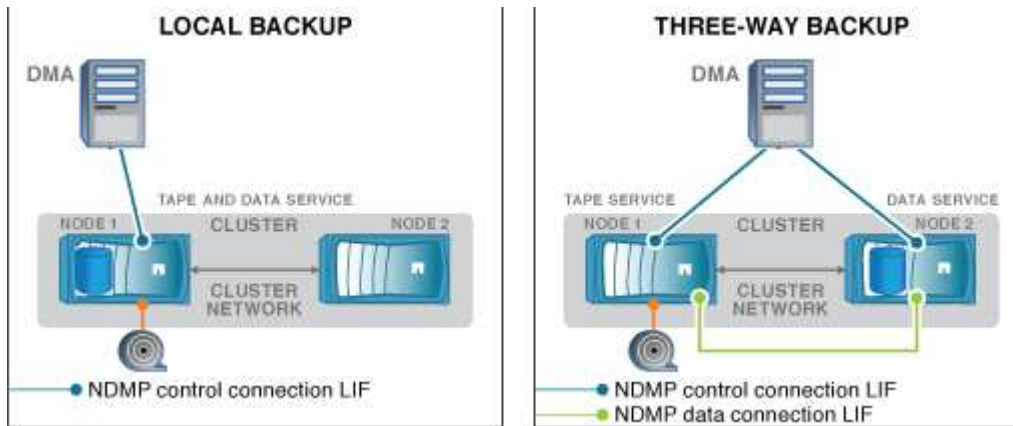
**Che cosa sono le informazioni di affinità**

Con l'applicazione di backup consapevole DEL CAB, il server NDMP fornisce informazioni univoche sulla posizione dei volumi e dei dispositivi a nastro. Utilizzando queste informazioni di affinità, l'applicazione di backup può eseguire un backup locale invece di un backup a tre vie se un volume e un dispositivo a nastro condividono la stessa affinità.

Se la connessione di controllo NDMP viene stabilita su una LIF di gestione dei nodi, LIF di gestione dei cluster,

O un LIF intercluster, l'applicazione di backup può utilizzare le informazioni di affinità per determinare se un volume e un dispositivo a nastro si trovano sullo stesso nodo ed eseguire quindi un'operazione di backup o ripristino locale o a tre vie. Se la connessione di controllo NDMP viene stabilita su una LIF dati, l'applicazione di backup esegue sempre un backup a tre vie.

#### Backup NDMP locale e backup NDMP a tre vie



Utilizzando le informazioni di affinità relative a volumi e dispositivi a nastro, DMA (applicazione di backup) esegue un backup NDMP locale sul volume e sul dispositivo a nastro situato nel nodo 1 del cluster. Se il volume si sposta dal nodo 1 al nodo 2, le informazioni di affinità relative al volume e al dispositivo a nastro cambiano. Pertanto, per un backup successivo, il DMA esegue un'operazione di backup NDMP a tre vie. In questo modo si garantisce la continuità del criterio di backup per il volume indipendentemente dal nodo in cui il volume viene spostato.

#### Informazioni correlate

[Qual è la funzione di Cluster Aware Backup Extension](#)

#### Il server NDMP supporta connessioni di controllo sicure in modalità SVM-scoped

È possibile stabilire una connessione di controllo sicura tra l'applicazione di gestione dei dati (DMA) e il server NDMP utilizzando socket sicuri (SSL/TLS) come meccanismo di comunicazione. Questa comunicazione SSL si basa sui certificati del server. Il server NDMP è in ascolto sulla porta 30000 (assegnata da IANA per il servizio "ndmps").

Dopo aver stabilito la connessione dal client su questa porta, viene eseguita la stretta di mano SSL standard in cui il server presenta il certificato al client. Quando il client accetta il certificato, l'handshake SSL è completo. Al termine di questo processo, tutte le comunicazioni tra il client e il server vengono crittografate. Il flusso di lavoro del protocollo NDMP rimane esattamente come in precedenza. La connessione NDMP sicura richiede solo l'autenticazione del certificato lato server. Un DMA può scegliere di stabilire una connessione connettendosi al servizio NDMP sicuro o al servizio NDMP standard.

Per impostazione predefinita, il servizio NDMP sicuro è disattivato per una macchina virtuale di storage (SVM). È possibile attivare o disattivare il servizio NDMP sicuro su una determinata SVM utilizzando `vserver services ndmp modify -vserver vserver -is-secure-control-connection-enabled [true|false]` comando.

#### Tipi di connessione dati NDMP

Nella modalità NDMP con ambito SVM (Storage Virtual Machine), i tipi di connessione dati NDMP supportati dipendono dal tipo di connessione di controllo NDMP LIF e dallo

stato dell'estensione CAB. Questo tipo di connessione dati NDMP indica se è possibile eseguire un'operazione di backup o ripristino NDMP locale o a tre vie.

È possibile eseguire un'operazione di backup o ripristino NDMP a tre vie su una rete TCP o TCP/IPv6. Le seguenti tabelle mostrano i tipi di connessione dati NDMP in base al tipo di connessione di controllo NDMP LIF e allo stato dell'estensione CAB.

**Tipo di connessione dati NDMP quando L'estensione CAB è supportata dall'applicazione di backup**

| Tipo LIF connessione di controllo NDMP | Tipo di connessione dati NDMP |
|----------------------------------------|-------------------------------|
| LIF di gestione dei nodi               | LOCAL (LOCALE), TCP, TCP/IPV6 |
| LIF dati                               | TCP, TCP/IPv6                 |
| LIF gestione cluster                   | LOCAL (LOCALE), TCP, TCP/IPV6 |
| LIF intercluster                       | LOCAL (LOCALE), TCP, TCP/IPV6 |

**Tipo di connessione dati NDMP quando L'estensione CAB non è supportata dall'applicazione di backup**

| Tipo LIF connessione di controllo NDMP | Tipo di connessione dati NDMP |
|----------------------------------------|-------------------------------|
| LIF di gestione dei nodi               | LOCAL (LOCALE), TCP, TCP/IPV6 |
| LIF dati                               | TCP, TCP/IPv6                 |
| LIF gestione cluster                   | TCP, TCP/IPv6                 |
| LIF intercluster                       | LOCAL (LOCALE), TCP, TCP/IPV6 |

**Informazioni correlate**

[Qual è la funzione di Cluster Aware Backup Extension](#)

["Gestione della rete"](#)

**Autenticazione dell'utente in modalità NDMP con ambito SVM**

Nella modalità NDMP con ambito SVM (Storage Virtual Machine), l'autenticazione utente NDMP è integrata con il controllo degli accessi basato sui ruoli. Nel contesto SVM, l'utente NDMP deve avere il ruolo "vsadmin" o "vsadmin-backup". In un contesto di cluster, l'utente NDMP deve avere il ruolo "admin" o "backup".

Oltre a questi ruoli predefiniti, un account utente associato a un ruolo personalizzato può essere utilizzato anche per l'autenticazione NDMP, a condizione che il ruolo personalizzato disponga della cartella "vserver Services ndmp" nella directory dei comandi e che il livello di accesso della cartella non sia "none". In questa modalità, è necessario generare una password NDMP per un determinato account utente, che viene creata tramite il controllo dell'accesso basato sul ruolo. Gli utenti del cluster in un ruolo di amministratore o backup possono accedere a una LIF di gestione dei nodi, a una LIF di gestione dei cluster o a una LIF di intercluster.



Gli utenti con ruolo vsadmin-backup o vsadmin possono accedere solo ai dati LIF per tale SVM. Pertanto, a seconda del ruolo di un utente, la disponibilità dei volumi e dei dispositivi a nastro per le operazioni di backup e ripristino varia.

Questa modalità supporta anche l'autenticazione utente per gli utenti NIS e LDAP. Pertanto, gli utenti NIS e LDAP possono accedere a più SVM con un ID utente e una password comuni. Tuttavia, l'autenticazione NDMP non supporta gli utenti di Active Directory.

In questa modalità, un account utente deve essere associato all'applicazione SSH e al metodo di autenticazione "User password".

### Informazioni correlate

[Comandi per la gestione della modalità NDMP con ambito SVM](#)

["Amministrazione del sistema"](#)

["Concetti di ONTAP"](#)

### Generare una password specifica per NDMP per gli utenti NDMP

Nella modalità NDMP con ambito SVM (Storage Virtual Machine), è necessario generare una password per un ID utente specifico. La password generata si basa sulla password di accesso effettiva per l'utente NDMP. Se la password di accesso effettiva viene modificata, è necessario generare nuovamente la password specifica di NDMP.

### Fasi

1. Utilizzare `vserver services ndmp generate-password` Per generare una password specifica per NDMP.

È possibile utilizzare questa password in qualsiasi operazione NDMP corrente o futura che richieda l'immissione della password.



Dal contesto della macchina virtuale di storage (SVM, precedentemente noto come Vserver), è possibile generare password NDMP per gli utenti che appartengono solo a tale SVM.

Nell'esempio seguente viene illustrato come generare una password specifica per NDMP per un ID utente user1:

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

2. Se si modifica la password con il normale account del sistema di storage, ripetere questa procedura per ottenere la nuova password specifica di NDMP.

## Impatto delle operazioni di backup e ripristino su nastro durante il disaster recovery nella configurazione MetroCluster

È possibile eseguire contemporaneamente operazioni di backup e ripristino su nastro durante il disaster recovery in una configurazione MetroCluster. È necessario comprendere in che modo queste operazioni vengono influenzate durante il disaster recovery.

Se le operazioni di backup e ripristino su nastro vengono eseguite su un volume di anSVM in una relazione di disaster recovery, è possibile continuare a eseguire operazioni di backup e ripristino su nastro incrementali dopo uno switchover e uno switchback.

## Informazioni sul motore di dump per i volumi FlexVol

### Informazioni sul motore di dump per i volumi FlexVol

Dump è una soluzione di backup e ripristino basata su copia Snapshot di ONTAP che consente di eseguire il backup di file e directory da una copia Snapshot a un dispositivo a nastro e di ripristinare i dati di cui è stato eseguito il backup in un sistema storage.

È possibile eseguire il backup dei dati del file system, ad esempio directory, file e relative impostazioni di sicurezza, su un dispositivo a nastro utilizzando il backup del dump. È possibile eseguire il backup di un intero volume, di un intero qtree o di una sottostruttura che non è né un intero volume né un intero qtree.

È possibile eseguire un backup o un ripristino dump utilizzando applicazioni di backup conformi a NDMP.

Quando si esegue un backup dump, è possibile specificare la copia Snapshot da utilizzare per un backup. Se non si specifica una copia Snapshot per il backup, il motore di dump crea una copia Snapshot per il backup. Una volta completata l'operazione di backup, il motore di dump elimina questa copia Snapshot.

È possibile eseguire backup di livello 0, incrementali o differenziali su nastro utilizzando il motore di dump.



Dopo il ripristino di una release precedente a Data ONTAP 8.3, è necessario eseguire un'operazione di backup di riferimento prima di eseguire un'operazione di backup incrementale.

### Informazioni correlate

["Upgrade, revert o downgrade"](#)

### Come funziona un backup dump

Un backup dump scrive i dati del file system da disco a nastro utilizzando un processo predefinito. È possibile eseguire il backup di un volume, di un qtree o di una sottostruttura che non è né un intero volume né un intero qtree.

La seguente tabella descrive il processo utilizzato da ONTAP per eseguire il backup dell'oggetto indicato dal percorso di dump:

| Fase | Azione                                                                                                                                                                                                                                                 |
|------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | Per un volume inferiore a quello completo o per i backup qtree completi, ONTAP attraversa le directory per identificare i file di cui eseguire il backup. Se si esegue il backup di un intero volume o qtree, ONTAP combina questa fase con la fase 2. |
| 2    | Per un backup completo di un volume o di un qtree completo, ONTAP identifica le directory nei volumi o qtree di cui eseguire il backup.                                                                                                                |
| 3    | ONTAP scrive le directory su nastro.                                                                                                                                                                                                                   |
| 4    | ONTAP scrive i file su nastro.                                                                                                                                                                                                                         |
| 5    | ONTAP scrive le informazioni dell'ACL (se applicabili) su nastro.                                                                                                                                                                                      |

Il backup del dump utilizza una copia Snapshot dei dati per il backup. Pertanto, non è necessario portare il volume offline prima di iniziare il backup.

Il backup del dump assegna un nome a ogni copia Snapshot creata `snapshot_for_backup.n`, dove `n` è un numero intero che inizia a 0. Ogni volta che il backup dump crea una copia Snapshot, il numero intero viene incrementato di 1. Il valore intero viene reimpostato su 0 dopo il riavvio del sistema di storage. Una volta completata l'operazione di backup, il motore di dump elimina questa copia Snapshot.

Quando ONTAP esegue più backup di dump contemporaneamente, il motore di dump crea più copie Snapshot. Ad esempio, se ONTAP esegue due backup di dump contemporaneamente, nei volumi da cui viene eseguito il backup dei dati vengono trovate le seguenti copie Snapshot: `snapshot_for_backup.0` e `snapshot_for_backup.1`.



Quando si esegue il backup da una copia Snapshot, il motore di dump non crea una copia Snapshot aggiuntiva.

### Tipi di dati di cui il motore di dump esegue il backup

Il motore di dump consente di eseguire il backup dei dati su nastro per proteggersi da disastri o interruzioni del controller. Oltre al backup di oggetti dati come file, directory, qtree o interi volumi, il motore di dump può eseguire il backup di molti tipi di informazioni su ciascun file. Conoscere i tipi di dati di cui il motore di dump può eseguire il backup e le restrizioni da prendere in considerazione può aiutarti a pianificare il tuo approccio al disaster recovery.

Oltre a eseguire il backup dei dati nei file, il motore di dump può eseguire il backup delle seguenti informazioni relative a ciascun file, a seconda dei casi:

- UNIX GID, Owner UID e permessi del file
- Tempi di accesso, creazione e modifica UNIX
- Tipo di file
- Dimensione del file
- Nome DOS, attributi DOS e tempo di creazione

- Elenchi di controllo degli accessi (ACL) con 1,024 voci di controllo degli accessi (ACE)
- Informazioni sul qtree
- Percorsi di giunzione

I percorsi di giunzione vengono sottoposti a backup come collegamenti simbolici.

- LUN e LUN

È possibile eseguire il backup di un intero oggetto LUN; tuttavia, non è possibile eseguire il backup di un singolo file all'interno dell'oggetto LUN. Allo stesso modo, è possibile ripristinare un intero oggetto LUN ma non un singolo file all'interno del LUN.



Il motore di dump esegue il backup dei cloni LUN come LUN indipendenti.

- File allineati alle macchine virtuali

Il backup dei file allineati alle macchine virtuali non è supportato nelle versioni precedenti a Data ONTAP 8.1.2.



Quando un clone del LUN con snapshot viene passato da Data ONTAP in 7-Mode a ONTAP, diventa un LUN non coerente. Il motore di dump non esegue il backup di LUN incoerenti.

Quando si ripristinano i dati su un volume, l'i/o client viene limitato alle LUN da ripristinare. La restrizione LUN viene rimossa solo al termine dell'operazione di dump restore. Allo stesso modo, durante un'operazione di ripristino di un singolo file o LUN SnapMirror, l'i/o del client viene limitato sia ai file che ai LUN ripristinati. Questa restrizione viene rimossa solo al termine dell'operazione di ripristino del singolo file o del LUN. Se viene eseguito un backup dump su un volume su cui viene eseguita un'operazione di ripristino dump o un singolo file o LUN di SnapMirror, i file o le LUN con restrizione i/o del client non vengono inclusi nel backup. Questi file o LUN vengono inclusi in una successiva operazione di backup se la restrizione i/o del client viene rimossa.



Un LUN eseguito su Data ONTAP 8.3 di cui è stato eseguito il backup su nastro può essere ripristinato solo alla versione 8.3 e successive e non a una release precedente. Se il LUN viene ripristinato a una release precedente, il LUN viene ripristinato come file.

Quando si esegue il backup di un volume secondario SnapVault o di una destinazione SnapMirror su nastro, viene eseguito il backup solo dei dati sul volume. Non viene eseguito il backup dei metadati associati. Pertanto, quando si tenta di ripristinare il volume, vengono ripristinati solo i dati di tale volume. Le informazioni sulle relazioni di SnapMirror del volume non sono disponibili nel backup e pertanto non vengono ripristinate.

Se si esegue il dump di un file che dispone solo delle autorizzazioni di Windows NT e lo si ripristina in un qtree o volume UNIX, il file ottiene le autorizzazioni UNIX predefinite per quel qtree o volume.

Se si esegue il dump di un file che dispone solo di autorizzazioni UNIX e lo si ripristina in un qtree o volume di stile NTFS, il file ottiene le autorizzazioni Windows predefinite per quel qtree o volume.

Altri dump e ripristini mantengono le autorizzazioni.

È possibile eseguire il backup dei file allineati alle macchine virtuali e di `vm-align-sector` opzione. Per ulteriori informazioni sui file allineati alle macchine virtuali, vedere ["Gestione dello storage logico"](#).

## Quali sono le catene di incremento

Una catena di incrementi è una serie di backup incrementali dello stesso percorso. Poiché è possibile specificare qualsiasi livello di backup in qualsiasi momento, è necessario comprendere le catene di incremento per poter eseguire backup e ripristini in modo efficace. È possibile eseguire 31 livelli di operazioni di backup incrementali.

Esistono due tipi di catene di incremento:

- Una catena di incrementi consecutiva, una sequenza di backup incrementali che inizia con il livello 0 e viene aumentata di 1 per ogni backup successivo.
- Una catena di incrementi non consecutiva, in cui i backup incrementali ignorano i livelli o hanno livelli fuori sequenza, come 0, 2, 3, 1, 4, o più comunemente 0, 1, 1, 1 o 0, 1, 2, 1, 2.

I backup incrementali si basano sul backup di livello inferiore più recente. Ad esempio, la sequenza dei livelli di backup 0, 2, 3, 1, 4 fornisce due catene di incrementi: 0, 2, 3 e 0, 1, 4. La seguente tabella illustra le basi dei backup incrementali:

| Ordine di backup | Livello di incremento | Catena di incremento | Base                                                                                                  | File di cui è stato eseguito il backup                                                                                    |
|------------------|-----------------------|----------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| 1                | 0                     | Entrambi             | File sul sistema storage                                                                              | Tutti i file nel percorso di backup                                                                                       |
| 2                | 2                     | 0, 2, 3              | Backup di livello 0                                                                                   | File nel percorso di backup creato dal backup di livello 0                                                                |
| 3                | 3                     | 0, 2, 3              | Backup di livello 2                                                                                   | File nel percorso di backup creato a partire dal backup di livello 2                                                      |
| 4                | 1                     | 0, 1, 4              | Backup di livello 0, perché si tratta del livello più recente che è inferiore al backup di livello 1  | File nel percorso di backup creato dopo il backup di livello 0, inclusi i file che si trovano nei backup di livello 2 e 3 |
| 5                | 4                     | 0, 1, 4              | Il backup di livello 1, perché è un livello inferiore ed è più recente dei backup di livello 0, 2 o 3 | File creati a partire dal backup di livello 1                                                                             |

## Qual è il fattore di blocco

Un blocco di nastri è costituito da 1,024 byte di dati. Durante un backup o ripristino su nastro, è possibile specificare il numero di blocchi di nastro trasferiti in ogni operazione di

lettura/scrittura. Questo numero è chiamato *fattore di blocco*.

È possibile utilizzare un fattore di blocco compreso tra 4 e 256. Se si prevede di ripristinare un backup su un sistema diverso da quello che ha eseguito il backup, il sistema di ripristino deve supportare il fattore di blocco utilizzato per il backup. Ad esempio, se si utilizza un fattore di blocco di 128, il sistema su cui si ripristina il backup deve supportare un fattore di blocco di 128.

Durante un backup NDMP, `MOVER_RECORD_SIZE` determina il fattore di blocco. ONTAP consente un valore massimo di 256 KB per `MOVER_RECORD_SIZE`.

### **Quando riavviare un backup di dump**

Un backup dump a volte non termina a causa di errori interni o esterni, come errori di scrittura su nastro, interruzioni di alimentazione, interruzioni accidentali dell'utente o incongruenze interne nel sistema storage. Se il backup non riesce per uno di questi motivi, è possibile riavviarlo.

È possibile scegliere di interrompere e riavviare un backup per evitare periodi di traffico intenso sul sistema di storage o per evitare la concorrenza per altre risorse limitate sul sistema di storage, come un'unità a nastro. È possibile interrompere un backup lungo e riavviarlo in un secondo momento se un ripristino (o backup) più urgente richiede la stessa unità a nastro. I backup riavviabili persistono durante i riavvii. È possibile riavviare un backup su nastro interrotto solo se sono soddisfatte le seguenti condizioni:

- Il backup interrotto si trova nella fase IV
- Sono disponibili tutte le copie Snapshot associate bloccate dal comando dump.
- La cronologia del file deve essere attivata.

Quando un'operazione di dump viene interrotta e lasciata in uno stato di ripristino, le copie Snapshot associate vengono bloccate. Queste copie Snapshot vengono rilasciate dopo l'eliminazione del contesto di backup. È possibile visualizzare l'elenco dei contesti di backup utilizzando `vserver services ndmp restartable backup show` comando.

```

cluster::> vserver services ndmpd restartable-backup show
Vserver      Context Identifier      Is Cleanup Pending?
-----
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

Vserver: vserver1
Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
Volume Name: /vserver1/vol1
Is Cleanup Pending?: false
Backup Engine Type: dump
Is Snapshot Copy Auto-created?: true
Dump Path: /vol/vol1
Incremental Backup Level ID: 0
Dump Name: /vserver1/vol1
Context Last Updated Time: 1460624875
Has Offset Map?: true
Offset Verify: true
Is Context Restartable?: true
Is Context Busy?: false
Restart Pass: 4
Status of Backup: 2
Snapshot Copy Name: snapshot_for_backup.1
State of the Context: 7

cluster::>"

```

### Come funziona un ripristino dump

Un ripristino dump scrive i dati del file system da nastro a disco utilizzando un processo predefinito.

La procedura riportata nella tabella seguente mostra il funzionamento del ripristino dump:

| Fase | Azione                                                       |
|------|--------------------------------------------------------------|
| 1    | ONTAP cataloga i file che devono essere estratti dal nastro. |
| 2    | ONTAP crea directory e file vuoti.                           |

| Fase | Azione                                                                                                       |
|------|--------------------------------------------------------------------------------------------------------------|
| 3    | ONTAP legge un file dal nastro, lo scrive su disco e imposta le autorizzazioni (inclusi gli ACL) su di esso. |
| 4    | ONTAP ripete le fasi 2 e 3 fino a quando tutti i file specificati non vengono copiati dal nastro.            |

### Tipi di dati ripristinati dal motore di dump

Quando si verifica un'interruzione del controller o di un'emergenza, il motore di dump offre diversi metodi per ripristinare tutti i dati di cui è stato eseguito il backup, dai singoli file agli attributi dei file, alle intere directory. Conoscere i tipi di dati ripristinati dal motore di dump e quando utilizzare il metodo di recovery può contribuire a ridurre al minimo i tempi di inattività.

È possibile ripristinare i dati in una LUN mappata online. Tuttavia, le applicazioni host non possono accedere a questo LUN fino al completamento dell'operazione di ripristino. Una volta completata l'operazione di ripristino, la cache host dei dati LUN deve essere svuotata per garantire la coerenza con i dati ripristinati.

Il motore di dump può recuperare i seguenti dati:

- Contenuto di file e directory
- Permessi di file UNIX
- ACL

Se si ripristina un file che dispone solo delle autorizzazioni di file UNIX su un qtree o volume NTFS, il file non dispone di ACL Windows NT. Il sistema di storage utilizza solo le autorizzazioni di file UNIX per questo file fino a quando non viene creato un ACL di Windows NT.



Se si ripristinano gli ACL di cui è stato eseguito il backup dai sistemi storage che eseguono Data ONTAP 8.2 ai sistemi storage che eseguono Data ONTAP 8.1.x e versioni precedenti con un limite ACE inferiore a 1,024, viene ripristinato un ACL predefinito.

- Informazioni sul qtree

Le informazioni qtree vengono utilizzate solo se un qtree viene ripristinato nella directory principale di un volume. Le informazioni qtree non vengono utilizzate se un qtree viene ripristinato in una directory inferiore, ad esempio `/vs1/vol1/subdir/lowerdir` e cessa di essere un qtree.

- Tutti gli altri attributi di file e directory
- Flussi Windows NT
- LUN

- Un LUN deve essere ripristinato a livello di volume o qtree per rimanere come LUN.

Se viene ripristinato in una directory, viene ripristinato come file perché non contiene metadati validi.

- Un LUN 7-Mode viene ripristinato come LUN su un volume ONTAP.
- È possibile ripristinare un volume 7-Mode su un volume ONTAP.



- I file allineati alle macchine virtuali ripristinati in un volume di destinazione ereditano le proprietà di allineamento delle macchine virtuali del volume di destinazione.
- Il volume di destinazione per un'operazione di ripristino potrebbe avere file con blocchi obbligatori o di avviso.

Durante l'esecuzione dell'operazione di ripristino su un volume di destinazione di questo tipo, il motore di dump ignora questi blocchi.

### Considerazioni prima del ripristino dei dati

È possibile ripristinare i dati di backup nel percorso originale o in una destinazione diversa. Se si ripristinano i dati di cui si è eseguito il backup in una destinazione diversa, è necessario preparare la destinazione per l'operazione di ripristino.

Prima di ripristinare i dati nel percorso originale o in una destinazione diversa, è necessario disporre delle seguenti informazioni e soddisfare i seguenti requisiti:

- Il livello del ripristino
- Il percorso in cui si stanno ripristinando i dati
- Il fattore di blocco utilizzato durante il backup
- Se si esegue un ripristino incrementale, tutti i nastri devono trovarsi nella catena di backup
- Unità a nastro disponibile e compatibile con il nastro da cui eseguire il ripristino

Prima di ripristinare i dati in una destinazione diversa, è necessario eseguire le seguenti operazioni:

- Se si sta ripristinando un volume, è necessario crearne uno nuovo.
- Se si sta ripristinando un qtree o una directory, è necessario rinominare o spostare i file che hanno probabilmente lo stesso nome dei file che si stanno ripristinando.



In ONTAP 9, i nomi qtree supportano il formato Unicode. Le versioni precedenti di ONTAP non supportano questo formato. Se un qtree con nomi Unicode in ONTAP 9 viene copiato in una release precedente di ONTAP utilizzando `ndmptcopy` Comando o tramite il ripristino da un'immagine di backup in un nastro, il qtree viene ripristinato come una normale directory e non come un qtree con formato Unicode.



Se un file ripristinato ha lo stesso nome di un file esistente, il file esistente viene sovrascritto dal file ripristinato. Tuttavia, le directory non vengono sovrascritte.

Per rinominare un file, una directory o un qtree durante il ripristino senza utilizzare DAR, è necessario impostare la variabile di ambiente `DI ESTRAZIONE` su `E`.

### Spazio richiesto sul sistema di storage di destinazione

Sono necessari circa 100 MB di spazio in più sul sistema di storage di destinazione rispetto alla quantità di dati da ripristinare.



L'operazione di ripristino verifica lo spazio del volume e la disponibilità di inode sul volume di destinazione all'avvio dell'operazione di ripristino. Impostazione della variabile di ambiente `FORCE` su `y` fa in modo che l'operazione di ripristino salti i controlli dello spazio del volume e della disponibilità di inode sul percorso di destinazione. Se lo spazio del volume o gli inode disponibili sul volume di destinazione non sono sufficienti, l'operazione di ripristino ripristina la quantità di dati consentita dallo spazio del volume di destinazione e dalla disponibilità dell'inode. L'operazione di ripristino si interrompe quando non rimane più spazio o inode del volume.

### Limiti di scalabilità per sessioni di dump backup e ripristino

È necessario conoscere il numero massimo di sessioni di backup e ripristino dump che possono essere eseguite simultaneamente su sistemi storage con capacità di memoria di sistema diverse. Questo numero massimo dipende dalla memoria di sistema di un sistema di storage.

I limiti indicati nella seguente tabella si riferiscono al motore di dump o ripristino. I limiti menzionati nei limiti di scalabilità per le sessioni NDMP si riferiscono al server NDMP, che sono superiori ai limiti del motore.

| Memoria di sistema di un sistema storage        | Numero totale di sessioni di backup e ripristino dump |
|-------------------------------------------------|-------------------------------------------------------|
| Meno di 16 GB                                   | 4                                                     |
| Superiore o uguale a 16 GB ma inferiore a 24 GB | 16                                                    |
| Maggiore o uguale a 24 GB                       | 32                                                    |



Se si utilizza `ndmpcopy` Comando per copiare i dati all'interno dei sistemi storage, vengono stabilite due sessioni NDMP, una per il backup del dump e l'altra per il ripristino del dump.

È possibile ottenere la memoria di sistema del sistema di storage utilizzando `sysconfig -a` comando (disponibile attraverso il nodeshell). Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine `man`.

### Informazioni correlate

[Limiti di scalabilità per le sessioni NDMP](#)

### Supporto di backup e ripristino su nastro tra Data ONTAP in 7-Mode e ONTAP

È possibile ripristinare i dati di cui è stato eseguito il backup da un sistema storage in 7-Mode o in esecuzione su ONTAP in un sistema storage in 7-Mode o in esecuzione su ONTAP.

Le seguenti operazioni di backup e ripristino su nastro sono supportate tra Data ONTAP in 7-Mode e ONTAP:

- Backup di un volume 7-Mode su un'unità a nastro collegata a un sistema storage che esegue ONTAP
- Backup di un volume ONTAP su un'unità a nastro collegata a un sistema 7-Mode
- Ripristino dei dati di backup di un volume 7-Mode da un'unità a nastro collegata a un sistema storage che esegue ONTAP

- Ripristino dei dati di backup di un volume ONTAP da un'unità a nastro collegata a un sistema 7-Mode
- Ripristino di un volume 7-Mode su un volume ONTAP



- A 7-Mode LUN is restored as a LUN on an ONTAP volume.
- You should retain the ONTAP LUN identifiers when restoring a 7-Mode LUN to an existing ONTAP LUN.

- Ripristino di un volume ONTAP su un volume 7-Mode



Un LUN ONTAP viene ripristinato come file normale su un volume 7-Mode.

## Elimina i contesti avviabili

Se si desidera avviare un backup invece di riavviare un contesto, è possibile eliminarlo.

### A proposito di questa attività

È possibile eliminare un contesto avviabile utilizzando `vserver services ndmp restartable-backup delete` fornendo il nome SVM e l'ID di contesto.

### Fasi

1. Eliminare un contesto avviabile:

```
vserver services ndmp restartable-backup delete -vserver vserver-name -context  
-id context_identifier.
```

```

cluster::> vservice ndmp restartable-backup show
Vserver      Context Identifier      Is Cleanup Pending?
-----
vserver1     330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1     481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2     5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vservice ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vservice ndmp restartable-backup show
Vserver      Context Identifier      Is Cleanup Pending?
-----
vserver1     330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2     5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"

```

### Come funziona il dump su un volume secondario SnapVault

È possibile eseguire operazioni di backup su nastro sui dati mirrorati sul volume secondario SnapVault. È possibile eseguire il backup su nastro solo dei dati mirrorati sul volume secondario SnapVault e non dei metadati della relazione SnapVault.

Quando si infrangono le relazioni mirrorate alla protezione dei dati (`snapmirror break`) O quando si verifica una risincronizzazione di SnapMirror, è sempre necessario eseguire un backup di riferimento.

### Come funziona il dump con il failover dello storage e le operazioni ARL

Prima di eseguire operazioni di dump backup o ripristino, è necessario comprendere il funzionamento di queste operazioni con operazioni di failover dello storage (takeover e giveback) o di trasferimento aggregato (ARL). Il `-override-vetoes` L'opzione determina il comportamento del motore di dump durante un failover dello storage o un'operazione ARL.

Quando è in esecuzione un'operazione di dump backup o ripristino e il `-override-vetoes` l'opzione è impostata su `false`, Un failover dello storage avviato dall'utente o un'operazione ARL viene interrotta. Tuttavia, se il `-override-vetoes` l'opzione è impostata su `true`, Quindi, il failover dello storage o l'operazione ARL viene proseguita e l'operazione di backup o ripristino del dump viene interrotta. Quando un'operazione ARL o di failover dello storage viene avviata automaticamente dal sistema storage, un'operazione di backup o ripristino dump attivo viene sempre interrotta. Non è possibile riavviare le operazioni di backup e ripristino dump anche dopo il completamento delle operazioni ARL o di failover dello storage.

## Operazioni di dump quando è supportata l'estensione DELLA CABINA

Se l'applicazione di backup supporta l'estensione CAB, è possibile continuare a eseguire operazioni di backup e ripristino incrementali senza riconfigurare le policy di backup dopo un failover dello storage o un'operazione ARL.

## Operazioni di dump quando l'estensione DELLA CABINA non è supportata

Se l'applicazione di backup non supporta l'estensione CAB, è possibile continuare a eseguire operazioni di backup e ripristino del dump incrementale se si esegue la migrazione della LIF configurata nel criterio di backup nel nodo che ospita l'aggregato di destinazione. In caso contrario, dopo il failover dello storage e l'operazione ARL, è necessario eseguire un backup di riferimento prima di eseguire l'operazione di backup incrementale.



Per le operazioni di failover dello storage, la LIF configurata nel criterio di backup deve essere migrata al nodo partner.

### Informazioni correlate

["Concetti di ONTAP"](#)

["Alta disponibilità"](#)

## Come funziona il dump con lo spostamento del volume

Le operazioni di backup e ripristino su nastro e lo spostamento del volume possono essere eseguite in parallelo fino al tentativo di cutover finale da parte del sistema di storage. Al termine di questa fase, non sono consentite nuove operazioni di backup e ripristino del nastro sul volume che viene spostato. Tuttavia, le operazioni correnti continuano a essere eseguite fino al completamento.

La seguente tabella descrive il comportamento delle operazioni di backup e ripristino su nastro dopo l'operazione di spostamento del volume:

| Se si eseguono operazioni di backup e ripristino su nastro in...                                                        | Quindi...                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Modalità NDMP con ambito SVM (Storage Virtual Machine) quando l'estensione CAB è supportata dall'applicazione di backup | È possibile continuare a eseguire operazioni di backup e ripristino su nastro incrementali su volumi di sola lettura/scrittura senza riconfigurare i criteri di backup.                                                                                                                                                                                                                                          |
| Modalità NDMP SVM-scoped quando l'estensione CAB non è supportata dall'applicazione di backup                           | È possibile continuare a eseguire operazioni di backup e ripristino su nastro incrementali su volumi di sola lettura/scrittura se si esegue la migrazione della LIF configurata nel criterio di backup nel nodo che ospita l'aggregato di destinazione. In caso contrario, dopo lo spostamento del volume, è necessario eseguire un backup di riferimento prima di eseguire l'operazione di backup incrementale. |



Quando si verifica uno spostamento del volume, se il volume appartenente a un SVM diverso sul nodo di destinazione ha lo stesso nome del volume spostato, non è possibile eseguire operazioni di backup incrementali del volume spostato.

#### Informazioni correlate

["Concetti di ONTAP"](#)

#### Come funziona il dump quando un volume FlexVol è pieno

Prima di eseguire un'operazione di backup incrementale del dump, è necessario assicurarsi che lo spazio libero nel volume FlexVol sia sufficiente.

Se l'operazione non riesce, è necessario aumentare lo spazio libero nel volume Flex Vol aumentandone le dimensioni o eliminando le copie Snapshot. Quindi eseguire nuovamente l'operazione di backup incrementale.

#### Come funziona il dump quando cambia il tipo di accesso al volume

Quando un volume di destinazione SnapMirror o un volume secondario SnapVault cambia stato da lettura/scrittura a sola lettura o da sola lettura a lettura/scrittura, è necessario eseguire un'operazione di backup o ripristino su nastro di base.

I volumi secondari di destinazione e SnapVault di SnapMirror sono volumi di sola lettura. Se si eseguono operazioni di backup e ripristino su nastro su tali volumi, è necessario eseguire un'operazione di backup o ripristino di base ogni volta che il volume cambia stato da sola lettura a sola lettura/scrittura o da lettura/scrittura a sola lettura.

#### Informazioni correlate

["Concetti di ONTAP"](#)

#### Come funziona il dump con il ripristino di un singolo file o LUN SnapMirror

Prima di eseguire operazioni di dump backup o ripristino su un volume su cui viene ripristinato un singolo file o LUN utilizzando la tecnologia SnapMirror, è necessario comprendere il funzionamento delle operazioni di dump con un'operazione di ripristino di un singolo file o LUN.

Durante un'operazione di ripristino di un singolo file o LUN SnapMirror, l'i/o del client viene limitato al file o al LUN da ripristinare. Al termine dell'operazione di ripristino di un singolo file o LUN, la restrizione i/o sul file o sul LUN viene rimossa. Se viene eseguito un backup dump su un volume in cui viene ripristinato un singolo file o LUN, il file o LUN con restrizione i/o del client non viene incluso nel backup dump. In una successiva operazione di backup, il backup di questo file o LUN viene eseguito su nastro dopo la rimozione della restrizione i/o.

Non è possibile eseguire contemporaneamente un ripristino dump e un'operazione di ripristino di un singolo file o LUN SnapMirror sullo stesso volume.

#### Influenza delle operazioni di backup e ripristino dump nelle configurazioni MetroCluster

Prima di eseguire operazioni di dump backup e ripristino in una configurazione MetroCluster, è necessario comprendere in che modo le operazioni di dump vengono influenzate quando si verifica un'operazione di switchover o switchback.

### Eseguire il dump dell'operazione di backup o ripristino e passare al switchover

Prendere in considerazione due cluster: Cluster 1 e cluster 2. Durante un'operazione di dump backup o ripristino sul cluster 1, se viene avviato uno switchover dal cluster 1 al cluster 2, si verifica quanto segue:

- Se il valore di `override-vetoes` l'opzione è `false`, lo switchover viene interrotto e l'operazione di backup o ripristino continua.
- Se il valore dell'opzione è `true`, l'operazione di backup o ripristino del dump viene interrotta e lo switchover continua.

### Eseguire un'operazione di dump backup o ripristino seguita da switchback

Viene eseguito uno switchover dal cluster 1 al cluster 2 e viene avviata un'operazione di dump backup o ripristino sul cluster 2. L'operazione di dump esegue il backup o il ripristino di un volume che si trova nel cluster 2. A questo punto, se viene avviato uno switchback dal cluster 2 al cluster 1, si verifica quanto segue:

- Se il valore di `override-vetoes` l'opzione è `false`, quindi lo switchback viene annullato e l'operazione di backup o ripristino continua.
- Se il valore dell'opzione è `true`, l'operazione di backup o ripristino viene interrotta e lo switchback continua.

### Operazione di dump backup o ripristino avviata durante uno switchover o uno switchback

Durante lo switchover dal cluster 1 al cluster 2, se viene avviata un'operazione di dump backup o ripristino sul cluster 1, l'operazione di backup o ripristino non riesce e lo switchover continua.

Durante uno switchback dal cluster 2 al cluster 1, se viene avviata un'operazione di dump backup o ripristino dal cluster 2, l'operazione di backup o ripristino non riesce e lo switchback continua.

## Informazioni sul motore SMTape per volumi FlexVol

### Informazioni sul motore SMTape per volumi FlexVol

SMTape è una soluzione di disaster recovery di ONTAP che esegue il backup di blocchi di dati su nastro. È possibile utilizzare SMTape per eseguire backup dei volumi su nastri. Tuttavia, non è possibile eseguire un backup a livello di qtree o sottostruttura. SMTape supporta backup baseline, differenziali e incrementali. SMTape non richiede una licenza.

È possibile eseguire un'operazione di backup e ripristino SMTape utilizzando un'applicazione di backup compatibile con NDMP. È possibile scegliere SMTape per eseguire operazioni di backup e ripristino solo nella modalità NDMP con ambito SVM (Storage Virtual Machine).



Il processo di revversion non è supportato quando è in corso una sessione di backup o ripristino SMTape. È necessario attendere il termine della sessione oppure interrompere la sessione NDMP.

Con SMTape, è possibile eseguire il backup di 255 copie Snapshot. Per i backup baseline, incrementali o differenziali successivi, è necessario eliminare le copie Snapshot di backup precedenti.

Prima di eseguire un ripristino baseline, il volume su cui vengono ripristinati i dati deve essere di tipo `DP` e questo volume deve essere nello stato limitato. Una volta eseguito correttamente il ripristino, il volume viene automaticamente online. È possibile eseguire ripristini incrementali o differenziali successivi su questo volume

nell'ordine in cui sono stati eseguiti i backup.

### **Utilizzare le copie Snapshot durante il backup SMTape**

È necessario comprendere come vengono utilizzate le copie Snapshot durante un backup di base SMTape e un backup incrementale. È inoltre necessario tenere presente alcune considerazioni durante l'esecuzione di un backup con SMTape.

#### **Backup di riferimento**

Durante l'esecuzione di un backup di riferimento, è possibile specificare il nome della copia Snapshot di cui eseguire il backup su nastro. Se non viene specificata alcuna copia Snapshot, a seconda del tipo di accesso del volume (lettura/scrittura o sola lettura), viene creata automaticamente una copia Snapshot o vengono utilizzate le copie Snapshot esistenti. Quando si specifica una copia Snapshot per il backup, viene eseguito anche il backup su nastro di tutte le copie Snapshot precedenti alla copia Snapshot specificata.

Se non si specifica una copia Snapshot per il backup, si verifica quanto segue:

- Per un volume di lettura/scrittura, viene creata automaticamente una copia Snapshot.

La copia Snapshot appena creata e tutte le copie Snapshot precedenti vengono sottoposte a backup su nastro.

- Per un volume di sola lettura, viene eseguito il backup su nastro di tutte le copie Snapshot, inclusa l'ultima copia Snapshot.

Non viene eseguito il backup delle nuove copie Snapshot create dopo l'avvio del backup.

#### **Backup incrementale**

Per le operazioni di backup incrementali o differenziali SMTape, le applicazioni di backup conformi a NDMP creano e gestiscono le copie Snapshot.

È necessario specificare sempre una copia Snapshot durante l'esecuzione di un'operazione di backup incrementale. Per un'operazione di backup incrementale riuscita, la copia Snapshot di cui è stato eseguito il backup durante l'operazione di backup precedente (baseline o incrementale) deve trovarsi sul volume da cui viene eseguito il backup. Per assicurarsi di utilizzare questa copia Snapshot di backup, è necessario prendere in considerazione il criterio Snapshot assegnato a questo volume durante la configurazione del criterio di backup.

#### **Considerazioni sui backup SMTape sulle destinazioni SnapMirror**

- Una relazione mirror per la protezione dei dati crea copie Snapshot temporanee sul volume di destinazione per la replica.

Non utilizzare queste copie Snapshot per il backup SMTape.

- Se si verifica un aggiornamento di SnapMirror su un volume di destinazione in una relazione mirror di protezione dei dati durante un'operazione di backup SMTape sullo stesso volume, la copia Snapshot di cui è stato eseguito il backup da SMTape non deve essere eliminata sul volume di origine.

Durante l'operazione di backup, SMTape blocca la copia Snapshot sul volume di destinazione e, se la copia Snapshot corrispondente viene eliminata sul volume di origine, l'operazione di aggiornamento di SnapMirror successiva non riesce.



- Non utilizzare queste copie Snapshot durante il backup incrementale.

## Funzionalità SMTape

Le funzionalità SMTape, come backup di copie Snapshot, backup incrementali e differenziali, conservazione delle funzionalità di deduplica e compressione sui volumi ripristinati e seeding dei nastri, consentono di ottimizzare le operazioni di backup e ripristino dei nastri.

SMTape offre le seguenti funzionalità:

- Offre una soluzione di disaster recovery
- Consente backup incrementali e differenziali
- Esegue il backup delle copie Snapshot
- Consente il backup e il ripristino dei volumi deduplicati e preserva la deduplica sui volumi ripristinati
- Esegue il backup dei volumi compressi e mantiene la compressione sui volumi ripristinati
- Consente il seeding dei nastri

SMTape supporta il fattore di blocco in multipli di 4 KB, nell'intervallo da 4 KB a 256 KB.



È possibile ripristinare i dati su volumi creati solo in due release principali consecutive di ONTAP.

## Funzionalità non supportate in SMTape

SMTape non supporta backup avviabili e verifica dei file di cui è stato eseguito il backup.

## Limiti di scalabilità per le sessioni di backup e ripristino SMTape

Durante l'esecuzione delle operazioni di backup e ripristino SMTape tramite NDMP o CLI (seeding su nastro), è necessario conoscere il numero massimo di sessioni di backup e ripristino SMTape che è possibile eseguire contemporaneamente su sistemi storage con capacità di memoria di sistema diverse. Questo numero massimo dipende dalla memoria di sistema di un sistema di storage.



I limiti di scalabilità delle sessioni di backup e ripristino SMTape sono diversi dai limiti delle sessioni NDMP e dei limiti delle sessioni di dump.

| Memoria di sistema del sistema storage          | Numero totale di sessioni di backup e ripristino SMTape |
|-------------------------------------------------|---------------------------------------------------------|
| Meno di 16 GB                                   | 6                                                       |
| Superiore o uguale a 16 GB ma inferiore a 24 GB | 16                                                      |
| Maggiore o uguale a 24 GB                       | 32                                                      |

È possibile ottenere la memoria di sistema del sistema di storage utilizzando `sysconfig -a` comando (disponibile attraverso il `nodeshell`). Per ulteriori informazioni sull'utilizzo di questo comando, vedere le pagine `man`.

#### Informazioni correlate

[Limiti di scalabilità per le sessioni NDMP](#)

[Limiti di scalabilità per sessioni di dump backup e ripristino](#)

#### Che cos'è il seeding del nastro

Il seeding dei nastri è una funzionalità SMTape che consente di inizializzare un volume FlexVol di destinazione in una relazione mirror di protezione dei dati.

Il seeding su nastro consente di stabilire una relazione mirror per la protezione dei dati tra un sistema di origine e un sistema di destinazione su una connessione a bassa larghezza di banda.

Il mirroring incrementale delle copie Snapshot dall'origine alla destinazione è possibile su una connessione a bassa larghezza di banda. Tuttavia, il mirroring iniziale della copia Snapshot di base richiede molto tempo su una connessione a bassa larghezza di banda. In questi casi, è possibile eseguire un backup SMTape del volume di origine su un nastro e utilizzare il nastro per trasferire la copia Snapshot di base iniziale nella destinazione. È quindi possibile impostare gli aggiornamenti incrementali di SnapMirror nel sistema di destinazione utilizzando la connessione a bassa larghezza di banda.

#### Informazioni correlate

["Concetti di ONTAP"](#)

#### Funzionamento di SMTape con il failover dello storage e le operazioni ARL

Prima di eseguire operazioni di backup o ripristino SMTape, è necessario comprendere il funzionamento di queste operazioni con operazioni di failover dello storage (takeover e giveback) o di riposizionamento degli aggregati (ARL). Il `-override-vetoes` L'opzione determina il comportamento del motore SMTape durante un'operazione ARL o di failover dello storage.

Quando è in esecuzione un'operazione di backup o ripristino SMTape e il `-override-vetoes` l'opzione è impostata su `false`, Un failover dello storage avviato dall'utente o un'operazione ARL viene interrotta e l'operazione di backup o ripristino viene completata. Se l'applicazione di backup supporta l'estensione CAB, è possibile continuare a eseguire operazioni di backup e ripristino SMTape incrementali senza riconfigurare i criteri di backup. Tuttavia, se il `-override-vetoes` l'opzione è impostata su `true`, Quindi il failover dello storage o l'operazione ARL viene proseguita e l'operazione di backup o ripristino SMTape viene interrotta.

#### Informazioni correlate

["Gestione della rete"](#)

["Alta disponibilità"](#)

#### Funzionamento di SMTape con lo spostamento del volume

Le operazioni di backup SMTape e le operazioni di spostamento del volume possono essere eseguite in parallelo fino a quando il sistema storage non tenta la fase di cutover finale. Dopo questa fase, non è possibile eseguire nuove operazioni di backup SMTape

sul volume che viene spostato. Tuttavia, le operazioni correnti continuano a essere eseguite fino al completamento.

Prima di avviare la fase di cutover di un volume, l'operazione di spostamento del volume verifica la presenza di operazioni di backup SMTape attive sullo stesso volume. Se sono presenti operazioni di backup SMTape attive, l'operazione di spostamento del volume passa a uno stato di cutover rinviato e consente il completamento delle operazioni di backup SMTape. Una volta completate queste operazioni di backup, è necessario riavviare manualmente l'operazione di spostamento del volume.

Se l'applicazione di backup supporta l'estensione CAB, è possibile continuare a eseguire operazioni di backup e ripristino su nastro incrementali su volumi di sola lettura/scrittura senza riconfigurare i criteri di backup.

Le operazioni di ripristino di base e di spostamento del volume non possono essere eseguite contemporaneamente; tuttavia, il ripristino incrementale può essere eseguito in parallelo con le operazioni di spostamento del volume, con un comportamento simile a quello delle operazioni di backup SMTape durante le operazioni di spostamento del volume.

#### **Informazioni correlate**

["Concetti di ONTAP"](#)

#### **Funzionamento di SMTape con le operazioni di re-hosting dei volumi**

Le operazioni SMTape non possono iniziare quando è in corso un'operazione di rehost del volume su un volume. Quando un volume è coinvolto in un'operazione di rehost del volume, le sessioni SMTape non devono essere avviate su quel volume.

Se è in corso un'operazione di rehost del volume, il backup o il ripristino SMTape non riesce. Se è in corso un backup o ripristino SMTape, le operazioni di rehost del volume non riescono e viene visualizzato un messaggio di errore appropriato. Questa condizione si applica alle operazioni di backup o ripristino basate su NDMP e CLI.

#### **In che modo i criteri di backup NDMP vengono influenzati durante ADB**

Quando il bilanciamento automatico dei dati (ADB) è attivato, il bilanciamento analizza le statistiche di utilizzo degli aggregati per identificare l'aggregato che ha superato la percentuale di utilizzo ad alta soglia configurata.

Dopo aver identificato l'aggregato che ha superato la soglia, il bilanciamento identifica un volume che può essere spostato in aggregati che risiedono in un altro nodo del cluster e tenta di spostare tale volume. Questa situazione influisce sul criterio di backup configurato per questo volume perché se l'applicazione di gestione dei dati (DMA) non è a conoscenza DEL CAB, l'utente deve riconfigurare il criterio di backup ed eseguire l'operazione di backup di riferimento.



Se il DMA è in GRADO di riconoscere IL CAB e il criterio di backup è stato configurato utilizzando un'interfaccia specifica, ADB non viene interessato.

#### **Impatto delle operazioni di backup e ripristino SMTape nelle configurazioni MetroCluster**

Prima di eseguire operazioni di backup e ripristino SMTape in una configurazione MetroCluster, è necessario comprendere in che modo le operazioni SMTape vengono influenzate quando si verifica un'operazione di switchover o switchback.

### **Operazione di backup o ripristino SMTape seguita da switchover**

Prendere in considerazione due cluster: Cluster 1 e cluster 2. Durante un'operazione di backup o ripristino SMTape sul cluster 1, se viene avviato uno switchover dal cluster 1 al cluster 2, si verifica quanto segue:

- Se il valore di `-override-vetoes` l'opzione è `false`, il processo di switchover viene interrotto e l'operazione di backup o ripristino continua.
- Se il valore dell'opzione è `true`, L'operazione di backup o ripristino SMTape viene interrotta e il processo di switchover continua.

### **Operazione di backup o ripristino SMTape seguita da switchback**

Viene eseguito uno switchover dal cluster 1 al cluster 2 e viene avviata un'operazione di backup o ripristino SMTape sul cluster 2. L'operazione SMTape esegue il backup o il ripristino di un volume che si trova nel cluster 2. A questo punto, se viene avviato uno switchback dal cluster 2 al cluster 1, si verifica quanto segue:

- Se il valore di `-override-vetoes` l'opzione è `false`, il processo di switchback viene interrotto e l'operazione di backup o ripristino continua.
- Se il valore dell'opzione è `true`, l'operazione di backup o ripristino viene interrotta e il processo di switchback continua.

### **Operazione di backup o ripristino SMTape avviata durante uno switchover o uno switchback**

Durante un processo di switchover dal cluster 1 al cluster 2, se viene avviata un'operazione di backup o ripristino SMTape sul cluster 1, l'operazione di backup o ripristino non riesce e lo switchover continua.

Durante un processo di switchback dal cluster 2 al cluster 1, se viene avviata un'operazione di backup o ripristino SMTape dal cluster 2, l'operazione di backup o ripristino non riesce e lo switchback continua.

## **Monitorare le operazioni di backup e ripristino dei volumi FlexVol**

### **Monitoraggio delle operazioni di backup e ripristino dei nastri per la panoramica dei volumi FlexVol**

È possibile visualizzare i file di registro eventi per monitorare le operazioni di backup e ripristino del nastro. ONTAP registra automaticamente eventi di backup e ripristino significativi e l'ora in cui si verificano in un file di registro denominato `backup` nel controller `/etc/log/` directory. Per impostazione predefinita, la registrazione degli eventi è impostata su `on`.

È possibile visualizzare i file di registro eventi per i seguenti motivi:

- Verifica della riuscita di un backup notturno
- Raccolta di statistiche sulle operazioni di backup
- Per utilizzare le informazioni contenute nei file di log degli eventi precedenti per diagnosticare i problemi relativi alle operazioni di backup e ripristino

Una volta alla settimana, i file di registro degli eventi vengono ruotati. Il `/etc/log/backup` il file viene rinominato in `/etc/log/backup.0`, il `/etc/log/backup.0` il file viene rinominato in `/etc/log/backup.1` e così via. Il sistema salva i file di log per un massimo di sei settimane; pertanto, è possibile disporre di un massimo di sette file di messaggi (`/etc/log/backup.[0-5]` e la corrente `/etc/log/backup` file).

### Accedere ai file di registro degli eventi

È possibile accedere ai file di registro eventi per le operazioni di backup e ripristino su nastro in `/etc/log/` directory utilizzando `rdfile` comando al nodeshell. È possibile visualizzare questi file di registro eventi per monitorare le operazioni di backup e ripristino su nastro.

#### A proposito di questa attività

Con configurazioni aggiuntive, ad esempio un ruolo di controllo degli accessi con accesso a `spi` servizio web o account utente configurato con `http` metodo di accesso, è anche possibile utilizzare un browser web per accedere a questi file di log.

#### Fasi

1. Per accedere al nodeshell, immettere il seguente comando:

```
node run -node node_name
```

`node_name` è il nome del nodo.

2. Per accedere ai file di registro eventi per le operazioni di backup e ripristino su nastro, immettere il seguente comando:

```
rdfile /etc/log/backup
```

#### Informazioni correlate

["Amministrazione del sistema"](#)

["Concetti di ONTAP"](#)

### Formato del messaggio di dump e ripristino del registro eventi

#### Panoramica del formato dei messaggi del registro eventi di dump e ripristino

Per ogni evento di dump e ripristino, viene scritto un messaggio nel file di log di backup.

Il formato del messaggio di dump e ripristino del registro eventi è il seguente:

```
type timestamp identifier event (event_info)
```

Il seguente elenco descrive i campi nel formato dei messaggi del registro eventi:

- Ogni messaggio di registro inizia con uno degli indicatori di tipo descritti nella tabella seguente:

| Tipo           | Descrizione               |
|----------------|---------------------------|
| log (registro) | Registrazione dell'evento |
| dmp            | Evento dump               |
| rst            | Evento di ripristino      |

- `timestamp` mostra la data e l'ora dell'evento.
- Il `identifier` Il campo per un evento dump include il percorso dump e l'ID univoco per il dump. Il `identifier` il campo di un evento di ripristino utilizza solo il nome del percorso di destinazione di ripristino come identificatore univoco. I messaggi di evento correlati alla registrazione non includono un `identifier` campo.

#### Quali sono gli eventi di registrazione

Il campo evento di un messaggio che inizia con un registro specifica l'inizio di una registrazione o la fine di una registrazione.

Contiene uno degli eventi mostrati nella tabella seguente:

| Evento        | Descrizione                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------|
| Start_Logging | Indica l'inizio della registrazione o che la registrazione è stata riattivata dopo essere stata disattivata. |
| Stop_Logging  | Indica che la registrazione è stata disattivata.                                                             |

#### Quali sono gli eventi di dump

Il campo dell'evento per un evento dump contiene un tipo di evento seguito da informazioni specifiche dell'evento tra parentesi.

La seguente tabella descrive gli eventi, le relative descrizioni e le relative informazioni che potrebbero essere registrate per un'operazione di dump:

| Evento              | Descrizione                                            | Informazioni sull'evento                                      |
|---------------------|--------------------------------------------------------|---------------------------------------------------------------|
| Inizio              | Viene avviato il dump NDMP                             | Livello di dump e tipo di dump                                |
| Fine                | Dump completati correttamente                          | Quantità di dati elaborati                                    |
| Interrompere        | L'operazione viene annullata                           | Quantità di dati elaborati                                    |
| Opzioni             | Vengono elencate le opzioni specificate                | Tutte le opzioni e i relativi valori, incluse le opzioni NDMP |
| TAPE_Open           | Il nastro è aperto per la lettura/scrittura            | Il nome del nuovo dispositivo a nastro                        |
| Tape_close          | Il nastro è chiuso per la lettura/scrittura            | Il nome del dispositivo a nastro                              |
| Cambiamento di fase | Un dump sta entrando in una nuova fase di elaborazione | Il nome della nuova fase                                      |

| <b>Evento</b> | <b>Descrizione</b>                                                | <b>Informazioni sull'evento</b>                                       |
|---------------|-------------------------------------------------------------------|-----------------------------------------------------------------------|
| Errore        | Si è verificato un evento imprevisto in un dump                   | Messaggio di errore                                                   |
| Snapshot      | Viene creata o individuata una copia Snapshot                     | Il nome e l'ora della copia Snapshot                                  |
| Base_dump     | È stata individuata una voce di dump di base nel metafile interno | Il livello e il tempo del dump di base (solo per i dump incrementali) |

#### **Quali sono gli eventi di ripristino**

Il campo evento per un evento di ripristino contiene un tipo di evento seguito da informazioni specifiche dell'evento tra parentesi.

La seguente tabella fornisce informazioni sugli eventi, le relative descrizioni e le relative informazioni che è possibile registrare per un'operazione di ripristino:

| <b>Evento</b>       | <b>Descrizione</b>                                           | <b>Informazioni sull'evento</b>                               |
|---------------------|--------------------------------------------------------------|---------------------------------------------------------------|
| Inizio              | Ripristino NDMP avviato                                      | Livello di ripristino e tipo di ripristino                    |
| Fine                | Ripristini completati correttamente                          | Numero di file e quantità di dati elaborati                   |
| Interrompere        | L'operazione viene annullata                                 | Numero di file e quantità di dati elaborati                   |
| Opzioni             | Vengono elencate le opzioni specificate                      | Tutte le opzioni e i relativi valori, incluse le opzioni NDMP |
| TAPE_Open           | Il nastro è aperto per la lettura/scrittura                  | Il nome del nuovo dispositivo a nastro                        |
| Tape_close          | Il nastro è chiuso per la lettura/scrittura                  | Il nome del dispositivo a nastro                              |
| Cambiamento di fase | Il ripristino sta entrando in una nuova fase di elaborazione | Il nome della nuova fase                                      |
| Errore              | Il ripristino rileva un evento imprevisto                    | Messaggio di errore                                           |

#### **Attivazione o disattivazione della registrazione degli eventi**

È possibile attivare o disattivare la registrazione degli eventi.

## Fasi

1. Per attivare o disattivare la registrazione degli eventi, immettere il seguente comando nella shell del cluster:

```
options -option_name backup.log.enable -option-value {on | off}
```

`on` attiva la registrazione degli eventi.

`off` disattiva la disconnessione degli eventi.



La registrazione degli eventi è attivata per impostazione predefinita.

## Messaggi di errore per il backup su nastro e il ripristino dei volumi FlexVol

### Messaggi di errore relativi al backup e al ripristino

#### Limitazione delle risorse: Nessun thread disponibile

- **Messaggio**

```
Resource limitation: no available thread
```

- **Causa**

Il numero massimo di thread i/o locali su nastro attivi è attualmente in uso. È possibile disporre di un massimo di 16 unità a nastro locali attive.

- **Azione correttiva**

Attendere il completamento di alcuni processi su nastro prima di avviare un nuovo processo di backup o ripristino.

#### Prenotazione del nastro anticipata

- **Messaggio**

```
Tape reservation preempted
```

- **Causa**

L'unità a nastro è in uso da un'altra operazione o il nastro è stato chiuso prematuramente.

- **Azione correttiva**

Assicurarsi che l'unità a nastro non venga utilizzata da un'altra operazione e che l'applicazione DMA non abbia interrotto il processo, quindi riprovare.

#### Impossibile inizializzare il supporto

- **Messaggio**

```
Could not initialize media
```



- **Causa**

Questo errore potrebbe verificarsi per uno dei seguenti motivi:

- L'unità a nastro utilizzata per il backup è danneggiata o danneggiata.
- Il nastro non contiene il backup completo o è corrotto.
- Il numero massimo di thread i/o locali su nastro attivi è attualmente in uso.

È possibile disporre di un massimo di 16 unità a nastro locali attive.

- **Azione correttiva**

- Se l'unità a nastro è danneggiata o danneggiata, riprovare a eseguire l'operazione con un'unità a nastro valida.
- Se il nastro non contiene il backup completo o è corrotto, non è possibile eseguire l'operazione di ripristino.
- Se le risorse su nastro non sono disponibili, attendere il completamento di alcuni processi di backup o ripristino, quindi riprovare l'operazione.

#### **Numero massimo di dump o ripristini consentiti (limite massimo di sessione) in corso**

- **Messaggio**

Maximum number of allowed dumps or restores (*maximum session limit*) in progress

- **Causa**

Il numero massimo di processi di backup o ripristino è già in esecuzione.

- **Azione correttiva**

Riprovare l'operazione al termine di alcuni dei lavori attualmente in esecuzione.

#### **Errore di supporto in scrittura su nastro**

- **Messaggio**

Media error on tape write

- **Causa**

Il nastro utilizzato per il backup è danneggiato.

- **Azione correttiva**

Sostituire il nastro e riprovare a eseguire il processo di backup.

#### **Scrittura del nastro non riuscita**

- **Messaggio**

Tape write failed

- **Causa**

Il nastro utilizzato per il backup è danneggiato.

- **Azione correttiva**

Sostituire il nastro e riprovare a eseguire il processo di backup.

#### **Scrittura nastro non riuscita - il nuovo nastro ha rilevato un errore di supporto**

- **Messaggio**

Tape write failed - new tape encountered media error

- **Causa**

Il nastro utilizzato per il backup è danneggiato.

- **Azione correttiva**

Sostituire il nastro e riprovare a eseguire il backup.

#### **Scrittura nastro non riuscita - il nuovo nastro è rotto o protetto da scrittura**

- **Messaggio**

Tape write failed - new tape is broken or write protected

- **Causa**

Il nastro utilizzato per il backup è corrotto o protetto da scrittura.

- **Azione correttiva**

Sostituire il nastro e riprovare a eseguire il backup.

#### **Scrittura nastro non riuscita - il nuovo nastro è già alla fine del supporto**

- **Messaggio**

Tape write failed - new tape is already at the end of media

- **Causa**

Spazio sul nastro insufficiente per completare il backup.

- **Azione correttiva**

Sostituire il nastro e riprovare a eseguire il backup.

#### **Errore di scrittura del nastro**

- **Messaggio**

Tape write error - The previous tape had less than the required minimum capacity, size MB, for this tape operation, The operation should be restarted from the beginning

- **Causa**

La capacità del nastro non è sufficiente per contenere i dati di backup.

- **Azione correttiva**

Utilizzare nastri con capacità maggiore e riprovare a eseguire il processo di backup.

#### **Errore di lettura del supporto su nastro**

- **Messaggio**

Media error on tape read

- **Causa**

Il nastro da cui vengono ripristinati i dati è corrotto e potrebbe non contenere i dati di backup completi.

- **Azione correttiva**

Se si è certi che il nastro disponga del backup completo, riprovare l'operazione di ripristino. Se il nastro non contiene il backup completo, non è possibile eseguire l'operazione di ripristino.

#### **Errore di lettura del nastro**

- **Messaggio**

Tape read error

- **Causa**

L'unità a nastro è danneggiata o il nastro non contiene il backup completo.

- **Azione correttiva**

Se l'unità a nastro è danneggiata, utilizzare un'altra unità a nastro. Se il nastro non contiene il backup completo, non è possibile ripristinare i dati.

#### **Già alla fine del nastro**

- **Messaggio**

Already at the end of tape

- **Causa**

Il nastro non contiene dati o deve essere riavvolto.

- **Azione correttiva**

Se il nastro non contiene dati, utilizzare il nastro che contiene il backup e riprovare a eseguire il processo di ripristino. In caso contrario, riavvolgere il nastro e riprovare a eseguire il processo di ripristino.

**La dimensione del record del nastro è troppo piccola. Provare a utilizzare un formato più grande.**

- **Messaggio**

`Tape record size is too small. Try a larger size.`

- **Causa**

Il fattore di blocco specificato per l'operazione di ripristino è inferiore al fattore di blocco utilizzato durante il backup.

- **Azione correttiva**

Utilizzare lo stesso fattore di blocco specificato durante il backup.

**La dimensione del record del nastro deve essere block\_size1 e non block\_size2**

- **Messaggio**

`Tape record size should be block_size1 and not block_size2`

- **Causa**

Il fattore di blocco specificato per il ripristino locale non è corretto.

- **Azione correttiva**

Riprovare a eseguire il processo di ripristino con `block_size1` come fattore di blocco.

**La dimensione del record del nastro deve essere compresa tra 4 KB e 256 KB**

- **Messaggio**

`Tape record size must be in the range between 4KB and 256KB`

- **Causa**

Il fattore di blocco specificato per l'operazione di backup o ripristino non rientra nell'intervallo consentito.

- **Azione correttiva**

Specificare un fattore di blocco compreso tra 4 KB e 256 KB.

## **Messaggi di errore NDMP**

### **Errore di comunicazione di rete**

- **Messaggio**

`Network communication error`

- **Causa**

La comunicazione con un nastro remoto in una connessione NDMP a tre vie non è riuscita.

- **Azione correttiva**

Verificare la connessione di rete al telecomando.

#### **Messaggio da Read Socket: Error\_string**

- **Messaggio**

Message from Read Socket: error\_string

- **Causa**

Ripristinare la comunicazione dal nastro remoto nella connessione NDMP a 3 vie con errori.

- **Azione correttiva**

Verificare la connessione di rete al telecomando.

#### **Messaggio da Write Dirnet: Error\_string**

- **Messaggio**

Message from Write Dirnet: error\_string

- **Causa**

Si è verificato un errore nella comunicazione di backup con un nastro remoto in una connessione NDMP a tre vie.

- **Azione correttiva**

Verificare la connessione di rete al telecomando.

#### **Read Socket Received EOF**

- **Messaggio**

Read Socket received EOF

- **Causa**

Il tentativo di comunicare con un nastro remoto in una connessione NDMP a tre vie ha raggiunto la fine del contrassegno file. Potrebbe essere in corso un ripristino a tre direzioni da un'immagine di backup con un blocco di dimensioni maggiori.

- **Azione correttiva**

Specificare la dimensione del blocco corretta e riprovare l'operazione di ripristino.

ndmpd numero di versione non valido: numero\_versione ``

- **Messaggio**

ndmpd invalid version number: version\_number

- **Causa**

La versione NDMP specificata non è supportata dal sistema di storage.

- **Azione correttiva**

Specificare la versione 4 di NDMP.

ID\_sessione ndmpd non attivo

- **Messaggio**

ndmpd session session\_ID not active

- **Causa**

La sessione NDMP potrebbe non esistere.

- **Azione correttiva**

Utilizzare `ndmpd status` Per visualizzare le sessioni NDMP attive.

Impossibile ottenere vol Ref per Volume volume\_name

- **Messaggio**

Could not obtain vol ref for Volume vol\_name

- **Causa**

Impossibile ottenere il riferimento del volume perché il volume potrebbe essere utilizzato da altre operazioni.

- **Azione correttiva**

Riprovare l'operazione in un secondo momento.

Tipo di connessione dati ["NDMP4\_ADDR\_TCP"|"NDMP4\_ADDR\_TCP\_IPv6"] non supportato per le connessioni di controllo ["IPv6"|"IPv4"]

- **Messaggio**

Data connection type ["NDMP4\_ADDR\_TCP"|"NDMP4\_ADDR\_TCP\_IPv6"] not supported for ["IPv6"|"IPv4"] control connections

- **Causa**

In modalità NDMP con ambito nodo, la connessione dati NDMP stabilita deve essere dello stesso tipo di

indirizzo di rete (IPv4 o IPv6) della connessione di controllo NDMP.

- **Azione correttiva**

Contattare il fornitore dell'applicazione di backup.

#### **DATA LISTEN (ASCOLTO DATI): Errore di preconditione di preparazione della connessione dati CAB**

- **Messaggio**

DATA LISTEN: CAB data connection prepare precondition error

- **Causa**

L'ascolto dei dati NDMP non riesce quando l'applicazione di backup ha negoziato l'estensione CAB con il server NDMP e c'è una mancata corrispondenza nel tipo di indirizzo di connessione dati NDMP specificato tra i messaggi NDMP\_CAB\_DATA\_CONN\_PREPARE e NDMP\_DATA\_LISTEN.

- **Azione correttiva**

Contattare il fornitore dell'applicazione di backup.

#### **DATA CONNECT: Errore di preconditione di preparazione della connessione dati CAB**

- **Messaggio**

DATA CONNECT: CAB data connection prepare precondition error

- **Causa**

La connessione dati NDMP non riesce quando l'applicazione di backup ha negoziato l'estensione CAB con il server NDMP e c'è una mancata corrispondenza nel tipo di indirizzo di connessione dati NDMP specificato tra i messaggi NDMP\_CAB\_DATA\_CONN\_PREPARE e NDMP\_DATA\_CONNECT.

- **Azione correttiva**

Contattare il fornitore dell'applicazione di backup.

#### **Errore:show failed: Impossibile ottenere la password per l'utente '<username>'**

- **Messaggio**

Error: show failed: Cannot get password for user '<username>'

- **Causa**

Configurazione dell'account utente incompleta per NDMP

- **Azione correttiva**

Assicurarsi che l'account utente sia associato al metodo di accesso SSH e che il metodo di autenticazione sia la password utente.

## Messaggi di errore di dump

### Il volume di destinazione è di sola lettura

- **Messaggio**

`Destination volume is read-only`

- **Causa**

Il percorso verso il quale si tenta di eseguire l'operazione di ripristino è di sola lettura.

- **Azione correttiva**

Provare a ripristinare i dati in un'altra posizione.

### Il qtree di destinazione è di sola lettura

- **Messaggio**

`Destination qtree is read-only`

- **Causa**

Il qtree su cui si tenta di eseguire il ripristino è di sola lettura.

- **Azione correttiva**

Provare a ripristinare i dati in un'altra posizione.

### Dump temporaneamente disattivati sul volume, riprovare

- **Messaggio**

`Dumps temporarily disabled on volume, try again`

- **Causa**

Il backup dump NDMP viene tentato su un volume di destinazione SnapMirror che fa parte di uno dei due `snapmirror break` oppure un `snapmirror resync` operazione.

- **Azione correttiva**

Attendere il `snapmirror break` oppure `snapmirror resync` operazione per terminare e quindi eseguire l'operazione di dump.



Ogni volta che lo stato di un volume di destinazione SnapMirror cambia da lettura/scrittura a sola lettura o da sola lettura a lettura/scrittura, è necessario eseguire un backup di riferimento.

### Etichette NFS non riconosciute

- **Messaggio**



Error: Aborting: dump encountered NFS security labels in the file system

- **Causa**

Le etichette di sicurezza NFS sono supportate a partire da ONTAP 9.9.1 quando NFSv4.2 è attivato. Tuttavia, le etichette di sicurezza NFS non sono attualmente riconosciute dal motore di dump. Se incontra etichette di sicurezza NFS su file, directory o qualsiasi file speciale in qualsiasi formato di dump, il dump non riesce.

- **Azione correttiva**

Verificare che nessun file o directory abbia etichette di sicurezza NFS.

#### Nessun file creato

- **Messaggio**

No files were created

- **Causa**

È stato tentato un DAR di directory senza abilitare la funzionalità DAR avanzata.

- **Azione correttiva**

Abilitare la funzionalità DAR avanzata e riprovare a eseguire il DAR.

#### Ripristino del file <file name> non riuscito

- **Messaggio**

Restore of the file file name failed

- **Causa**

Quando viene eseguito un DAR (Direct Access Recovery) di un file il cui nome file è uguale a quello di un LUN sul volume di destinazione, il DAR non riesce.

- **Azione correttiva**

Riprovare DAR del file.

#### Troncamento non riuscito per src inode <inode number>...

- **Messaggio**

Truncation failed for src inode <inode number>. Error <error number>. Skipping inode.

- **Causa**

L'inode di un file viene cancellato quando il file viene ripristinato.

- **Azione correttiva**

Prima di utilizzare il volume, attendere il completamento dell'operazione di ripristino su un volume.

#### Impossibile bloccare uno snapshot richiesto dal dump

- **Messaggio**

Unable to lock a snapshot needed by dump

- **Causa**

La copia Snapshot specificata per il backup non è disponibile.

- **Azione correttiva**

Riprovare a eseguire il backup con una copia Snapshot diversa.

Utilizzare `snap list` Per visualizzare l'elenco delle copie Snapshot disponibili.

#### Impossibile individuare i file bitmap

- **Messaggio**

Unable to locate bitmap files

- **Causa**

I file bitmap richiesti per l'operazione di backup potrebbero essere stati cancellati. In questo caso, il backup non può essere riavviato.

- **Azione correttiva**

Eseguire nuovamente il backup.

#### Il volume si trova temporaneamente in uno stato transitorio

- **Messaggio**

Volume is temporarily in a transitional state

- **Causa**

Il volume di cui viene eseguito il backup si trova temporaneamente in uno stato non montato.

- **Azione correttiva**

Attendere qualche istante ed eseguire di nuovo il backup.

#### Messaggi di errore SMTape

##### Blocchi fuori servizio

- **Messaggio**

Chunks out of order

- **Causa**

I nastri di backup non vengono ripristinati nella sequenza corretta.

- **Azione correttiva**

Ripetere l'operazione di ripristino e caricare i nastri nella sequenza corretta.

#### **Formato chunk non supportato**

- **Messaggio**

Chunk format not supported

- **Causa**

L'immagine di backup non è di SMTape.

- **Azione correttiva**

Se l'immagine di backup non è SMTape, riprovare l'operazione con un nastro che dispone del backup SMTape.

#### **Impossibile allocare la memoria**

- **Messaggio**

Failed to allocate memory

- **Causa**

La memoria del sistema è esaurita.

- **Azione correttiva**

Riprovare a eseguire il processo in un secondo momento quando il sistema non è troppo occupato.

#### **Impossibile ottenere il buffer dei dati**

- **Messaggio**

Failed to get data buffer

- **Causa**

Il sistema storage ha esaurito i buffer.

- **Azione correttiva**

Attendere il completamento di alcune operazioni del sistema di storage, quindi riprovare a eseguire il processo.

#### Impossibile trovare l'istantanea

- **Messaggio**

Failed to find snapshot

- **Causa**

La copia Snapshot specificata per il backup non è disponibile.

- **Azione correttiva**

Controllare se la copia Snapshot specificata è disponibile. In caso contrario, riprovare con la copia Snapshot corretta.

#### Impossibile creare lo snapshot

- **Messaggio**

Failed to create snapshot

- **Causa**

Il volume contiene già il numero massimo di copie Snapshot.

- **Azione correttiva**

Eliminare alcune copie Snapshot, quindi riprovare l'operazione di backup.

#### Impossibile bloccare snapshot

- **Messaggio**

Failed to lock snapshot

- **Causa**

La copia Snapshot è in uso o è stata eliminata.

- **Azione correttiva**

Se la copia Snapshot viene utilizzata da un'altra operazione, attendere il completamento dell'operazione, quindi riprovare a eseguire il backup. Se la copia Snapshot è stata eliminata, non è possibile eseguire il backup.

#### Impossibile eliminare lo snapshot

- **Messaggio**

Failed to delete snapshot

- **Causa**

Impossibile eliminare la copia Snapshot automatica perché è in uso da altre operazioni.

- **Azione correttiva**

Utilizzare `snap` Per determinare lo stato della copia Snapshot. Se la copia Snapshot non è necessaria, eliminarla manualmente.

#### Impossibile ottenere l'ultimo snapshot

- **Messaggio**

Failed to get latest snapshot

- **Causa**

La copia Snapshot più recente potrebbe non esistere perché il volume viene inizializzato da SnapMirror.

- **Azione correttiva**

Riprovare al termine dell'inizializzazione.

#### Impossibile caricare il nuovo nastro

- **Messaggio**

Failed to load new tape

- **Causa**

Errore nell'unità a nastro o nel supporto.

- **Azione correttiva**

Sostituire il nastro e riprovare l'operazione.

#### Impossibile inizializzare il nastro

- **Messaggio**

Failed to initialize tape

- **Causa**

Questo messaggio di errore potrebbe essere visualizzato per uno dei seguenti motivi:

- L'immagine di backup non è di SMTape.
- Il fattore di blocco del nastro specificato non è corretto.
- Il nastro è corrotto o danneggiato.
- Viene caricato il nastro errato per il ripristino.

- **Azione correttiva**

- Se l'immagine di backup non è SMTape, riprovare l'operazione con un nastro che dispone di backup SMTape.
- Se il fattore di blocco non è corretto, specificare il fattore di blocco corretto e riprovare l'operazione.

- Se il nastro è corrotto, non è possibile eseguire l'operazione di ripristino.
- Se viene caricato il nastro errato, riprovare l'operazione con il nastro corretto.

#### **Impossibile inizializzare il flusso di ripristino**

##### **• Messaggio**

`Failed to initialize restore stream`

##### **• Causa**

Questo messaggio di errore potrebbe essere visualizzato per uno dei seguenti motivi:

- L'immagine di backup non è di SMTape.
- Il fattore di blocco del nastro specificato non è corretto.
- Il nastro è corrotto o danneggiato.
- Viene caricato il nastro errato per il ripristino.

##### **• Azione correttiva**

- Se l'immagine di backup non è SMTape, riprovare l'operazione con un nastro che dispone del backup SMTape.
- Se il fattore di blocco non è corretto, specificare il fattore di blocco corretto e riprovare l'operazione.
- Se il nastro è corrotto, non è possibile eseguire l'operazione di ripristino.
- Se viene caricato il nastro errato, riprovare l'operazione con il nastro corretto.

#### **Impossibile leggere l'immagine di backup**

##### **• Messaggio**

`Failed to read backup image`

##### **• Causa**

Il nastro è corrotto.

##### **• Azione correttiva**

Se il nastro è corrotto, non è possibile eseguire l'operazione di ripristino.

#### **Intestazione immagine mancante o danneggiata**

##### **• Messaggio**

`Image header missing or corrupted`

##### **• Causa**

Il nastro non contiene un backup SMTape valido.

##### **• Azione correttiva**

Riprovare con un nastro contenente un backup valido.

#### Asserzione interna

- **Messaggio**

Internal assertion

- **Causa**

Si è verificato un errore interno SMTape.

- **Azione correttiva**

Notificare l'errore e inviare il `etc/log/backup` file al supporto tecnico.

#### Numero magico dell'immagine di backup non valido

- **Messaggio**

Invalid backup image magic number

- **Causa**

L'immagine di backup non è di SMTape.

- **Azione correttiva**

Se l'immagine di backup non è SMTape, riprovare l'operazione con un nastro che dispone del backup SMTape.

#### Checksum immagine di backup non valido

- **Messaggio**

Invalid backup image checksum

- **Causa**

Il nastro è corrotto.

- **Azione correttiva**

Se il nastro è corrotto, non è possibile eseguire l'operazione di ripristino.

#### Nastro di input non valido

- **Messaggio**

Invalid input tape

- **Causa**

La firma dell'immagine di backup non è valida nell'intestazione del nastro. Il nastro presenta dati corrotti o non contiene un'immagine di backup valida.

- **Azione correttiva**

Riprovare a eseguire il processo di ripristino con un'immagine di backup valida.

#### **Percorso del volume non valido**

- **Messaggio**

`Invalid volume path`

- **Causa**

Il volume specificato per l'operazione di backup o ripristino non viene trovato.

- **Azione correttiva**

Riprovare a eseguire il processo con un percorso del volume e un nome del volume validi.

#### **Mancata corrispondenza nell'ID set di backup**

- **Messaggio**

`Mismatch in backup set ID`

- **Causa**

Il nastro caricato durante una sostituzione del nastro non fa parte del set di backup.

- **Azione correttiva**

Caricare il nastro corretto e riprovare a eseguire il processo.

#### **Mancata corrispondenza nell'indicatore di data e ora del backup**

- **Messaggio**

`Mismatch in backup time stamp`

- **Causa**

Il nastro caricato durante una sostituzione del nastro non fa parte del set di backup.

- **Azione correttiva**

Utilizzare `smtape restore -h` comando per verificare le informazioni di intestazione di un nastro.

#### **Processo interrotto a causa dell'arresto**

- **Messaggio**

`Job aborted due to shutdown`

- **Causa**



Riavvio del sistema storage in corso.

- **Azione correttiva**

Riprovare a eseguire il processo dopo il riavvio del sistema di storage.

#### **Processo interrotto a causa dell'eliminazione automatica di Snapshot**

- **Messaggio**

Job aborted due to Snapshot autodelete

- **Causa**

Il volume non dispone di spazio sufficiente e ha attivato l'eliminazione automatica delle copie Snapshot.

- **Azione correttiva**

Liberare spazio nel volume e riprovare a eseguire il processo.

#### **Il nastro è attualmente in uso da altre operazioni**

- **Messaggio**

Tape is currently in use by other operations

- **Causa**

L'unità a nastro è in uso da un altro lavoro.

- **Azione correttiva**

Riprovare a eseguire il backup al termine del processo attualmente attivo.

#### **Nastri fuori servizio**

- **Messaggio**

Tapes out of order

- **Causa**

Il primo nastro della sequenza di nastri per l'operazione di ripristino non ha l'intestazione dell'immagine.

- **Azione correttiva**

Caricare il nastro con l'intestazione dell'immagine e riprovare a eseguire il processo.

#### **Trasferimento non riuscito (interrotto a causa di un'operazione MetroCluster)**

- **Messaggio**

Transfer failed (Aborted due to MetroCluster operation)

- **Causa**

L'operazione SMTape viene interrotta a causa di un'operazione di switchover o switchback.

- **Azione correttiva**

Eseguire l'operazione SMTape al termine dell'operazione di switchover o switchback.

#### **Trasferimento non riuscito (interruzione avviata da ARL)**

- **Messaggio**

`Transfer failed (ARL initiated abort)`

- **Causa**

Mentre è in corso un'operazione SMTape se viene avviato un trasferimento di aggregato, l'operazione SMTape viene interrotta.

- **Azione correttiva**

Eseguire l'operazione SMTape al termine dell'operazione di trasferimento degli aggregati.

#### **Trasferimento non riuscito (interruzione avviata da CFO)**

- **Messaggio**

`Transfer failed (CFO initiated abort)`

- **Causa**

L'operazione SMTape viene interrotta a causa di un'operazione di failover dello storage (Takeover e giveback) di un aggregato CFO.

- **Azione correttiva**

Eseguire l'operazione SMTape al termine del failover dello storage dell'aggregato CFO.

#### **Trasferimento non riuscito (interruzione avviata da SFO)**

- **Messaggio**

`Transfer failed (SFO initiated abort)`

- **Causa**

L'operazione SMTape viene interrotta a causa di un'operazione di failover dello storage (Takeover e giveback).

- **Azione correttiva**

Eseguire l'operazione SMTape al termine dell'operazione di failover dello storage (Takeover e giveback).

#### Aggregato sottostante in fase di migrazione

- **Messaggio**

Underlying aggregate under migration

- **Causa**

Se viene avviata un'operazione SMTape su un aggregato in fase di migrazione (failover dello storage o riposizionamento dell'aggregato), l'operazione SMTape non riesce.

- **Azione correttiva**

Eseguire l'operazione SMTape al termine della migrazione aggregata.

#### Il volume è attualmente in fase di migrazione

- **Messaggio**

Volume is currently under migration

- **Causa**

La migrazione dei volumi e il backup SMTape non possono essere eseguiti contemporaneamente.

- **Azione correttiva**

Riprovare a eseguire il processo di backup al termine della migrazione del volume.

#### Volume offline

- **Messaggio**

Volume offline

- **Causa**

Il volume di cui viene eseguito il backup non è in linea.

- **Azione correttiva**

Portare il volume online e riprovare il backup.

#### Volume non limitato

- **Messaggio**

Volume not restricted

- **Causa**

Il volume di destinazione in cui vengono ripristinati i dati non è limitato.

- **Azione correttiva**

Limitare il volume e riprovare l'operazione di ripristino.

## Configurazione NDMP

### Panoramica della configurazione NDMP

È possibile configurare rapidamente un cluster ONTAP 9 in modo che utilizzi il protocollo di gestione dei dati di rete (NDMP) per eseguire il backup dei dati direttamente su nastro utilizzando un'applicazione di backup di terze parti.

Se l'applicazione di backup supporta Cluster Aware Backup (CAB), è possibile configurare NDMP come *SVM-scoped* o *node-scoped*:

- SVM-scope a livello di cluster (admin SVM) consente di eseguire il backup di tutti i volumi ospitati su diversi nodi del cluster. Se possibile, si consiglia di utilizzare NDMP con ambito SVM.
- NDMP con ambito nodo consente di eseguire il backup di tutti i volumi ospitati su quel nodo.

Se l'applicazione di backup non supporta CAB, è necessario utilizzare NDMP con ambito nodo.

Gli NDMP con ambito SVM e nodo si escludono a vicenda e non possono essere configurati sullo stesso cluster.



NDMP con ambito del nodo è obsoleto in ONTAP 9.

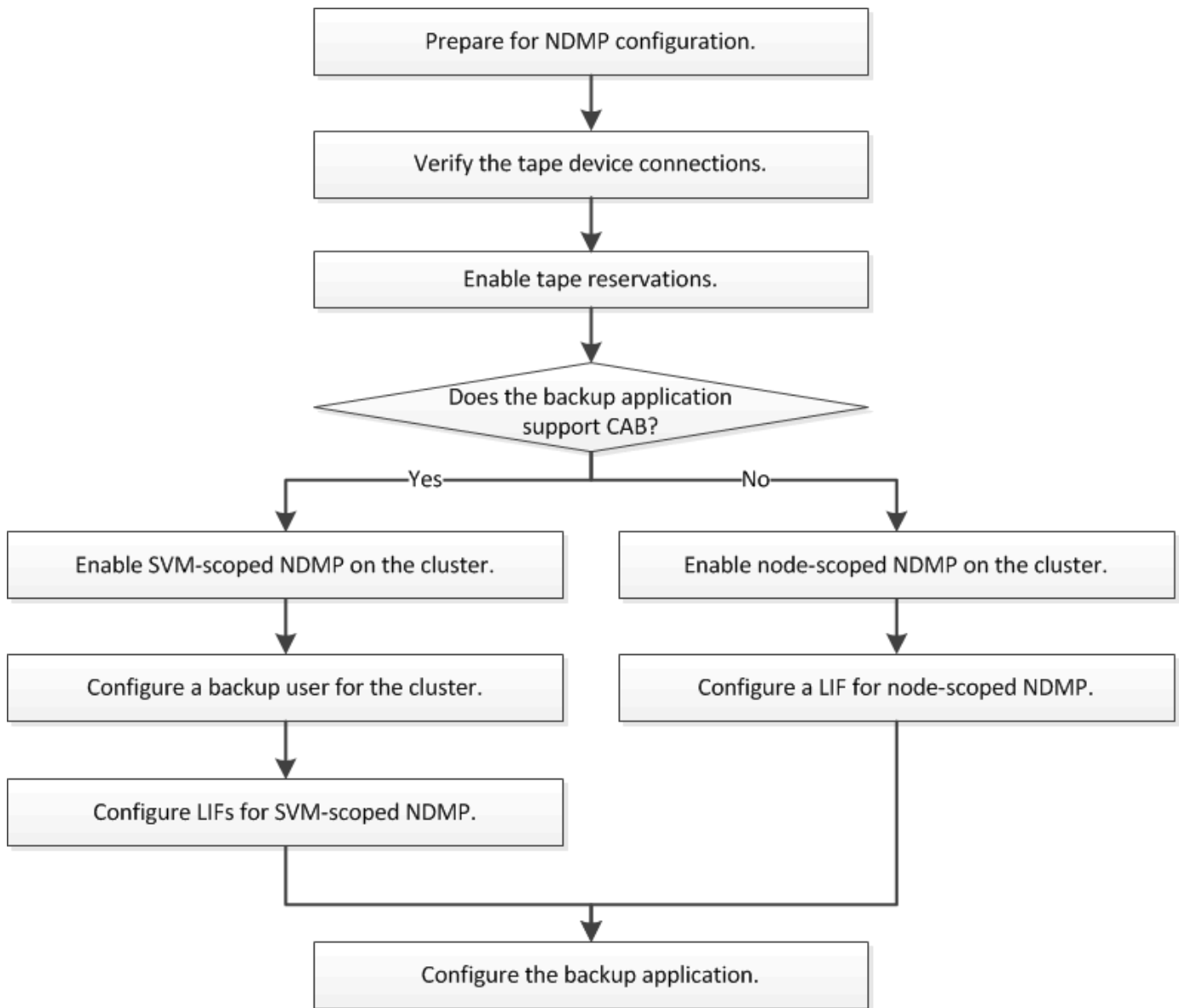
Scopri di più ["Backup cluster-aware \(CAB\)"](#).

Prima di configurare NDMP, verificare quanto segue:

- Si dispone di un'applicazione di backup di terze parti (chiamata anche Data Management Application o DMA).
- Sei un amministratore del cluster.
- Sono installati i dispositivi a nastro e un server multimediale opzionale.
- I dispositivi a nastro sono collegati al cluster tramite uno switch Fibre Channel (FC) e non direttamente.
- Almeno un dispositivo a nastro ha un numero di unità logica (LUN) pari a 0.

### Workflow di configurazione NDMP

L'impostazione del backup su nastro su NDMP richiede la preparazione della configurazione NDMP, la verifica delle connessioni dei dispositivi a nastro, l'attivazione delle prenotazioni su nastro, la configurazione di NDMP a livello di SVM o di nodo, l'abilitazione di NDMP sul cluster, la configurazione di un utente di backup, la configurazione di LIF e la configurazione dell'applicazione di backup.



## Preparazione per la configurazione NDMP

Prima di configurare l'accesso al backup su nastro tramite NDMP (Network Data Management Protocol), è necessario verificare che la configurazione pianificata sia supportata, verificare che le unità a nastro siano elencate come unità qualificate su ciascun nodo, verificare che tutti i nodi dispongano di LIF intercluster, E identificare se l'applicazione di backup supporta l'estensione CAB (Cluster Aware Backup).

### Fasi

1. Fare riferimento alla matrice di compatibilità del provider di applicazioni di backup per il supporto ONTAP (NetApp non qualifica le applicazioni di backup di terze parti con ONTAP o NDMP).

Verificare che i seguenti componenti NetApp siano compatibili:

- La versione di ONTAP 9 in esecuzione sul cluster.
- Il vendor e la versione dell'applicazione di backup: Ad esempio, Veritas NetBackup 8.2 o CommVault.

- I dettagli dei dispositivi a nastro, come il produttore, il modello e l'interfaccia delle unità a nastro, ad esempio IBM Ultrium 8 o HPE StoreEver Ultrium 30750 LTO-8.
- Le piattaforme dei nodi nel cluster, ad esempio FAS8700 o A400.



Le matrici di supporto per la compatibilità ONTAP legacy per le applicazioni di backup sono disponibili in ["Tool di matrice di interoperabilità NetApp"](#).

2. Verificare che le unità a nastro siano elencate come unità qualificate nel file di configurazione del nastro integrato di ciascun nodo:

- a. Nell'interfaccia della riga di comando, visualizzare il file di configurazione del nastro integrato utilizzando `storage tape show-supported-status` comando.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1

Tape Drives                                Is
-----                                -
Certance Ultrium 2                        true      Dynamically Qualified
Certance Ultrium 3                        true      Dynamically Qualified
Digital DLT2000                          true      Qualified
```

- b. Confrontare le unità a nastro con l'elenco delle unità qualificate nell'output.



I nomi dei dispositivi a nastro nell'output potrebbero variare leggermente rispetto ai nomi sull'etichetta del dispositivo o nella matrice di interoperabilità. Ad esempio, Digital DLT2000 può anche essere noto come DLT2k. È possibile ignorare queste differenze di denominazione minori.

- c. Se un dispositivo non è elencato come qualificato nell'output anche se il dispositivo è qualificato secondo la matrice di interoperabilità, scaricare e installare un file di configurazione aggiornato per il dispositivo utilizzando le istruzioni sul sito del supporto NetApp.

["Download NetApp: File di configurazione dei dispositivi su nastro"](#)

Un dispositivo qualificato potrebbe non essere elencato nel file di configurazione del nastro integrato se il dispositivo a nastro è stato qualificato dopo la spedizione del nodo.

3. Verificare che ogni nodo del cluster disponga di una LIF intercluster:

- a. Visualizzare le LIF di intercluster sui nodi utilizzando `network interface show -role intercluster` comando.

```
cluster1::> network interface show -role intercluster
```

|            | Logical   | Status     | Network       | Current    |
|------------|-----------|------------|---------------|------------|
| Current Is |           |            |               |            |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       |
| Port       | Home      |            |               |            |
| -----      | -----     | -----      | -----         | -----      |
| -----      | -----     | -----      | -----         | -----      |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 |
| e0a        | true      |            |               |            |

- b. Se non esiste una LIF di intercluster su un nodo, creare una LIF di intercluster utilizzando `network interface create` comando.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster
```

```
cluster1::> network interface show -role intercluster
```

|            | Logical   | Status     | Network       | Current    |
|------------|-----------|------------|---------------|------------|
| Current Is |           |            |               |            |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       |
| Port       | Home      |            |               |            |
| -----      | -----     | -----      | -----         | -----      |
| -----      | -----     | -----      | -----         | -----      |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 |
| e0a        | true      |            |               |            |
| cluster1   | IC2       | up/up      | 192.0.2.68/24 | cluster1-2 |
| e0b        | true      |            |               |            |

### "Gestione della rete"

- Identificare se l'applicazione di backup supporta Cluster Aware Backup (CAB) utilizzando la documentazione fornita con l'applicazione di backup.

Il supporto CAB è un fattore chiave per determinare il tipo di backup che è possibile eseguire.

## Verificare le connessioni del dispositivo a nastro

Assicurarsi che tutti i dischi e i media changer siano visibili in ONTAP come dispositivi.

Fasi

- 1. Visualizzare le informazioni su tutti i dischi e i media changer utilizzando storage tape show comando.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID           Device Type      Description
Status
-----
sw4:10.11           tape drive      HP LTO-3
normal
0b.125L1            media changer   HP MSL G3 Series
normal
0d.4                tape drive      IBM LTO 5 ULT3580
normal
0d.4L1              media changer   IBM 3573-TL
normal
...
```

- 2. Se non viene visualizzata un'unità a nastro, risolvere il problema.
- 3. Se non viene visualizzato un media changer, visualizzare le informazioni sui media changer utilizzando storage tape show-media-changer e risolvere il problema.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
    WWNN: 2:00a:000e11:10b919
    WWPN: 2:00b:000e11:10b919
  Serial Number: 00FRU7800000_LL1

  Errors: -

Paths:
Node           Initiator  Alias    Device State
Status
-----
cluster1-01    2b        mc0      in-use
normal
...
```



## Attivare le prenotazioni su nastro

È necessario assicurarsi che le unità a nastro siano riservate all'utilizzo da parte delle applicazioni di backup per le operazioni di backup NDMP.

### A proposito di questa attività

Le impostazioni di prenotazione variano in diverse applicazioni di backup e devono corrispondere all'applicazione di backup e ai nodi o ai server che utilizzano gli stessi dischi. Consultare la documentazione del fornitore dell'applicazione di backup per le impostazioni di prenotazione corrette.

### Fasi

1. Attivare le prenotazioni utilizzando `options -option-name tape.reservations -option-value persistent` comando.

Il seguente comando consente di attivare le prenotazioni con `persistent` valore:

```
cluster1::> options -option-name tape.reservations -option-value
persistent
2 entries were modified.
```

2. Verificare che le prenotazioni siano attivate su tutti i nodi utilizzando `options tape.reservations` e quindi esaminare l'output.

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                persistent

cluster1-2
    tape.reservations                persistent
2 entries were displayed.
```

## Configurare NDMP con ambito SVM

### Abilitare NDMP con ambito SVM sul cluster

Se il DMA supporta l'estensione CAB (Cluster Aware Backup), è possibile eseguire il backup di tutti i volumi ospitati su diversi nodi di un cluster attivando NDMP con ambito SVM, attivando il servizio NDMP sul cluster (SVM amministrativa) e configurando i LIF per la connessione dati e di controllo.

### Di cosa hai bisogno

L'estensione DELLA CABINA deve essere supportata dal DMA.

### A proposito di questa attività

La disattivazione della modalità NDMP con ambito nodo attiva la modalità NDMP con ambito SVM sul cluster.

## Fasi

1. Abilita la modalità NDMP SVM-scoped:

```
cluster1::> system services ndmp node-scope-mode off
```

La modalità NDMP SVM-scoped è abilitata.

2. Attivare il servizio NDMP sulla SVM di amministrazione:

```
cluster1::> vserver services ndmp on -vserver cluster1
```

Il tipo di autenticazione è impostato su `challenge` per impostazione predefinita, l'autenticazione in chiaro è disattivata.



Per una comunicazione sicura, è necessario disattivare l'autenticazione in chiaro.

3. Verificare che il servizio NDMP sia abilitato:

```
cluster1::> vserver services ndmp show
```

| Vserver  | Enabled | Authentication type |
|----------|---------|---------------------|
| -----    | -----   | -----               |
| cluster1 | true    | challenge           |
| vs1      | false   | challenge           |

## Abilitare un utente di backup per l'autenticazione NDMP

Per autenticare NDMP con ambito SVM dall'applicazione di backup, è necessario disporre di un utente amministrativo con privilegi sufficienti e di una password NDMP.

### A proposito di questa attività

È necessario generare una password NDMP per gli utenti amministratori del backup. È possibile abilitare gli utenti amministratori di backup a livello di cluster o SVM e, se necessario, creare un nuovo utente. Per impostazione predefinita, gli utenti con i seguenti ruoli possono eseguire l'autenticazione per il backup NDMP:

- A livello di cluster: `admin` oppure `backup`
- SVM individuali: `vsadmin` oppure `vsadmin-backup`

Se si utilizza un utente NIS o LDAP, l'utente deve esistere sul rispettivo server. Non è possibile utilizzare un utente Active Directory.

## Fasi

1. Visualizza gli utenti e i permessi di amministrazione correnti:

```
security login show
```

2. Se necessario, creare un nuovo utente di backup NDMP con `security login create` E il ruolo appropriato per i privilegi SVM a livello di cluster o singoli.

È possibile specificare un nome utente per il backup locale o un nome utente NIS o LDAP per `-user-or-group-name` parametro.

Il seguente comando crea l'utente di backup `backup_admin1` con backup ruolo per l'intero cluster:

```
cluster1::> security login create -user-or-group-name backup_admin1  
-application ssh -authmethod password -role backup
```

Il seguente comando crea l'utente di backup `vsbackup_admin1` con `vsadmin-backup` Ruolo di una singola SVM:

```
cluster1::> security login create -user-or-group-name vsbackup_admin1  
-application ssh -authmethod password -role vsadmin-backup
```

Inserire una password per il nuovo utente e confermare.

3. Generare una password per la SVM amministrativa utilizzando `vserver services ndmp generate password` comando.

La password generata deve essere utilizzata per autenticare la connessione NDMP dall'applicazione di backup.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1  
-user backup_admin1
```

```
Vserver: cluster1  
User: backup_admin1  
Password: qG5CqQHYxw7tE57g
```

## Configurare le LIF

È necessario identificare le LIF che verranno utilizzate per stabilire una connessione dati tra le risorse di dati e nastro e per controllare la connessione tra la SVM amministrativa e l'applicazione di backup. Dopo aver identificato i LIF, è necessario verificare che i criteri di firewall e failover siano impostati per i LIF e specificare il ruolo di interfaccia preferito.

A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["LIF e policy di servizio in ONTAP 9.6 e versioni successive"](#).

## Fasi

1. Identificare le LIF di gestione di intercluster, cluster e nodi utilizzando `network interface show` con il `-role` parametro.

Il seguente comando visualizza le LIF dell'intercluster:

```
cluster1::> network interface show -role intercluster
```

|            | Logical   | Status     | Network       | Current    |
|------------|-----------|------------|---------------|------------|
| Current Is |           |            |               |            |
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       |
| Port       | Home      |            |               |            |
| -----      | -----     | -----      | -----         |            |
| -----      | -----     |            |               |            |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 |
| e0a        | true      |            |               |            |
| cluster1   | IC2       | up/up      | 192.0.2.68/24 | cluster1-2 |
| e0b        | true      |            |               |            |

Il seguente comando visualizza la LIF di gestione del cluster:

```
cluster1::> network interface show -role cluster-mgmt
```

|            | Logical      | Status     | Network       | Current    |
|------------|--------------|------------|---------------|------------|
| Current Is |              |            |               |            |
| Vserver    | Interface    | Admin/Oper | Address/Mask  | Node       |
| Port       | Home         |            |               |            |
| -----      | -----        | -----      | -----         |            |
| -----      | -----        |            |               |            |
| cluster1   | cluster_mgmt | up/up      | 192.0.2.60/24 | cluster1-2 |
| e0M        | true         |            |               |            |

Il seguente comando visualizza le LIF di gestione dei nodi:

```
cluster1::> network interface show -role node-mgmt
```

|            | Logical          | Status     | Network       | Current    |
|------------|------------------|------------|---------------|------------|
| Current Is |                  |            |               |            |
| Vserver    | Interface        | Admin/Oper | Address/Mask  | Node       |
| Port       | Home             |            |               |            |
| -----      | -----            | -----      | -----         | -----      |
| -----      | -----            |            |               |            |
| cluster1   | cluster1-1_mgmt1 | up/up      | 192.0.2.69/24 | cluster1-1 |
| e0M        | true             |            |               |            |
|            | cluster1-2_mgmt1 | up/up      | 192.0.2.70/24 | cluster1-2 |
| e0M        | true             |            |               |            |

- Assicurarsi che il criterio firewall sia abilitato per NDMP sulle LIF di intercluster, gestione cluster (gestione cluster) e gestione nodi (gestione nodi):

- a. Verificare che il criterio firewall sia abilitato per NDMP utilizzando `system services firewall policy show` comando.

Il seguente comando visualizza il criterio del firewall per la LIF di gestione del cluster:

```
cluster1::> system services firewall policy show -policy cluster
```

| Vserver | Policy  | Service | Allowed     |
|---------|---------|---------|-------------|
| -----   | -----   | -----   | -----       |
| cluster | cluster | dns     | 0.0.0.0/0   |
|         |         | http    | 0.0.0.0/0   |
|         |         | https   | 0.0.0.0/0   |
|         |         | ** ndmp | 0.0.0.0/0** |
|         |         | ndmps   | 0.0.0.0/0   |
|         |         | ntp     | 0.0.0.0/0   |
|         |         | rsh     | 0.0.0.0/0   |
|         |         | snmp    | 0.0.0.0/0   |
|         |         | ssh     | 0.0.0.0/0   |
|         |         | telnet  | 0.0.0.0/0   |

10 entries were displayed.

Il seguente comando visualizza il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy show -policy intercluster
```

| Vserver  | Policy       | Service | Allowed           |
|----------|--------------|---------|-------------------|
| -----    | -----        | -----   | -----             |
| cluster1 | intercluster | dns     | -                 |
|          |              | http    | -                 |
|          |              | https   | -                 |
|          |              | **ndmp  | 0.0.0.0/0, ::/0** |
|          |              | ndmps   | -                 |
|          |              | ntp     | -                 |
|          |              | rsh     | -                 |
|          |              | ssh     | -                 |
|          |              | telnet  | -                 |

9 entries were displayed.

Il seguente comando visualizza il criterio firewall per la LIF di gestione dei nodi:

```
cluster1::> system services firewall policy show -policy mgmt
```

| Vserver    | Policy | Service | Allowed           |
|------------|--------|---------|-------------------|
| cluster1-1 | mgmt   | dns     | 0.0.0.0/0, ::/0   |
|            |        | http    | 0.0.0.0/0, ::/0   |
|            |        | https   | 0.0.0.0/0, ::/0   |
|            |        | **ndmp  | 0.0.0.0/0, ::/0** |
|            |        | ndmps   | 0.0.0.0/0, ::/0   |
|            |        | ntp     | 0.0.0.0/0, ::/0   |
|            |        | rsh     | -                 |
|            |        | snmp    | 0.0.0.0/0, ::/0   |
|            |        | ssh     | 0.0.0.0/0, ::/0   |
|            |        | telnet  | -                 |

10 entries were displayed.

- b. Se il criterio del firewall non è attivato, attivare il criterio del firewall utilizzando `system services firewall policy modify` con il `-service` parametro.

Il seguente comando abilita il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy modify -vserver cluster1  
-policy intercluster -service ndmp 0.0.0.0/0
```

### 3. Assicurarsi che la policy di failover sia impostata correttamente per tutte le LIF:

- a. Verificare che il criterio di failover per la LIF di gestione del cluster sia impostato su `broadcast-domain-wide` e il criterio per le LIF di gestione di intercluster e nodi è impostato su `local-only` utilizzando `network interface show -failover` comando.

Il seguente comando visualizza il criterio di failover per le LIF di gestione del cluster, dell'intercluster e dei nodi:

```
cluster1::> network interface show -failover
```

| Failover Vserver Group | Logical Interface | Home Node:Port | Failover Policy            |
|------------------------|-------------------|----------------|----------------------------|
| cluster1 cluster       | cluster1_clus1    | cluster1-1:e0a | local-only                 |
|                        |                   |                | Failover Targets:<br>..... |
| **cluster1 Default**   | cluster_mgmt      | cluster1-1:e0m | broadcast-domain-wide      |
|                        |                   |                | Failover Targets:<br>..... |
|                        | **IC1             | cluster1-1:e0a | local-only                 |
| Default**              |                   |                | Failover Targets:<br>..... |
|                        | **IC2             | cluster1-1:e0b | local-only                 |
| Default**              |                   |                | Failover Targets:<br>..... |
| **cluster1-1 Default** | cluster1-1_mgmt1  | cluster1-1:e0m | local-only                 |
|                        |                   |                | Failover Targets:<br>..... |
| **cluster1-2 Default** | cluster1-2_mgmt1  | cluster1-2:e0m | local-only                 |
|                        |                   |                | Failover Targets:<br>..... |

- a. Se i criteri di failover non sono impostati correttamente, modificare il criterio di failover utilizzando `network interface modify` con il `-failover-policy` parametro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

4. Specificare le LIF richieste per la connessione dati utilizzando `vserver services ndmp modify` con il `preferred-interface-role` parametro.

```
cluster1::> vserver services ndmp modify -vserver cluster1 -preferred  
-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Verificare che il ruolo di interfaccia preferito sia impostato per il cluster utilizzando `vserver services ndmp show` comando.

```
cluster1::> vserver services ndmp show -vserver cluster1  
  
Vserver: cluster1  
NDMP Version: 4  
.....  
.....  
Preferred Interface Role: intercluster, cluster-mgmt, node-  
mgmt
```

## Configurare NDMP con ambito nodo

### Abilitare NDMP con ambito di nodo sul cluster

È possibile eseguire il backup dei volumi ospitati su un singolo nodo attivando NDMP con ambito nodo, attivando il servizio NDMP e configurando una LIF per la connessione dati e di controllo. Questa operazione può essere eseguita per tutti i nodi del cluster.



NDMP con ambito del nodo è obsoleto in ONTAP 9.

### A proposito di questa attività

Quando si utilizza NDMP in modalità Node-Scope, l'autenticazione deve essere configurata per nodo. Per ulteriori informazioni, vedere ["L'articolo della Knowledge base "come configurare l'autenticazione NDMP in modalità 'node-scope'"](#).

### Fasi

1. Abilita la modalità NDMP con ambito dei nodi:

```
cluster1::> system services ndmp node-scope-mode on
```

La modalità ambito-nodo NDMP è abilitata.

2. Abilitare il servizio NDMP su tutti i nodi nel cluster:

L'utilizzo del carattere jolly "\*" attiva il servizio NDMP su tutti i nodi contemporaneamente.

Specificare una password per l'autenticazione della connessione NDMP da parte dell'applicazione di backup.



```
cluster1::> system services ndmp on -node *
```

```
Please enter password:  
Confirm password:  
2 entries were modified.
```

### 3. Disattivare `-clear-text` Opzione per la comunicazione sicura della password NDMP:

Utilizzando il carattere jolly "\*" disables the `-clear-text` su tutti i nodi contemporaneamente.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

### 4. Verificare che il servizio NDMP sia attivato e il `-clear-text` opzione disattivata:

```
cluster1::> system services ndmp show
```

| Node       | Enabled | Clear text | User Id |
|------------|---------|------------|---------|
| cluster1-1 | true    | false      | root    |
| cluster1-2 | true    | false      | root    |

2 entries were displayed.

## Configurare una LIF

È necessario identificare una LIF che verrà utilizzata per stabilire una connessione dati e controllare la connessione tra il nodo e l'applicazione di backup. Dopo aver identificato la LIF, è necessario verificare che i criteri di firewall e failover siano impostati per la LIF.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

### Fasi

1. Identificare la LIF di intercluster ospitata sui nodi utilizzando `network interface show` con il `-role` parametro.

```
cluster1::> network interface show -role intercluster
```

| Current Is | Logical   | Status     | Network       | Current    |      |
|------------|-----------|------------|---------------|------------|------|
| Vserver    | Interface | Admin/Oper | Address/Mask  | Node       | Port |
| Home       |           |            |               |            |      |
| -----      | -----     | -----      | -----         | -----      |      |
| -----      |           |            |               |            |      |
| cluster1   | IC1       | up/up      | 192.0.2.65/24 | cluster1-1 | e0a  |
| true       |           |            |               |            |      |
| cluster1   | IC2       | up/up      | 192.0.2.68/24 | cluster1-2 | e0b  |
| true       |           |            |               |            |      |

2. Assicurarsi che il criterio firewall sia abilitato per NDMP sulle LIF dell'intercluster:

- Verificare che il criterio firewall sia abilitato per NDMP utilizzando `system services firewall policy show` comando.

Il seguente comando visualizza il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy show -policy intercluster
```

| Vserver  | Policy       | Service | Allowed           |
|----------|--------------|---------|-------------------|
| -----    | -----        | -----   | -----             |
| cluster1 | intercluster | dns     | -                 |
|          |              | http    | -                 |
|          |              | https   | -                 |
|          |              | **ndmp  | 0.0.0.0/0, ::/0** |
|          |              | ndmps   | -                 |
|          |              | ntp     | -                 |
|          |              | rsh     | -                 |
|          |              | ssh     | -                 |
|          |              | telnet  | -                 |

9 entries were displayed.

- Se il criterio del firewall non è attivato, attivare il criterio del firewall utilizzando `system services firewall policy modify` con il `-service` parametro.

Il seguente comando abilita il criterio firewall per la LIF dell'intercluster:

```
cluster1::> system services firewall policy modify -vserver cluster1  
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Assicurarsi che il criterio di failover sia impostato correttamente per le LIF dell'intercluster:

- a. Verificare che il criterio di failover per le LIF dell'intercluster sia impostato su `local-only` utilizzando `network interface show -failover` comando.

```
cluster1::> network interface show -failover
```

| Vserver    | Logical Interface | Home Node:Port | Failover Policy   | Failover Group |
|------------|-------------------|----------------|-------------------|----------------|
| cluster1   | **IC1             | cluster1-1:e0a | local-only        |                |
| Default**  |                   |                |                   |                |
|            |                   |                | Failover Targets: |                |
|            |                   |                | .....             |                |
|            | **IC2             | cluster1-2:e0b | local-only        |                |
| Default**  |                   |                |                   |                |
|            |                   |                | Failover Targets: |                |
|            |                   |                | .....             |                |
| cluster1-1 | cluster1-1_mgmt1  | cluster1-1:e0m | local-only        | Default        |
|            |                   |                | Failover Targets: |                |
|            |                   |                | .....             |                |

- b. Se il criterio di failover non è impostato correttamente, modificare il criterio di failover utilizzando `network interface modify` con il `-failover-policy` parametro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

## Configurare l'applicazione di backup

Una volta configurato il cluster per l'accesso NDMP, è necessario raccogliere informazioni dalla configurazione del cluster e configurare il resto del processo di backup nell'applicazione di backup.

### Fasi

1. Raccogliere le seguenti informazioni configurate in precedenza in ONTAP:
  - Nome utente e password richiesti dall'applicazione di backup per creare la connessione NDMP
  - Gli indirizzi IP delle LIF di intercluster richieste dall'applicazione di backup per la connessione al cluster
2. In ONTAP, visualizzare gli alias assegnati da ONTAP a ciascun dispositivo utilizzando `storage tape alias show` comando.

Gli alias sono spesso utili nella configurazione dell'applicazione di backup.

```
cluster1::> storage tape show -alias
```

```
Device ID: 2a.0  
Device Type: tape drive  
Description: Hewlett-Packard LTO-5
```

| Node               | Alias | Mapping        |
|--------------------|-------|----------------|
| -----              | ----- | -----          |
| stsw-3220-4a-4b-02 | st2   | SN[HU19497WVR] |
| ...                |       |                |

3. Nell'applicazione di backup, configurare il resto del processo di backup utilizzando la documentazione dell'applicazione di backup.

#### Al termine

Se si verifica un evento di mobilità dei dati, ad esempio uno spostamento del volume o una migrazione LIF, è necessario essere pronti a reinizializzare le operazioni di backup interrotte.

## Replica tra il software NetApp Element e ONTAP

### Replica tra software NetApp Element e panoramica di ONTAP

È possibile garantire la continuità del business su un sistema di elementi utilizzando SnapMirror per replicare le copie Snapshot di un volume di elementi in una destinazione ONTAP. In caso di disastro nel sito Element, è possibile inviare i dati ai client dal sistema ONTAP, quindi riattivare il sistema Element al ripristino del servizio.

A partire da ONTAP 9.4, è possibile replicare le copie Snapshot di un LUN creato su un nodo ONTAP in un sistema di elementi. È possibile che sia stata creata una LUN durante un'interruzione del servizio presso il sito Element o che si stia utilizzando una LUN per migrare i dati da ONTAP a Element Software.

Si consiglia di utilizzare il backup Element to ONTAP se si applicano le seguenti condizioni:

- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI) di ONTAP, non Gestione di sistema o uno strumento di scripting automatico.
- Si sta utilizzando iSCSI per fornire dati ai client.

Per ulteriori informazioni sulla configurazione o concettuali, consultare la seguente documentazione:

- Configurazione dell'elemento

["Documentazione del software NetApp Element"](#)

- Concetti e configurazione di SnapMirror

["Panoramica sulla protezione dei dati"](#)

## Sulla replica tra Element e ONTAP

A partire da ONTAP 9.3, è possibile utilizzare SnapMirror per replicare le copie Snapshot di un volume elemento in una destinazione ONTAP. In caso di disastro nel sito Element, è possibile inviare i dati ai client dal sistema ONTAP, quindi riattivare il volume di origine Element al ripristino del servizio.

A partire da ONTAP 9.4, è possibile replicare le copie Snapshot di un LUN creato su un nodo ONTAP in un sistema di elementi. È possibile che sia stata creata una LUN durante un'interruzione del servizio presso il sito Element o che si stia utilizzando una LUN per migrare i dati da ONTAP a Element Software.

### Tipi di relazione di protezione dei dati

SnapMirror offre due tipi di relazione per la protezione dei dati. Per ciascun tipo, SnapMirror crea una copia Snapshot del volume di origine dell'elemento prima di inizializzare o aggiornare la relazione:

- In una relazione di protezione dei dati di *disaster recovery (DR)*, il volume di destinazione contiene solo la copia Snapshot creata da SnapMirror, da cui è possibile continuare a fornire i dati in caso di disastro nel sito primario.
- In una relazione di *conservazione a lungo termine* data Protection, il volume di destinazione contiene copie Snapshot point-in-time create dal software Element, nonché la copia Snapshot creata da SnapMirror. Ad esempio, è possibile conservare le copie Snapshot mensili create nell'arco di 20 anni.

### Policy predefinite

La prima volta che si richiama SnapMirror, esegue un *trasferimento baseline* dal volume di origine al volume di destinazione. La *policy SnapMirror* definisce il contenuto della linea di base e gli eventuali aggiornamenti.

È possibile utilizzare una policy predefinita o personalizzata quando si crea una relazione di protezione dei dati. Il *tipo di policy* determina quali copie Snapshot includere e quante copie conservare.

La tabella seguente mostra i criteri predefiniti. Utilizzare `MirrorLatest` Policy per creare una relazione DR tradizionale. Utilizzare `MirrorAndVault` oppure `Unified7year` Policy per creare una relazione di replica unificata, in cui DR e conservazione a lungo termine sono configurati sullo stesso volume di destinazione.

| Policy         | Tipo di policy   | Comportamento degli aggiornamenti                                                                                                                                                                                    |
|----------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MirrorLatest   | mirror asincrono | Trasferire la copia Snapshot creata da SnapMirror.                                                                                                                                                                   |
| MirrorAndVault | vault mirror     | Trasferire la copia Snapshot creata da SnapMirror e le copie Snapshot meno recenti effettuate dall'ultimo aggiornamento, a condizione che siano dotate di etichette SnapMirror "daily" o "settimanale".              |
| Unified7year   | vault mirror     | Trasferire la copia Snapshot creata da SnapMirror e le copie Snapshot meno recenti effettuate dall'ultimo aggiornamento, a condizione che siano dotate delle etichette SnapMirror "daily", "settimanale" o "mOnhly". |



Per informazioni complete sulle policy di SnapMirror, incluse indicazioni su quali policy utilizzare, vedere ["Protezione dei dati"](#).

## Informazioni sulle etichette SnapMirror

Ogni policy con il tipo di policy “mirror-vault” deve avere una regola che specifica quali copie Snapshot replicare. La regola “daily”, ad esempio, indica che solo le copie Snapshot assegnate all’etichetta SnapMirror “daily” devono essere replicate. L’etichetta SnapMirror viene assegnata quando si configurano le copie Snapshot degli elementi.

### Replica da un cluster di origine elemento a un cluster di destinazione ONTAP

È possibile utilizzare SnapMirror per replicare le copie Snapshot di un volume elemento in un sistema di destinazione ONTAP. In caso di disastro nel sito Element, è possibile inviare i dati ai client dal sistema ONTAP, quindi riattivare il volume di origine Element al ripristino del servizio.

Un volume Element equivale approssimativamente a un LUN ONTAP. SnapMirror crea un LUN con il nome del volume Element quando viene inizializzata una relazione di protezione dei dati tra il software Element e ONTAP. SnapMirror replica i dati su un LUN esistente se il LUN soddisfa i requisiti per la replica Element to ONTAP.

Le regole di replica sono le seguenti:

- Un volume ONTAP può contenere dati provenienti da un solo volume elemento.
- Non è possibile replicare i dati da un volume ONTAP a più volumi di elementi.

### Replica da un cluster di origine ONTAP a un cluster di destinazione elemento

A partire da ONTAP 9.4, è possibile replicare le copie Snapshot di un LUN creato su un sistema ONTAP in un volume Element:

- Se esiste già una relazione SnapMirror tra un’origine elemento e una destinazione ONTAP, un LUN creato durante la fornitura dei dati dalla destinazione viene replicato automaticamente quando l’origine viene riattivata.
- In caso contrario, è necessario creare e inizializzare una relazione SnapMirror tra il cluster di origine ONTAP e il cluster di destinazione degli elementi.

Le regole di replica sono le seguenti:

- La relazione di replica deve avere una policy di tipo “async-mirror”.

Le policy di tipo “mirror-vault” non sono supportate.

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di un LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare un LUN da un volume ONTAP a più volumi di elementi.

## Prerequisiti

Prima di configurare una relazione di protezione dei dati tra Element e ONTAP, è necessario aver completato le seguenti attività:

- Il cluster di elementi deve eseguire il software NetApp Element versione 10.1 o successiva.
- Il cluster ONTAP deve eseguire ONTAP 9.3 o versione successiva.
- SnapMirror deve essere stato concesso in licenza sul cluster ONTAP.

- È necessario configurare volumi nei cluster Element e ONTAP sufficientemente grandi per gestire i trasferimenti di dati anticipati.
- Se si utilizza il tipo di policy “mirror-vault”, è necessario configurare un’etichetta SnapMirror per la replica delle copie Snapshot degli elementi.



È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element. Per ulteriori informazioni, consultare ["Documentazione del software NetApp Element"](#)

- È necessario assicurarsi che la porta 5010 sia disponibile.
- Se si prevede che potrebbe essere necessario spostare un volume di destinazione, è necessario assicurarsi che la connettività full-mesh esista tra l'origine e la destinazione. Ogni nodo del cluster di origine degli elementi deve essere in grado di comunicare con ogni nodo del cluster di destinazione ONTAP.

### Dettagli del supporto

La seguente tabella mostra i dettagli del supporto per il backup Element to ONTAP.

| Risorsa o funzione | Dettagli del supporto                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SnapMirror         | <ul style="list-style-type: none"> <li>• La funzione di ripristino di SnapMirror non è supportata.</li> <li>• Il <code>MirrorAllSnapshots</code> e <code>XDPEndpoint</code> i criteri non sono supportati.</li> <li>• Il tipo di policy “vault” non è supportato.</li> <li>• La regola definita dal sistema “all_source_snapshot” non è supportata.</li> <li>• Il tipo di policy “mirror-vault” è supportato solo per la replica dal software Element a ONTAP. Utilizzare “async-mirror” per la replica da ONTAP al software Element.</li> <li>• Il <code>-schedule</code> e <code>-prefix</code> opzioni per <code>snapmirror policy add-rule</code> non sono supportati.</li> <li>• Il <code>-preserve</code> e <code>-quick-resync</code> opzioni per <code>snapmirror resync</code> non sono supportati.</li> <li>• L'efficienza dello storage non viene preservata.</li> <li>• Le implementazioni di protezione dei dati fan-out e cascata non sono supportate.</li> </ul> |
| ONTAP              | <ul style="list-style-type: none"> <li>• ONTAP Select è supportato a partire da ONTAP 9.4 ed Element 10.3.</li> <li>• Cloud Volumes ONTAP è supportato a partire da ONTAP 9.5 ed Element 11.0.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Elemento           | <ul style="list-style-type: none"> <li>• Il limite delle dimensioni del volume è 8 TiB.</li> <li>• La dimensione del blocco di volume deve essere di 512 byte. Le dimensioni di un blocco di 4K byte non sono supportate.</li> <li>• Le dimensioni del volume devono essere un multiplo di 1 MiB.</li> <li>• Gli attributi del volume non vengono conservati.</li> <li>• Il numero massimo di copie Snapshot da replicare è 30.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|              |                                                                                                                                                                                                                                                                                        |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rete         | <ul style="list-style-type: none"> <li>• È consentita una singola connessione TCP per ogni trasferimento.</li> <li>• Il nodo Element deve essere specificato come indirizzo IP. La ricerca del nome host DNS non è supportata.</li> <li>• Gli IPspaces non sono supportati.</li> </ul> |
| SnapLock     | I volumi SnapLock non sono supportati.                                                                                                                                                                                                                                                 |
| FlexGroup    | I volumi FlexGroup non sono supportati.                                                                                                                                                                                                                                                |
| DR. SVM      | I volumi ONTAP in una configurazione DR SVM non sono supportati.                                                                                                                                                                                                                       |
| MetroCluster | I volumi ONTAP in una configurazione MetroCluster non sono supportati.                                                                                                                                                                                                                 |

## Workflow per la replica tra Element e ONTAP

Sia che si stiano replicando i dati da Element a ONTAP o da ONTAP a Element, è necessario configurare una pianificazione del processo, specificare una policy e creare e inizializzare la relazione. È possibile utilizzare un criterio predefinito o personalizzato.

Il flusso di lavoro presuppone che siano state completate le attività preliminari elencate nella [Prerequisiti](#). Per informazioni complete sulle policy di SnapMirror, incluse indicazioni su quali policy utilizzare, vedere ["Protezione dei dati"](#).





## Attivare SnapMirror nel software Element

### Attivare SnapMirror sul cluster di elementi

È necessario attivare SnapMirror sul cluster di elementi prima di poter creare una

relazione di replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element.

#### Prima di iniziare

- Il cluster di elementi deve eseguire il software NetApp Element versione 10.1 o successiva.
- SnapMirror può essere abilitato solo per i cluster di elementi utilizzati con i volumi NetApp ONTAP.

#### A proposito di questa attività

Il sistema Element viene fornito con SnapMirror disattivato per impostazione predefinita. SnapMirror non viene attivato automaticamente come parte di una nuova installazione o di un aggiornamento.



Una volta attivato, SnapMirror non può essere disattivato. È possibile disattivare la funzione SnapMirror e ripristinare le impostazioni predefinite solo ripristinando l'immagine predefinita del cluster.

#### Fasi

1. Fare clic su **Clusters > Impostazioni**.
2. Individuare le impostazioni specifiche del cluster per SnapMirror.
3. Fare clic su **Enable SnapMirror** (attiva SnapMirror)

#### Attivare SnapMirror sul volume di origine dell'elemento

Prima di creare una relazione di replica, è necessario attivare SnapMirror sul volume di origine dell'elemento. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element.


#### Prima di iniziare

- È necessario aver attivato SnapMirror sul cluster di elementi.
- La dimensione del blocco del volume deve essere di 512 byte.
- Il volume non deve partecipare alla replica remota degli elementi.
- Il tipo di accesso al volume non deve essere "Replication Target".

#### A proposito di questa attività

La procedura riportata di seguito presuppone che il volume esista già. È inoltre possibile attivare SnapMirror quando si crea o clona un volume.

#### Fasi

1. Selezionare **Management > Volumes**.
2. Selezionare  per il volume.
3. Nel menu a discesa, selezionare **Modifica**.
4. Nella finestra di dialogo **Edit Volume** (Modifica volume), selezionare **Enable SnapMirror** (attiva SnapMirror).
5. Selezionare **Save Changes** (Salva modifiche).

#### Creare un endpoint SnapMirror

È necessario creare un endpoint SnapMirror prima di poter creare una relazione di

replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element.

### Prima di iniziare

È necessario aver attivato SnapMirror sul cluster di elementi.

### Fasi

1. Fare clic su **Data Protection > SnapMirror Endpoints**.
2. Fare clic su **Create Endpoint** (Crea endpoint).
3. Nella finestra di dialogo **Crea nuovo endpoint**, immettere l'indirizzo IP di gestione del cluster ONTAP.
4. Inserire l'ID utente e la password dell'amministratore del cluster ONTAP.
5. Fare clic su **Create Endpoint** (Crea endpoint).

## Configurare una relazione di replica

### Creare una pianificazione del processo di replica

Sia che si stiano replicando i dati da Element a ONTAP o da ONTAP a Element, è necessario configurare una pianificazione del processo, specificare una policy e creare e inizializzare la relazione. È possibile utilizzare un criterio predefinito o personalizzato.

È possibile utilizzare `job schedule cron create` per creare una pianificazione del processo di replica. La pianificazione del processo determina quando SnapMirror aggiorna automaticamente la relazione di protezione dei dati a cui viene assegnata la pianificazione.

### A proposito di questa attività

Quando si crea una relazione di protezione dei dati, viene assegnata una pianificazione dei processi. Se non si assegna una pianificazione del lavoro, è necessario aggiornare la relazione manualmente.

### Fase

1. Creare una pianificazione del processo:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Per `-month`, `-dayofweek`, e `-hour`, è possibile specificare `all` per eseguire il processo ogni mese, giorno della settimana e ora, rispettivamente.

A partire da ONTAP 9.10.1, è possibile includere il server virtuale per la pianificazione del processo:

```
job schedule cron create -name job_name -vserver Vserver_name -month month
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

Nell'esempio seguente viene creata una pianificazione del processo denominata `my_weekly` il sabato alle 3:00:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

## Personalizzare un criterio di replica

### Creare un criterio di replica personalizzato

È possibile utilizzare un criterio predefinito o personalizzato quando si crea una relazione di replica. Per una policy di replica unificata personalizzata, è necessario definire una o più *regole* che determinano quali copie Snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento.

È possibile creare un criterio di replica personalizzato se il criterio predefinito per una relazione non è adatto. È possibile, ad esempio, comprimere i dati in un trasferimento di rete o modificare il numero di tentativi eseguiti da SnapMirror per trasferire le copie Snapshot.

### A proposito di questa attività

Il *tipo di policy* del criterio di replica determina il tipo di relazione che supporta. La tabella seguente mostra i tipi di policy disponibili.

| Tipo di policy   | Tipo di relazione |
|------------------|-------------------|
| mirror asincrono | Dr. SnapMirror    |
| vault mirror     | Replica unificata |

### Fase

1. Creare un criterio di replica personalizzato:

```
snapmirror policy create -vserver SVM -policy policy -type async-  
mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority  
low|normal -is-network-compression-enabled true|false
```

Per la sintassi completa dei comandi, vedere la pagina man.

A partire da ONTAP 9.5, è possibile specificare la pianificazione per la creazione di una pianificazione di copia Snapshot comune per le relazioni sincroni di SnapMirror utilizzando `-common-snapshot` `-schedule` parametro. Per impostazione predefinita, il programma di copia Snapshot comune per le relazioni sincrone di SnapMirror è di un'ora. È possibile specificare un valore compreso tra 30 minuti e due ore per la pianificazione della copia Snapshot per le relazioni sincroni di SnapMirror.

Nell'esempio seguente viene creato un criterio di replica personalizzato per il DR SnapMirror che consente la compressione di rete per i trasferimenti di dati:

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
DR_compressed -type async-mirror -comment "DR with network compression  
enabled" -is-network-compression-enabled true
```

Nell'esempio seguente viene creata una policy di replica personalizzata per la replica unificata:

```
cluster_dst::> snapmirror policy create -vserver svml -policy my_unified  
-type mirror-vault
```

### Al termine

Per i tipi di policy “mirror-vault”, è necessario definire le regole che determinano quali copie Snapshot vengono trasferite durante l’inizializzazione e l’aggiornamento.

Utilizzare `snapmirror policy show` Per verificare che il criterio SnapMirror sia stato creato. Per la sintassi completa dei comandi, vedere la pagina [man](#).

### Definire una regola per un criterio

Per i criteri personalizzati con il tipo di policy “mirror-vault”, è necessario definire almeno una regola che determina quali copie Snapshot vengono trasferite durante l’inizializzazione e l’aggiornamento. È inoltre possibile definire le regole per i criteri di default con il tipo di policy “mirror-vault”.

### A proposito di questa attività

Ogni policy con il tipo di policy “mirror-vault” deve avere una regola che specifica quali copie Snapshot replicare. La regola “bimestrale”, ad esempio, indica che devono essere replicate solo le copie Snapshot assegnate all’etichetta SnapMirror “bimestrale”. L’etichetta SnapMirror viene assegnata quando si configurano le copie Snapshot degli elementi.

Ogni tipo di policy è associato a una o più regole definite dal sistema. Queste regole vengono assegnate automaticamente a un criterio quando si specifica il relativo tipo di criterio. La tabella seguente mostra le regole definite dal sistema.

| Regola definita dal sistema | Utilizzato nei tipi di policy  | Risultato                                                                                                                                  |
|-----------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| sm_created                  | mirror asincrono, vault mirror | Una copia Snapshot creata da SnapMirror viene trasferita all’inizializzazione e all’aggiornamento.                                         |
| ogni giorno                 | vault mirror                   | Le nuove copie Snapshot sull’origine con l’etichetta SnapMirror “daily” vengono trasferite all’inizializzazione e all’aggiornamento.       |
| settimanale                 | vault mirror                   | Le nuove copie Snapshot sull’origine con l’etichetta SnapMirror “settimanale” vengono trasferite all’inizializzazione e all’aggiornamento. |

|         |              |                                                                                                                                       |
|---------|--------------|---------------------------------------------------------------------------------------------------------------------------------------|
| mensile | vault mirror | Le nuove copie Snapshot sull'origine con l'etichetta SnapMirror "mOnhly" vengono trasferite all'inizializzazione e all'aggiornamento. |
|---------|--------------|---------------------------------------------------------------------------------------------------------------------------------------|

È possibile specificare regole aggiuntive in base alle esigenze, per i criteri predefiniti o personalizzati. Ad esempio:

- Per impostazione predefinita `MirrorAndVault` Policy, è possibile creare una regola chiamata "bimestrale" per associare le copie Snapshot sull'origine con l'etichetta "bimestrale" SnapMirror.
- Per una policy personalizzata con il tipo di policy "mirror-vault", è possibile creare una regola chiamata "bisettimanale" per far corrispondere le copie Snapshot sull'origine con l'etichetta "bisettimanale" SnapMirror.

## Fase

1. Definire una regola per un criterio:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
-label snapmirror-label -keep retention_count
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror `bi-monthly` al valore predefinito `MirrorAndVault` policy:

```
cluster_dst:> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror `bi-weekly` al personalizzato `my_snapvault` policy:

```
cluster_dst:> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

Nell'esempio seguente viene aggiunta una regola con l'etichetta SnapMirror `app_consistent` al personalizzato `Sync` policy:

```
cluster_dst:> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

È quindi possibile replicare le copie Snapshot dal cluster di origine che corrispondono a questa etichetta SnapMirror:

```
cluster_src::> snapshot create -vserver vs1 -volume voll -snapshot  
snapshot1 -snapmirror-label app_consistent
```

## Creare una relazione di replica

### Creare una relazione da un'origine elemento a una destinazione ONTAP

La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene definita *relazione di protezione dei dati*. È possibile utilizzare `snapmirror create` Comando per creare una relazione di protezione dei dati da un'origine elemento a una destinazione ONTAP o da un'origine ONTAP a una destinazione elemento.

È possibile utilizzare SnapMirror per replicare le copie Snapshot di un volume elemento in un sistema di destinazione ONTAP. In caso di disastro nel sito Element, è possibile inviare i dati ai client dal sistema ONTAP, quindi riattivare il volume di origine Element al ripristino del servizio.

#### Prima di iniziare

- Il nodo Element contenente il volume da replicare deve essere stato reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica di SnapMirror.
- Se si utilizza il tipo di policy "mirror-vault", è necessario configurare un'etichetta SnapMirror per la replica delle copie Snapshot degli elementi.



È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element. Per ulteriori informazioni, consultare ["Documentazione degli elementi"](#).

#### A proposito di questa attività

Specificare il percorso di origine dell'elemento nel modulo `hostip:/lun/name`, dove "lun" è la stringa effettiva "lun" e. `name` È il nome del volume Element.

Un volume Element equivale approssimativamente a un LUN ONTAP. SnapMirror crea un LUN con il nome del volume Element quando viene inizializzata una relazione di protezione dei dati tra il software Element e ONTAP. SnapMirror replica i dati su un LUN esistente se il LUN soddisfa i requisiti per la replica dal software Element a ONTAP.

Le regole di replica sono le seguenti:

- Un volume ONTAP può contenere dati provenienti da un solo volume elemento.
- Non è possibile replicare i dati da un volume ONTAP a più volumi di elementi.

In ONTAP 9.3 e versioni precedenti, un volume di destinazione può contenere fino a 251 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume di destinazione può contenere fino a 1019 copie Snapshot.

#### Fase

1. Dal cluster di destinazione, creare una relazione di replica da un'origine elemento a una destinazione ONTAP:

```
snapmirror create -source-path hostip:/lun/name -destination-path SVM:volume
```

```
|cluster://SVM/volume -type XDP -schedule schedule -policy policy
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita MirrorLatest policy:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy MirrorLatest
```

Nell'esempio seguente viene creata una relazione di replica unificata utilizzando l'impostazione predefinita MirrorAndVault policy:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy MirrorAndVault
```

Nell'esempio riportato di seguito viene creata una relazione di replica unificata utilizzando Unified7year policy:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy Unified7year
```

Nell'esempio riportato di seguito viene creata una relazione di replica unificata utilizzando il metodo personalizzato my\_unified policy:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily  
-policy my_unified
```

## Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

## Creare una relazione da un'origine ONTAP a una destinazione dell'elemento

A partire da ONTAP 9.4, è possibile utilizzare SnapMirror per replicare le copie Snapshot di un LUN creato su un'origine ONTAP verso una destinazione dell'elemento. È possibile che si stia utilizzando il LUN per migrare i dati da ONTAP a Element Software.

## Prima di iniziare

- Il nodo di destinazione dell'elemento deve essere stato reso accessibile a ONTAP.



- Il volume Element deve essere stato abilitato per la replica di SnapMirror.

### A proposito di questa attività

Specificare il percorso di destinazione dell'elemento nel modulo `hostip:/lun/name`, dove "lun" è la stringa effettiva "lun" e. name È il nome del volume Element.

Le regole di replica sono le seguenti:

- La relazione di replica deve avere una policy di tipo "async-mirror".
- È possibile utilizzare un criterio predefinito o personalizzato.
- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di un LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare un LUN da un volume ONTAP a più volumi di elementi.

### Fase

1. Creare una relazione di replica da un'origine ONTAP a una destinazione dell'elemento:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume -destination
-path hostip:/lun/name -type XDP -schedule schedule -policy policy
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene creata una relazione di DR SnapMirror utilizzando l'impostazione predefinita MirrorLatest policy:

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

Nell'esempio riportato di seguito viene creata una relazione di DR SnapMirror utilizzando il metodo personalizzato my\_mirror policy:

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy my_mirror
```

### Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

### Inizializzare una relazione di replica

Per tutti i tipi di relazione, l'inizializzazione esegue un *trasferimento baseline*: Esegue una copia Snapshot del volume di origine, quindi trasferisce la copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.

## Prima di iniziare

- Il nodo Element contenente il volume da replicare deve essere stato reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica di SnapMirror.
- Se si utilizza il tipo di policy “mirror-vault”, è necessario configurare un’etichetta SnapMirror per la replica delle copie Snapshot degli elementi.

## A proposito di questa attività

Specificare il percorso di origine dell’elemento nel modulo *hostip:/lun/name*, dove “lun” è la stringa effettiva “lun” e *name* È il nome del volume Element.

L’inizializzazione può richiedere molto tempo. Si consiglia di eseguire il trasferimento di riferimento in ore non di punta.



Se l’inizializzazione di una relazione da un’origine ONTAP a una destinazione dell’elemento non riesce per qualsiasi motivo, continuerà a fallire anche dopo aver corretto il problema (ad esempio, un nome LUN non valido). La soluzione è la seguente:

1. Eliminare la relazione.
2. Eliminare il volume di destinazione dell’elemento.
3. Creare un nuovo volume di destinazione elemento.
4. Creare e inizializzare una nuova relazione dall’origine ONTAP al volume di destinazione dell’elemento.

## Fase

1. Inizializzare una relazione di replica:

```
snapmirror initialize -source-path hostip:/lun/name -destination-path  
SVM:volume|cluster://SVM/volume
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell’esempio riportato di seguito viene inizializzata la relazione tra il volume di origine 0005 All’indirizzo IP 10.0.0.11 e al volume di destinazione volA\_dst acceso svm\_backup:

```
cluster_dst:> snapmirror initialize -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

## Fornire i dati da un volume di destinazione DR SnapMirror

### Rendere il volume di destinazione scrivibile

Quando Disaster disattiva il sito primario per una relazione di disaster recovery SnapMirror, è possibile fornire i dati dal volume di destinazione con interruzioni minime. È possibile riattivare il volume di origine quando il servizio viene ripristinato nel sito primario.

È necessario rendere il volume di destinazione scrivibile prima di poter inviare i dati dal volume ai client. È

possibile utilizzare `snapmirror quiesce` per arrestare i trasferimenti pianificati verso la destinazione, il `snapmirror abort` per interrompere i trasferimenti in corso e il `snapmirror break` per rendere la destinazione scrivibile.

### A proposito di questa attività

Specificare il percorso di origine dell'elemento nel modulo `hostip:/lun/name`, dove "lun" è la stringa effettiva "lun" e. name È il nome del volume Element.

### Fasi

1. Interrompere i trasferimenti pianificati verso la destinazione:

```
snapmirror quiesce -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono interrotti i trasferimenti pianificati tra il volume di origine 0005 All'indirizzo IP 10.0.0.11 e al volume di destinazione volA\_dst acceso svm\_backup:

```
cluster_dst:> snapmirror quiesce -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

2. Interrompere i trasferimenti in corso verso la destinazione:

```
snapmirror abort -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono interrotti i trasferimenti in corso tra il volume di origine 0005 All'indirizzo IP 10.0.0.11 e al volume di destinazione volA\_dst acceso svm\_backup:

```
cluster_dst:> snapmirror abort -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

3. Interrompere la relazione di disaster recovery di SnapMirror:

```
snapmirror break -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene spezzata la relazione tra il volume di origine 0005 All'indirizzo IP 10.0.0.11 e al volume di destinazione volA\_dst acceso svm\_backup e il volume di destinazione volA\_dst acceso svm\_backup:

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

### Configurare il volume di destinazione per l'accesso ai dati

Una volta reso scrivibile il volume di destinazione, è necessario configurare il volume per l'accesso ai dati. Gli host SAN possono accedere ai dati dal volume di destinazione fino alla riattivazione del volume di origine.

1. Mappare il LUN dell'elemento al gruppo iniziatore appropriato.
2. Creare sessioni iSCSI dagli iniziatori host SAN alle LIF SAN.
3. Sul client SAN, eseguire una nuova scansione dello storage per rilevare il LUN connesso.

### Riattivare il volume di origine originale

È possibile ristabilire la relazione di protezione dei dati originale tra i volumi di origine e di destinazione quando non è più necessario fornire dati dalla destinazione.

#### A proposito di questa attività

La procedura riportata di seguito presuppone che la linea di base nel volume di origine originale sia intatta. Se la linea di base non è intatta, è necessario creare e inizializzare la relazione tra il volume da cui si stanno fornendo i dati e il volume di origine originale prima di eseguire la procedura.

Specificare il percorso di origine dell'elemento nel modulo *hostip:/lun/name*, dove "lun" è la stringa effettiva "lun" e. *name* È il nome del volume Element.

A partire da ONTAP 9.4, le copie Snapshot di un LUN create durante la distribuzione dei dati dalla destinazione ONTAP vengono replicate automaticamente quando l'origine dell'elemento viene riattivata.

Le regole di replica sono le seguenti:

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di un LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare un LUN da un volume ONTAP a più volumi di elementi.

#### Fasi

1. Eliminare la relazione di protezione dei dati originale:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name -policy policy
```

Per la sintassi completa dei comandi, vedere la pagina *man*.

Nell'esempio seguente viene eliminata la relazione tra il volume di origine originale, 0005 All'indirizzo IP 10.0.0.11 e al volume da cui si stanno servendo i dati, volA\_dst acceso svm\_backup:

```
cluster_dst:> snapmirror delete -source-path 10.0.0.11:/lun/0005  
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

## 2. Invertire la relazione di protezione dei dati originale:

```
snapmirror resync -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name -policy policy
```

Per la sintassi completa dei comandi, vedere la pagina man.

Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

Nell'esempio seguente viene invertita la relazione tra il volume di origine originale, 0005 All'indirizzo IP 10.0.0.11 e al volume da cui si stanno servendo i dati, volA\_dst acceso svm\_backup:

```
cluster_dst:> snapmirror resync -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

## 3. Aggiornare la relazione inversa:

```
snapmirror update -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name
```

Per la sintassi completa dei comandi, vedere la pagina man.



Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

Nell'esempio riportato di seguito viene aggiornata la relazione tra il volume da cui si stanno fornendo i dati, volA\_dst acceso svm\_backup e il volume di origine originale, 0005 All'indirizzo IP 10.0.0.11:

```
cluster_dst:> snapmirror update -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

## 4. Arrestare i trasferimenti pianificati per la relazione invertita:

```
snapmirror quiesce -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente vengono interrotti i trasferimenti pianificati tra il volume da cui si stanno fornendo i dati, volA\_dst acceso svm\_backup e il volume di origine originale, 0005 All'indirizzo IP 10.0.0.11:

```
cluster_dst:> snapmirror quiesce -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

#### 5. Arrestare i trasferimenti in corso per la relazione invertita:

```
snapmirror abort -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente interrompe i trasferimenti in corso tra il volume da cui si stanno servendo i dati, volA\_dst acceso svm\_backup`e il volume di origine originale, `0005 All'indirizzo IP 10.0.0.11:

```
cluster_dst:> snapmirror abort -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

#### 6. Interrompere la relazione inversa:

```
snapmirror break -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene spezzata la relazione tra il volume da cui si stanno fornendo i dati, volA\_dst acceso svm\_backup`e il volume di origine originale, `0005 All'indirizzo IP 10.0.0.11:

```
cluster_dst:> snapmirror break -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

#### 7. Eliminare la relazione di protezione dei dati invertita:

```
snapmirror delete -source-path SVM:volume|cluster://SVM/volume -destination  
-path hostip:/lun/name -policy policy
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene eliminata la relazione inversa tra il volume di origine originale, 0005 All'indirizzo IP 10.0.0.11 e al volume da cui si stanno servendo i dati, volA\_dst acceso svm\_backup:

```
cluster_src:> snapmirror delete -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

#### 8. Ristabilire la relazione di protezione dei dati originale:

```
snapmirror resync -source-path hostip:/lun/name -destination-path
```

```
SVM:volume|cluster://SVM/volume
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio seguente viene ristabilita la relazione tra il volume di origine originale, 0005 All'indirizzo IP 10.0.0.11 e al volume di destinazione originale, volA\_dst acceso svm\_backup:

```
cluster_dst:> snapmirror resync -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

### Al termine

Utilizzare `snapmirror show` Per verificare che sia stata creata la relazione SnapMirror. Per la sintassi completa dei comandi, vedere la pagina man.

## Aggiornare manualmente una relazione di replica

Potrebbe essere necessario aggiornare manualmente una relazione di replica se un aggiornamento non riesce a causa di un errore di rete.

### A proposito di questa attività

Specificare il percorso di origine dell'elemento nel modulo `hostip:/lun/name`, dove "lun" è la stringa effettiva "lun" e. name È il nome del volume Element.

### Fasi

1. Aggiornare manualmente una relazione di replica:

```
snapmirror update -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume
```

Per la sintassi completa dei comandi, vedere la pagina man.



Il comando non riesce se non esiste una copia Snapshot comune sull'origine e sulla destinazione. Utilizzare `snapmirror initialize` per reinizializzare la relazione.

Nell'esempio seguente viene aggiornata la relazione tra il volume di origine 0005 All'indirizzo IP 10.0.0.11 e al volume di destinazione volA\_dst acceso svm\_backup:

```
cluster_src:> snapmirror update -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

## Risincronizzare una relazione di replica

È necessario risincronizzare una relazione di replica dopo che si rende scrivibile un volume di destinazione, dopo che un aggiornamento non riesce perché non esiste una copia Snapshot comune sui volumi di origine e di destinazione o se si desidera modificare il criterio di replica per la relazione.

## A proposito di questa attività

Sebbene la risincronizzazione non richieda un trasferimento di riferimento, può richiedere molto tempo. È possibile eseguire la risincronizzazione in ore non di punta.

Specificare il percorso di origine dell'elemento nel modulo *hostip:/lun/name*, dove "lun" è la stringa effettiva "lun" e. name È il nome del volume Element.

## Fase

1. Risincronizzare i volumi di origine e di destinazione:

```
snapmirror resync -source-path hostip:/lun/name -destination-path SVM:volume  
|cluster://SVM/volume -type XDP -policy policy
```

Per la sintassi completa dei comandi, vedere la pagina man.

Nell'esempio riportato di seguito viene risincronata la relazione tra il volume di origine 0005 All'indirizzo IP 10.0.0.11 e al volume di destinazione volA\_dst acceso svm\_backup:

```
cluster_dst::> snapmirror resync -source-path 10.0.0.11:/lun/0005  
-policy MirrorLatest -destination-path svm_backup:volA_dst
```



# Monitoraggio di eventi, performance e stato

## Monitorare le performance del cluster con System Manager

### Monitorare le performance del cluster utilizzando System Manager

Gli argomenti di questa sezione mostrano come gestire lo stato e le performance del cluster con Gestione di sistema in ONTAP 9.7 e versioni successive.

È possibile monitorare le prestazioni del cluster visualizzando le informazioni relative al sistema nella dashboard di System Manager. La dashboard visualizza informazioni su avvisi e notifiche importanti, l'efficienza e la capacità dei livelli e dei volumi di storage, i nodi disponibili in un cluster, lo stato dei nodi in una coppia ha, le applicazioni e gli oggetti più attivi, e le metriche delle performance di un cluster o di un nodo.

La dashboard consente di determinare le seguenti informazioni:

- **\* Health\***: Quanto è sano il cluster?
- **Capacità**: Quale capacità è disponibile sul cluster?
- **Performance**: Quali sono le performance del cluster, in base a latenza, IOPS e throughput?
- **Rete**: Come viene configurata la rete con host e oggetti storage, come porte, interfacce e macchine virtuali di storage?

Nelle panoramiche su salute e capacità, fare clic su [→](#) per visualizzare informazioni aggiuntive ed eseguire attività.

Nella panoramica delle performance, puoi visualizzare le metriche in base all'ora, al giorno, alla settimana, al mese o all'anno.

Nella panoramica della rete viene visualizzato il numero di ciascun oggetto della rete (ad esempio, "8 porte NVMe/FC"). È possibile fare clic sui numeri per visualizzare i dettagli relativi a ciascun oggetto di rete.

### Visualizza le performance sulla dashboard del cluster

Utilizza la dashboard per prendere decisioni informate sui carichi di lavoro che potresti voler aggiungere o spostare. Puoi anche considerare i tempi di utilizzo più elevati per pianificare potenziali cambiamenti.

I valori delle performance si aggiornano ogni 3 secondi e il grafico delle performance si aggiorna ogni 15 secondi.

#### Fasi

1. Fare clic su **Dashboard**.
2. In **Performance**, selezionare l'intervallo.

### Identificare gli hot volumi e altri oggetti

Accelera le performance del tuo cluster identificando i volumi con accesso frequente (hot volumi) e i dati (hot objects).



A partire da ONTAP 9.10.1, è possibile utilizzare la funzione monitoraggio attività di analisi del file system per monitorare gli oggetti hot in un volume.


#### Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Filtrare le colonne IOPS, latenza e throughput per visualizzare i volumi e i dati utilizzati di frequente.

### Modificare QoS

A partire da ONTAP 9,8, per il provisioning dello storage, [Qualità del servizio \(QoS\)](#) è attivato per impostazione predefinita. È possibile disattivare la QoS o scegliere una policy QoS personalizzata durante il processo di provisioning. È inoltre possibile modificare la QoS dopo il provisioning dello storage.

#### Fasi

1. In Gestione sistema, selezionare **archiviazione**, quindi **volumi**.
2. Accanto al volume per cui si desidera modificare la qualità del servizio, selezionare  Quindi **Modifica**.

### Monitorare i rischi

A partire da ONTAP 9.10.0, è possibile utilizzare Gestione di sistema per monitorare i rischi segnalati da Consulente digitale Active IQ. A partire da ONTAP 9.10.1, è possibile utilizzare Gestione di sistema per riconoscere i rischi.

Il consulente digitale NetApp Active IQ segnala le opportunità per ridurre i rischi e migliorare le performance e l'efficienza del tuo ambiente di storage. Con System Manager, puoi conoscere i rischi segnalati da Active IQ e ricevere informazioni utili per amministrare lo storage e ottenere una maggiore disponibilità, una maggiore sicurezza e migliori performance dello storage.

### Collegamento all'account Active IQ

Per ricevere informazioni sui rischi da Active IQ, devi prima collegarti al tuo account Active IQ da Gestione sistema.

#### Fasi

1. In System Manager, fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. In **registrazione Active IQ**, fare clic su **Registra**.
3. Immettere le credenziali per Active IQ.
4. Una volta autenticate le credenziali, fare clic su **Confirm (Conferma) per collegare Active IQ a Gestore di sistema**.

### Visualizza il numero di rischi

A partire da ONTAP 9.10.0, è possibile visualizzare dal dashboard di Gestione sistema il numero di rischi segnalati da Active IQ.

#### Prima di iniziare

È necessario stabilire una connessione da Gestore di sistema all'account Active IQ. Fare riferimento a [Collegamento all'account Active IQ](#).

## Fasi

1. In System Manager, fare clic su **Dashboard**.
2. Nella sezione **Health**, visualizzare il numero di rischi segnalati.



È possibile visualizzare informazioni più dettagliate su ciascun rischio facendo clic sul messaggio che indica il numero di rischi. Vedere [Visualizza i dettagli dei rischi](#).

## Visualizza i dettagli dei rischi

A partire da ONTAP 9.10.0, è possibile visualizzare da System Manager come i rischi segnalati da Active IQ sono classificati in base alle aree di impatto. È inoltre possibile visualizzare informazioni dettagliate su ciascun rischio segnalato, il suo potenziale impatto sul sistema e le azioni correttive che è possibile intraprendere.

### Prima di iniziare

È necessario stabilire una connessione da Gestore di sistema all'account Active IQ. Fare riferimento a [Collegamento all'account Active IQ](#).

## Fasi

1. Fare clic su **Eventi > tutti gli eventi**.
2. Nella sezione **Panoramica**, sotto **Active IQ Suggerimenti**, visualizzare il numero di rischi in ciascuna categoria di area di impatto. Le categorie di rischio includono:
  - Performance ed efficienza
  - Disponibilità e protezione
  - Capacità
  - Configurazione
  - Sicurezza
3. Fare clic sulla scheda **Active IQ Suggerimenti** per visualizzare informazioni su ciascun rischio, tra cui:
  - Livello di impatto sul sistema
  - Categoria del rischio
  - Nodi interessati
  - Tipo di mitigazione necessaria
  - Azioni correttive da intraprendere

## Riconoscere i rischi

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per riconoscere i rischi aperti.

## Fasi

1. In System Manager, visualizzare l'elenco dei rischi eseguendo la procedura descritta in [Visualizza i dettagli dei rischi](#).
2. Fare clic sul nome del rischio di un rischio aperto che si desidera riconoscere.
3. Inserire le informazioni nei seguenti campi:
  - Promemoria (data)
  - Giustificazione

- Commenti

#### 4. Fare clic su **Conferma**.



Dopo aver riconosciuto un rischio, sono necessari alcuni minuti per riflettere la modifica nell'elenco dei suggerimenti di Active IQ.

### Annullare il riconoscimento dei rischi

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per annullare qualsiasi rischio precedentemente riconosciuto.

#### Fasi

1. In System Manager, visualizzare l'elenco dei rischi eseguendo la procedura descritta in [Visualizza i dettagli dei rischi](#).
2. Fare clic sul nome del rischio riconosciuto che si desidera annullare.
3. Inserire le informazioni nei seguenti campi:
  - Giustificazione
  - Commenti
4. Fare clic su **Annulla riconoscimento**.



Una volta che si annulla la conferma di un rischio, sono necessari alcuni minuti affinché la modifica venga riflessa nell'elenco dei suggerimenti di Active IQ.

### Informazioni su System Manager

A partire da ONTAP 9.11.1, System Manager visualizza *informazioni* che consentono di ottimizzare le prestazioni e la sicurezza del sistema.



Per visualizzare, personalizzare e rispondere alle informazioni, fare riferimento a. "[Ottieni informazioni utili per ottimizzare il tuo sistema](#)"

### Informazioni sulla capacità

System Manager può visualizzare le seguenti informazioni in risposta alle condizioni di capacità del sistema:

| Insight | Severità | Condizione | Correzioni |
|---------|----------|------------|------------|
|---------|----------|------------|------------|

|                                                   |                              |                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gli strati locali sono privi di spazio            | Rimediare ai rischi          | Uno o più Tier locali sono pieni e in rapida crescita di oltre il 95%. È possibile che i carichi di lavoro esistenti non siano in grado di crescere o, in casi estremi, che i carichi di lavoro esistenti esauriscano lo spazio ed effettuino un errore.       | <p><b>Correzione consigliata:</b> Eseguire una delle seguenti opzioni.</p> <ul style="list-style-type: none"> <li>• Cancellare la coda di ripristino del volume.</li> <li>• Consentire il thin provisioning sui volumi con thick provisioning per liberare lo storage intrappolato.</li> <li>• Sposta i volumi in un altro Tier locale.</li> <li>• Elimina le copie Snapshot non necessarie.</li> <li>• Eliminare le directory o i file non necessari nei volumi.</li> <li>• Consenti a Fabric Pool di eseguire il tiering dei dati nel cloud.</li> </ul> |
| Le applicazioni mancano di spazio                 | Richiede attenzione          | Uno o più volumi sono pieni più del 95%, ma non hanno la funzione di crescita automatica attivata.                                                                                                                                                             | <p><b>Consigliato:</b> Consente di attivare la crescita automatica fino al 150% della capacità di corrente.</p> <p><b>Altre opzioni:</b></p> <ul style="list-style-type: none"> <li>• Recupera spazio eliminando le copie Snapshot.</li> <li>• Ridimensionare i volumi.</li> <li>• Eliminare directory o file.</li> </ul>                                                                                                                                                                                                                                 |
| La capacità del volume FlexGroup non è bilanciata | Ottimizzazione dello storage | Le dimensioni dei volumi costituenti di uno o più volumi FlexGroup sono cresciute in modo non uniforme nel tempo, portando a uno squilibrio nell'utilizzo della capacità. Se i volumi costituenti diventano pieni, potrebbero verificarsi errori di scrittura. | <p><b>Consigliato:</b> Riequilibrare i volumi FlexGroup.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|                                                               |                              |                                                                                                                                                                                                                                                     |                                                                                                |
|---------------------------------------------------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| La capacità delle macchine virtuali storage sta per esaurirsi | Ottimizzazione dello storage | Una o più macchine virtuali storage hanno una capacità quasi massima vicina a quella massima. Non sarà quindi possibile eseguire il provisioning di ulteriore spazio per volumi nuovi o esistenti se le Storage VM raggiungono la capacità massima. | <b>Consigliato:</b> Se possibile, aumentare il limite massimo di capacità della VM di storage. |
|---------------------------------------------------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|

## Informazioni sulla sicurezza

System Manager può visualizzare le seguenti informazioni in risposta a condizioni che potrebbero compromettere la sicurezza dei dati o del sistema.

| Insight                                                               | Severità            | Condizione                                                                       | Correzioni                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------|---------------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I volumi sono ancora in modalità di apprendimento anti-ransomware     | Richiede attenzione | Uno o più volumi sono in modalità di apprendimento anti-ransomware da 90 giorni. | <b>Consigliato:</b> Abilitare la modalità anti-ransomware attiva per questi volumi.                                                                                                                                                                                                                                                                                                                                                                                                               |
| L'eliminazione automatica delle copie Snapshot è abilitata sui volumi | Richiede attenzione | L'eliminazione automatica dello snapshot è abilitata su uno o più volumi.        | <b>Consigliato:</b> Disattiva l'eliminazione automatica delle copie Snapshot. In caso contrario, in caso di attacco ransomware, il recovery di dati per questi volumi potrebbe non essere possibile.                                                                                                                                                                                                                                                                                              |
| I volumi non dispongono di policy Snapshot                            | Richiede attenzione | Uno o più volumi non dispongono di una policy Snapshot adeguata.                 | <b>Consigliato:</b> Allegare un criterio Snapshot ai volumi che non ne hanno uno. In caso contrario, in caso di attacco ransomware, il recovery di dati per questi volumi potrebbe non essere possibile.                                                                                                                                                                                                                                                                                          |
| FPolicy nativo non è configurato                                      | Best practice       | FPolicy nativo non è configurato su una o più macchine virtuali storage NAS.     | <b>Consigliato: IMPORTANTE:</b> Il blocco delle estensioni potrebbe causare risultati imprevisti. A partire dal 9.11.1, puoi abilitare FPolicy nativa per le macchine virtuali storage, che blocca oltre 3000 estensioni dei file conosciute per essere utilizzate per gli attacchi ransomware. <a href="#">"Configurare FPolicy nativo"</a> Nelle macchine virtuali storage NAS per controllare le estensioni dei file consentite o non consentite per la scrittura sui volumi nel tuo ambiente. |

|                                                       |               |                                                                                                                                      |                                                                                                                                                                                                                                                          |
|-------------------------------------------------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telnet è attivato                                     | Best practice | Secure Shell (SSH) deve essere utilizzato per un accesso remoto sicuro.                                                              | <b>Consigliato:</b> Disattivare Telnet e utilizzare SSH per un accesso remoto sicuro.                                                                                                                                                                    |
| Sono stati configurati troppi server NTP              | Best practice | Il numero di server configurati per NTP è inferiore a 3.                                                                             | <b>Consigliato:</b> Associare al cluster almeno tre server NTP. In caso contrario, possono verificarsi problemi con la sincronizzazione dell'ora del cluster.                                                                                            |
| Remote Shell (RSH) è attivato                         | Best practice | Secure Shell (SSH) deve essere utilizzato per un accesso remoto sicuro.                                                              | <b>Consigliato:</b> Disabilitare RSH e utilizzare SSH per un accesso remoto sicuro.                                                                                                                                                                      |
| Banner di accesso non configurato                     | Best practice | I messaggi di accesso non sono configurati né per il cluster, né per la VM di storage, né per entrambi.                              | <b>Consigliato:</b> Configurare i banner di accesso per il cluster e la VM di storage e abilitarne l'utilizzo.                                                                                                                                           |
| AutoSupport sta utilizzando un protocollo non sicuro  | Best practice | AutoSupport non è configurato per comunicare tramite HTTPS.                                                                          | <b>Consigliato:</b> Si consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per inviare messaggi AutoSupport al supporto tecnico.                                                                                            |
| L'utente amministratore predefinito non è bloccato    | Best practice | Nessuno ha effettuato l'accesso utilizzando un account amministrativo predefinito (admin o diag) e questi account non sono bloccati. | <b>Consigliato:</b> Blocca gli account amministrativi predefiniti quando non vengono utilizzati.                                                                                                                                                         |
| Secure Shell (SSH) sta utilizzando cifrari non sicuri | Best practice | La configurazione corrente utilizza cifrari CBC non protetti.                                                                        | <b>Raccomandato:</b> Si dovrebbe consentire solo cifrari sicuri sul server web per proteggere la comunicazione sicura con i visitatori. Rimuovere i cifrari con nomi contenenti "cbc", ad esempio "ais128-cbc", "AES192-cbc", "AES256-cbc" e "3DES-cbc". |
| La compliance FIPS globale 140-2 è disattivata        | Best practice | La compliance FIPS globale 140-2 è disabilitata nel cluster.                                                                         | <b>Consigliato:</b> Per motivi di sicurezza, è necessario abilitare la crittografia globale conforme a FIPS 140-2 per garantire che ONTAP possa comunicare in modo sicuro con client o client server esterni.                                            |

|                                                                       |                     |                                                                                             |                                                                                                                                                                                               |
|-----------------------------------------------------------------------|---------------------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I volumi non vengono monitorati alla ricerca di attacchi ransomware   | Richiede attenzione | La funzionalità anti-ransomware è disabilitata su uno o più volumi.                         | <b>Consigliato:</b> Abilitare l'anti-ransomware sui volumi. In caso contrario, potresti non accorgerti quando i volumi sono minacciati o sotto attacco.                                       |
| Le macchine virtuali storage non sono configurate per anti-ransomware | Best practice       | Una o più macchine virtuali storage non sono configurate per la protezione anti-ransomware. | <b>Consigliato:</b> Abilitare l'anti-ransomware sulle macchine virtuali storage. Altrimenti, potresti non notare quando le macchine virtuali storage sono minacciate o sottoposte a attacchi. |

## Informazioni di configurazione

System Manager può visualizzare le seguenti informazioni in risposta ai problemi relativi alla configurazione del sistema.

| Insight                                                        | Severità      | Condizione                                                                                                                                                                                                                                | Correzioni                                                   |
|----------------------------------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Il cluster non è configurato per le notifiche                  | Best practice | Email, webhook o trapshot SNMP non sono configurati per consentirti di ricevere notifiche su problemi con il cluster.                                                                                                                     | <b>Consigliato:</b> Configurare le notifiche per il cluster. |
| Il cluster non è configurato per gli aggiornamenti automatici. | Best practice | Il cluster non è stato configurato in modo da ricevere aggiornamenti automatici per il pacchetto di qualifica del disco più recente, il firmware del disco, il firmware dello shelf e i file del firmware SP/BMC quando sono disponibili. | <b>Consigliato:</b> Attivare questa funzione.                |



|                                          |               |                                                                                                                                                                                                       |                                                   |
|------------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| Il firmware del cluster non è aggiornato | Best practice | Il sistema non dispone dell'ultimo aggiornamento del firmware che potrebbe avere miglioramenti, patch di sicurezza o nuove funzioni che consentono di proteggere il cluster per prestazioni migliori. | <b>Consigliato:</b> Aggiornare il firmware ONTAP. |
|------------------------------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|

## Ottieni informazioni utili per ottimizzare il tuo sistema

System Manager consente di visualizzare informazioni utili per ottimizzare il sistema.

### A proposito di questa attività

A partire da ONTAP 9.11.0, puoi visualizzare informazioni in System Manager che ti aiutano a ottimizzare la capacità e la conformità alla sicurezza del tuo sistema.

A partire da ONTAP 9.11.1, è possibile visualizzare informazioni aggiuntive che consentono di ottimizzare la capacità, la conformità alla sicurezza e la configurazione del sistema.



**Il blocco delle estensioni può causare risultati imprevisti.** a partire da ONTAP 9.11.1, è possibile abilitare FPolicy nativo per le VM di archiviazione utilizzando Gestione sistema. Potresti ricevere un messaggio di System Manager Insight che ti consiglia di farlo "[Configurare FPolicy nativo](#)" Per una macchina virtuale di storage.

Con la modalità nativa di FPolicy, è possibile consentire o negare estensioni di file specifiche. System Manager consiglia oltre 3000 estensioni di file non consentite che sono state utilizzate in precedenti attacchi ransomware. Alcune di queste estensioni potrebbero essere utilizzate da file legittimi nell'ambiente in uso e il loro blocco potrebbe causare problemi imprevisti.

Pertanto, si consiglia di modificare l'elenco delle estensioni per soddisfare le esigenze dell'ambiente. Fare riferimento a. "[Come rimuovere un'estensione di file da una configurazione FPolicy nativa creata da System Manager utilizzando System Manager per ricreare il criterio](#)".

Per ulteriori informazioni su FPolicy nativo, vedere "[Tipi di configurazione FPolicy](#)".

In base alle Best practice, queste informazioni vengono visualizzate su una pagina da cui è possibile avviare azioni immediate per ottimizzare il sistema. Per ulteriori informazioni su ciascuna analisi, vedere "[Informazioni su System Manager](#)".

## Visualizza informazioni sull'ottimizzazione





### Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.

La pagina **Insights** mostra gruppi di informazioni. Ciascun gruppo di informazioni potrebbe contenere uno o più elementi. Vengono visualizzati i seguenti gruppi:

- Ha bisogno della vostra attenzione
- Rimediare ai rischi
- Ottimizza il tuo storage

2. (Facoltativo) filtrare le informazioni visualizzate facendo clic sui seguenti pulsanti nell'angolo in alto a destra della pagina:

-  Visualizza le informazioni relative alla sicurezza.
-  Visualizza le informazioni relative alla capacità.
-  Visualizza le informazioni relative alla configurazione.
-  Visualizza tutte le informazioni.

## Rispondi alle informazioni per ottimizzare il tuo sistema

In System Manager, puoi rispondere alle informazioni spendendole, esplorando diversi modi per risolvere i problemi o avviando il processo per risolverli.

### Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. Passare il mouse su una panoramica per visualizzare i pulsanti per eseguire le seguenti azioni:
  - **Chiudi**: Elimina le informazioni dalla vista. Per “undisperdere” le informazioni, fare riferimento a [\[customize-settings-insights\]](#).
  - **Esplora**: Scopri i vari modi per risolvere il problema menzionato nelle informazioni. Questo pulsante viene visualizzato solo se è presente più di un metodo di correzione.
  - **Fix**: Avviare il processo di risoluzione del problema menzionato nelle informazioni. Verrà richiesto di confermare se si desidera intraprendere l'azione necessaria per applicare la correzione.




Alcune di queste azioni possono essere avviate da altre pagine in System Manager, ma la pagina **Insights** ti aiuta a ottimizzare le attività quotidiane, consentendoti di avviare questa azione da questa pagina.

## Personalizzare le impostazioni per ottenere informazioni dettagliate

Puoi personalizzare le informazioni che ti verranno notificate in System Manager.


### Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. Nell'angolo superiore destro della pagina, fare clic su , Quindi selezionare **Impostazioni**.
3. Nella pagina **Impostazioni**, verificare che le caselle di controllo accanto alle informazioni di cui si desidera ricevere la notifica siano selezionate. Se in precedenza si è respinto un dato Insight, è possibile “undischissarlo” verificando che sia presente un segno di spunta nella relativa casella di controllo.
4. Fare clic su **Save** (Salva).

## Esportare le informazioni come file PDF

Puoi esportare tutte le informazioni pertinenti come file PDF.

### Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. Nell'angolo superiore destro della pagina, fare clic su , Quindi selezionare **Esporta**.

## Configurare FPolicy nativo

A partire da ONTAP 9.11.1, quando ricevi un System Manager Insight che suggerisce l'implementazione di FPolicy nativo, puoi configurarlo sui volumi e sulle macchine virtuali di storage.

### Prima di iniziare

Quando si accede a informazioni su System Manager, in **Applica procedure consigliate**, potrebbe essere visualizzato un messaggio che indica che FPolicy nativo non è configurato.

Per ulteriori informazioni sui tipi di configurazione FPolicy, fare riferimento a. "[Tipi di configurazione FPolicy](#)".

### Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. In **Applica Best practice**, individuare **Native FPolicy non è configurato**.
3. Leggere il seguente messaggio prima di intraprendere un'azione:



**Il blocco delle estensioni può causare risultati imprevisti.** a partire da ONTAP 9.11.1, è possibile abilitare FPolicy nativo per le VM di archiviazione utilizzando Gestione sistema. Con la modalità nativa di FPolicy, è possibile consentire o negare estensioni di file specifiche. System Manager consiglia oltre 3000 estensioni di file non consentite che sono state utilizzate in precedenti attacchi ransomware. Alcune di queste estensioni potrebbero essere utilizzate da file legittimi nell'ambiente in uso e il loro blocco potrebbe causare problemi imprevisti.

Pertanto, si consiglia di modificare l'elenco delle estensioni per soddisfare le esigenze dell'ambiente. Fare riferimento a. "[Come rimuovere un'estensione di file da una configurazione FPolicy nativa creata da System Manager utilizzando System Manager per ricreare il criterio](#)".

4. Fare clic su **Correggi**.
5. Selezionare le macchine virtuali storage a cui si desidera applicare FPolicy native.
6. Per ogni VM di storage, seleziona i volumi che riceveranno FPolicy nativa.
7. Fare clic su **Configura**.

## Monitorare e gestire le performance del cluster utilizzando la CLI

## Panoramica sulla gestione e sul monitoraggio delle performance

È possibile impostare attività di gestione e monitoraggio delle performance di base e identificare e risolvere problemi comuni relativi alle performance.

È possibile utilizzare queste procedure per monitorare e gestire le prestazioni del cluster se si applicano le seguenti ipotesi:

- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Si desidera visualizzare lo stato del sistema e gli avvisi, monitorare le prestazioni del cluster ed eseguire l'analisi delle cause principali utilizzando Active IQ Unified Manager (precedentemente noto come gestore unificato di OnCommand), oltre all'interfaccia della riga di comando di ONTAP.
- Si sta utilizzando l'interfaccia della riga di comando di ONTAP per configurare la qualità del servizio (QoS) dello storage.

QoS è disponibile anche in System Manager, NSLM, Wfa, VSC (VMware Plug-in) e API.

- Si desidera installare Unified Manager utilizzando un'appliance virtuale invece di un'installazione basata su Linux o Windows.
- Si desidera utilizzare una configurazione statica piuttosto che DHCP per installare il software.
- È possibile accedere ai comandi ONTAP al livello di privilegio avanzato.
- Sei un amministratore del cluster con il ruolo di "amministratore".

### Informazioni correlate

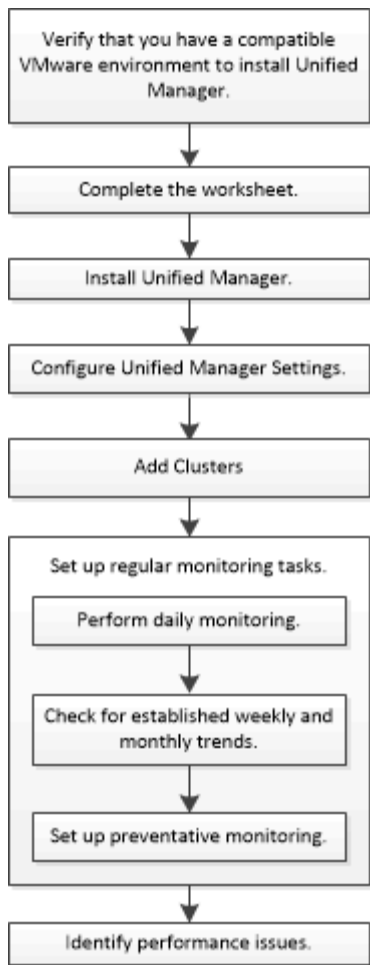
Se questi presupposti non sono corretti per la situazione, dovresti vedere le seguenti risorse:

- ["Installazione di Active IQ Unified Manager 9.8"](#)
- ["Amministrazione del sistema"](#)

## Monitorare le performance

### Panoramica del workflow di manutenzione e monitoraggio delle performance

Il monitoraggio e il mantenimento delle performance del cluster comportano l'installazione del software Active IQ Unified Manager, la configurazione di attività di monitoraggio di base, l'identificazione dei problemi di performance e la modifica secondo necessità.



### Verificare che l'ambiente VMware sia supportato

Per installare correttamente Active IQ Unified Manager, è necessario verificare che l'ambiente VMware soddisfi i requisiti necessari.

#### Fasi

1. Verificare che l'infrastruttura VMware soddisfi i requisiti di dimensionamento per l'installazione di Unified Manager.
2. Accedere alla ["Matrice di interoperabilità"](#) per verificare di disporre di una combinazione supportata dei seguenti componenti:
  - Versione di ONTAP
  - Versione del sistema operativo ESXi
  - Versione di VMware vCenter Server
  - Versione di VMware Tools
  - Tipo e versione del browser



Il ["Matrice di interoperabilità"](#) Elenca le configurazioni supportate per Unified Manager.

3. Fare clic sul nome della configurazione selezionata.

I dettagli della configurazione vengono visualizzati nella finestra Dettagli configurazione.

4. Esaminare le informazioni nelle seguenti schede:

- Note

Elenca avvisi e informazioni importanti specifici della configurazione.

- Policy e linee guida

Fornisce linee guida generali per tutte le configurazioni.

### Foglio di lavoro Active IQ Unified Manager

Prima di installare, configurare e connettere Active IQ Unified Manager, è necessario disporre di informazioni specifiche sull'ambiente in uso. È possibile registrare le informazioni nel foglio di lavoro.

#### Informazioni sull'installazione di Unified Manager

| Macchina virtuale su cui viene implementato il software | Il tuo valore |
|---------------------------------------------------------|---------------|
| Indirizzo IP del server ESXi                            |               |
| Nome di dominio completo dell'host                      |               |
| Host IP address (Indirizzo IP host)                     |               |
| Maschera di rete                                        |               |
| Indirizzo IP del gateway                                |               |
| Indirizzo DNS primario                                  |               |
| Indirizzo DNS secondario                                |               |
| Cerca domini                                            |               |
| Nome utente manutenzione                                |               |
| Password utente per la manutenzione                     |               |

#### Informazioni sulla configurazione di Unified Manager

| Impostazione                         | Il tuo valore |
|--------------------------------------|---------------|
| Indirizzo e-mail utente manutenzione |               |
| Server NTP                           |               |

|                                                       |                         |
|-------------------------------------------------------|-------------------------|
| Nome host o indirizzo IP del server SMTP              |                         |
| Nome utente SMTP                                      |                         |
| Password SMTP                                         |                         |
| Porta predefinita SMTP                                | 25 (valore predefinito) |
| E-mail da cui vengono inviate le notifiche di avviso  |                         |
| Nome distinto bind LDAP                               |                         |
| Password bind LDAP                                    |                         |
| Nome dell'amministratore di Active Directory          |                         |
| Password di Active Directory                          |                         |
| Nome distinto della base del server di autenticazione |                         |
| Nome host o indirizzo IP del server di autenticazione |                         |

#### Informazioni sul cluster

Acquisire le seguenti informazioni per ciascun cluster in Unified Manager.

| Cluster 1 di N.                                                                                                                                                                                          | Il tuo valore |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| Nome host o indirizzo IP di gestione del cluster                                                                                                                                                         |               |
| Nome utente amministratore di ONTAP<br><div>  All'amministratore deve essere stato assegnato il ruolo "admin". </div> |               |
| Password dell'amministratore di ONTAP                                                                                                                                                                    |               |
| Protocollo (HTTP o HTTPS)                                                                                                                                                                                |               |

#### Informazioni correlate

["Autenticazione amministratore e RBAC"](#)

#### Installare Active IQ Unified Manager

Per installare il software, è necessario scaricare il file di installazione dell'appliance virtuale (VA) e utilizzare un client VMware vSphere per implementare il file su un server VMware ESXi. Il VA è disponibile in un file OVA.

### Fasi

1. Accedere alla pagina **Download del software del sito di supporto NetApp** e individuare Active IQ Unified Manager.

<https://mysupport.netapp.com/products/index.html>

2. Selezionare **VMware vSphere** nel menu a discesa **Select Platform** e fare clic su **Go!**
3. Salvare il file "OVA" in una posizione locale o di rete accessibile al client VMware vSphere.
4. In VMware vSphere Client, fare clic su **file > Deploy OVF Template**.
5. Individuare il file "OVA" e utilizzare la procedura guidata per implementare l'appliance virtuale sul server ESXi.

È possibile utilizzare la scheda **Proprietà** della procedura guidata per immettere le informazioni di configurazione statiche.

6. Accendere la macchina virtuale.
7. Fare clic sulla scheda **Console** per visualizzare il processo di avvio iniziale.
8. Seguire le istruzioni per installare VMware Tools sulla macchina virtuale.
9. Configurare il fuso orario.
10. Immettere un nome utente e una password per la manutenzione.
11. Accedere all'URL visualizzato dalla console della macchina virtuale.

### Configurare le impostazioni Active IQ Unified Manager iniziali

La finestra di dialogo Configurazione iniziale di Active IQ Unified Manager viene visualizzata quando si accede per la prima volta all'interfaccia utente Web, che consente di configurare alcune impostazioni iniziali e aggiungere cluster.

### Fasi

1. Accettare l'impostazione predefinita AutoSupport Enabled (attivato).
2. Immettere i dettagli del server NTP, l'indirizzo e-mail dell'utente di manutenzione, il nome host del server SMTP e le opzioni SMTP aggiuntive, quindi fare clic su **Salva**.

### Al termine

Una volta completata la configurazione iniziale, viene visualizzata la pagina origini dati cluster, in cui è possibile aggiungere i dettagli del cluster.

### Specificare i cluster da monitorare

È necessario aggiungere un cluster a un server Active IQ Unified Manager per monitorare il cluster, visualizzare lo stato di rilevamento del cluster e monitorarne le prestazioni.



## Di cosa hai bisogno

- È necessario disporre delle seguenti informazioni:

- Nome host o indirizzo IP di gestione del cluster

Il nome host è il nome di dominio completo (FQDN, Fully Qualified Domain Name) o il nome breve utilizzato da Unified Manager per connettersi al cluster. Questo nome host deve essere risolto nell'indirizzo IP di gestione del cluster.

L'indirizzo IP di gestione del cluster deve essere la LIF di gestione del cluster della SVM (Administrative Storage Virtual Machine). Se si utilizza una LIF di gestione dei nodi, l'operazione non riesce.

- Nome utente e password dell'amministratore di ONTAP
- Tipo di protocollo (HTTP o HTTPS) che è possibile configurare sul cluster e numero di porta del cluster
- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- L'amministratore di ONTAP deve disporre dei ruoli di amministratore di ONTAPI e SSH.
- L'FQDN di Unified Manager deve essere in grado di eseguire il ping di ONTAP.

Per verificarlo, utilizzare il comando ONTAP `ping -node node_name -destination Unified_Manager_FQDN`.

## A proposito di questa attività

Per una configurazione MetroCluster, è necessario aggiungere i cluster locali e remoti e i cluster devono essere configurati correttamente.

## Fasi

1. Fare clic su **Configurazione > origini dati cluster**.
2. Dalla pagina Clusters, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Aggiungi cluster**, specificare i valori richiesti, ad esempio il nome host o l'indirizzo IP (IPv4 o IPv6) del cluster, il nome utente, la password, il protocollo di comunicazione e il numero di porta.

Per impostazione predefinita, il protocollo HTTPS è selezionato.

È possibile modificare l'indirizzo IP di gestione del cluster da IPv6 a IPv4 o da IPv4 a IPv6. Il nuovo indirizzo IP viene visualizzato nella griglia del cluster e nella pagina di configurazione del cluster al termine del successivo ciclo di monitoraggio.

4. Fare clic su **Aggiungi**.
5. Se si seleziona HTTPS, attenersi alla seguente procedura:
  - a. Nella finestra di dialogo **Authorize host** (autorizza host), fare clic su **View Certificate** (Visualizza certificato) per visualizzare le informazioni sul certificato del cluster.
  - b. Fare clic su **Sì**.

Unified Manager controlla il certificato solo quando il cluster viene aggiunto inizialmente, ma non lo controlla per ogni chiamata API a ONTAP.

Se il certificato è scaduto, non è possibile aggiungere il cluster. È necessario rinnovare il certificato SSL e aggiungere il cluster.

6. **Opzionale:** Visualizzazione dello stato di rilevamento del cluster:

a. Esaminare lo stato di rilevamento del cluster dalla pagina **Cluster Setup**.

Il cluster viene aggiunto al database di Unified Manager dopo l'intervallo di monitoraggio predefinito di circa 15 minuti.

## Impostare attività di monitoraggio di base

### Eeguire il monitoraggio giornaliero

È possibile eseguire il monitoraggio giornaliero per assicurarsi di non avere problemi immediati di performance che richiedono attenzione.

#### Fasi

1. Dall'interfaccia utente di Active IQ Unified Manager, accedere alla pagina **inventario eventi** per visualizzare tutti gli eventi correnti e obsoleti.
2. Dall'opzione **Visualizza**, selezionare `Active Performance Events` e determinare l'azione richiesta.

### Utilizza le tendenze delle performance settimanali e mensili per identificare i problemi di performance

L'identificazione delle tendenze delle performance può aiutarti a identificare se il cluster viene utilizzato in eccesso o sottoutilizzato analizzando la latenza del volume. È possibile utilizzare procedure simili per identificare i colli di bottiglia della CPU, della rete o di altri sistemi.

#### Fasi

1. Individuare il volume che si sospetta sia sottoutilizzato o utilizzato in eccesso.
2. Nella scheda **Dettagli volume**, fare clic su **30 d** per visualizzare i dati storici.
3. Nel menu a discesa "Interrompi dati per", selezionare **latenza**, quindi fare clic su **Invia**.
4. Deselezionare **aggregate** nella tabella di confronto dei componenti del cluster, quindi confrontare la latenza del cluster con il grafico della latenza del volume.
5. Selezionare **aggregate** e deselezionare tutti gli altri componenti nel grafico di confronto dei componenti del cluster, quindi confrontare la latenza aggregata con il grafico di latenza del volume.
6. Confrontare il grafico della latenza di lettura/scrittura con il grafico della latenza del volume.
7. Determinare se i carichi delle applicazioni client hanno causato un conflitto di carichi di lavoro e ribilanciare i carichi di lavoro in base alle necessità.
8. Determinare se l'aggregato è utilizzato in eccesso e causa conflitti e ribilanciare i carichi di lavoro in base alle necessità.

### Utilizza le soglie delle performance per generare notifiche di eventi

Gli eventi sono notifiche generate automaticamente da Active IQ Unified Manager quando si verifica una condizione predefinita o quando un valore del contatore delle prestazioni supera una soglia. Gli eventi consentono di identificare i problemi di performance nei cluster monitorati. È possibile configurare gli avvisi in modo che inviino automaticamente una notifica via email quando si verificano eventi di determinati tipi di gravità.

## Impostare le soglie delle performance

È possibile impostare soglie di performance per monitorare i problemi critici di performance. Le soglie definite dall'utente attivano un avviso o una notifica di eventi critici quando il sistema si avvicina o supera la soglia definita.

### Fasi

1. Creare le soglie degli eventi critici e di avviso:
  - a. Selezionare **Configurazione > soglie delle prestazioni**.
  - b. Fare clic su **Create** (Crea).
  - c. Selezionare il tipo di oggetto e specificare un nome e una descrizione del criterio.
  - d. Selezionare la condizione di contatore oggetti e specificare i valori limite che definiscono gli eventi di avviso e critici.
  - e. Selezionare il periodo di tempo in cui i valori limite devono essere violati per l'invio di un evento, quindi fare clic su **Salva**.
2. Assegnare il criterio di soglia all'oggetto di storage.
  - a. Accedere alla pagina Inventory (inventario) per lo stesso tipo di oggetto cluster selezionato in precedenza e scegliere **Performance** dall'opzione View (Visualizza).
  - b. Selezionare l'oggetto a cui si desidera assegnare il criterio di soglia, quindi fare clic su **Assegna criterio di soglia**.
  - c. Selezionare il criterio creato in precedenza, quindi fare clic su **Assegna policy**.

### Esempio

È possibile impostare soglie definite dall'utente per ottenere informazioni sui problemi critici relativi alle performance. Ad esempio, se si dispone di un Microsoft Exchange Server e si sa che si blocca se la latenza del volume supera i 20 millisecondi, è possibile impostare una soglia di avviso a 12 millisecondi e una soglia critica a 15 millisecondi. Con questa impostazione di soglia, è possibile ricevere notifiche quando la latenza del volume supera il limite.

|                           | Warning               |    | Critical |    |
|---------------------------|-----------------------|----|----------|----|
| Object Counter Condition* | Average Latency ms/op | 12 | ms/op    | 15 |

### Aggiungere avvisi

È possibile configurare gli avvisi in modo che notifichino quando viene generato un determinato evento. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un particolare tipo di severità. È possibile specificare la frequenza con cui si desidera ricevere una notifica e associare uno script all'avviso.

### Di cosa hai bisogno

- Per consentire al server Active IQ Unified Manager di utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento, è necessario aver configurato le impostazioni di notifica, ad esempio l'indirizzo e-mail dell'utente, il server SMTP e l'host trap SNMP.
- È necessario conoscere le risorse e gli eventi per i quali si desidera attivare l'avviso, nonché i nomi utente o gli indirizzi e-mail degli utenti che si desidera notificare.
- Se si desidera eseguire uno script in base all'evento, è necessario aggiungere lo script a Unified Manager

utilizzando la pagina script.

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

### A proposito di questa attività

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Configurazione avviso, come descritto di seguito.

### Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management > Alert Setup**.
2. Nella pagina **Alert Setup**, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Aggiungi avviso**, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.
4. Fare clic su **risorse** e selezionare le risorse da includere o escludere dall'avviso.

È possibile impostare un filtro specificando una stringa di testo nel campo **Nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse corrispondenti alla regola di filtro. La stringa di testo specificata fa distinzione tra maiuscole e minuscole.

Se una risorsa è conforme alle regole di inclusione ed esclusione specificate, la regola di esclusione ha la precedenza sulla regola di inclusione e l'avviso non viene generato per gli eventi correlati alla risorsa esclusa.

5. Fare clic su **Eventi** e selezionare gli eventi in base al nome dell'evento o al tipo di severità per cui si desidera attivare un avviso.



Per selezionare più eventi, premere il tasto Ctrl mentre si effettuano le selezioni.

6. Fare clic su **azioni**, selezionare gli utenti che si desidera notificare, scegliere la frequenza di notifica, scegliere se inviare una trap SNMP al ricevitore della trap e assegnare uno script da eseguire quando viene generato un avviso.



Se si modifica l'indirizzo di posta elettronica specificato per l'utente e si riapre l'avviso per la modifica, il campo Nome appare vuoto perché l'indirizzo di posta elettronica modificato non è più associato all'utente precedentemente selezionato. Inoltre, se l'indirizzo e-mail dell'utente selezionato è stato modificato dalla pagina utenti, l'indirizzo e-mail modificato non viene aggiornato per l'utente selezionato.

È inoltre possibile scegliere di inviare una notifica agli utenti tramite trap SNMP.

7. Fare clic su **Save** (Salva).

### Esempio di aggiunta di un avviso

Questo esempio mostra come creare un avviso che soddisfi i seguenti requisiti:

- Nome avviso: HealthTest
- Risorse: Include tutti i volumi il cui nome contiene "abc" ed esclude tutti i volumi il cui nome contiene "xyz"
- Eventi: Include tutti gli eventi sanitari critici
- Azioni: Include "sample@domain.com", uno script "Test" e l'utente deve ricevere una notifica ogni 15 minuti

Nella finestra di dialogo Aggiungi avviso, attenersi alla seguente procedura:

1. Fare clic su **Nome** e digitare `HealthTest` Nel campo **Nome avviso**.
2. Fare clic su **Resources** (risorse) e nella scheda include (Includi) selezionare **Volumes** (volumi) dall'elenco a discesa.
  - a. Invio `abc` Nel campo **Nome contiene** per visualizzare i volumi il cui nome contiene "abc".
  - b. Selezionare **<<All Volumes whose name contains 'abc'>>** dall'area risorse disponibili e spostarla nell'area risorse selezionate.
  - c. Fare clic su **Escludi** e digitare `xyz` Nel campo **Nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **critico** dal campo gravità evento.
4. Selezionare **All Critical Events** (tutti gli eventi critici) dall'area Matching Events (Eventi corrispondenti) e spostarla nell'area Selected Events (Eventi selezionati).
5. Fare clic su **azioni** e digitare `sample@domain.com` Nel campo Alert these users (Avvisa questi utenti).
6. Selezionare **promemoria ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

È possibile configurare un avviso per inviare ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario determinare l'ora in cui la notifica dell'evento è attiva per l'avviso.

7. Nel menu Select script to Execute (Seleziona script da eseguire), selezionare **Test script**.
8. Fare clic su **Save** (Salva).

#### Configurare le impostazioni degli avvisi

È possibile specificare quali eventi di Active IQ Unified Manager attivano gli avvisi, i destinatari e-mail degli avvisi e la frequenza degli stessi.

#### Di cosa hai bisogno

È necessario disporre del ruolo di amministratore dell'applicazione.

#### A proposito di questa attività

È possibile configurare impostazioni di avviso univoche per i seguenti tipi di eventi relativi alle prestazioni:

- Eventi critici attivati da violazioni di soglie definite dall'utente
- Eventi di avviso attivati da violazioni di soglie definite dall'utente, soglie definite dal sistema o soglie dinamiche

Per impostazione predefinita, gli avvisi e-mail vengono inviati agli utenti amministratori di Unified Manager per tutti i nuovi eventi. È possibile inviare avvisi e-mail ad altri utenti aggiungendo gli indirizzi e-mail di tali utenti.



Per disattivare l'invio di avvisi per determinati tipi di eventi, è necessario deselezionare tutte le caselle di controllo di una categoria di eventi. Questa azione non interrompe la visualizzazione degli eventi nell'interfaccia utente.

#### Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **Storage Management > Alert Setup**.

Viene visualizzata la pagina Alert Setup.

2. Fare clic su **Add** (Aggiungi) e configurare le impostazioni appropriate per ciascun tipo di evento.

Per inviare avvisi e-mail a più utenti, inserire una virgola tra ciascun indirizzo e-mail.

3. Fare clic su **Save** (Salva).

### Identificare i problemi di performance in Active IQ Unified Manager

Se si verifica un evento di performance, è possibile individuare l'origine del problema in Active IQ Unified Manager e utilizzare altri strumenti per risolverlo. È possibile ricevere una notifica via email di un evento o notarlo durante il monitoraggio giornaliero.

#### Fasi

1. Fare clic sul collegamento nella notifica e-mail, che consente di accedere direttamente all'oggetto di storage che ha un evento di performance.

| Se...                                                            | Quindi...                                                                                  |
|------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Ricevere una notifica via email di un evento                     | Fare clic sul collegamento per accedere direttamente alla pagina dei dettagli dell'evento. |
| Notare l'evento durante l'analisi della pagina inventario eventi | Selezionare l'evento per accedere direttamente alla pagina dei dettagli dell'evento.       |

2. Se l'evento ha superato una soglia definita dal sistema, seguire le azioni suggerite nell'interfaccia utente per risolvere il problema.
3. Se l'evento ha superato una soglia definita dall'utente, analizzarlo per determinare se è necessario intraprendere un'azione.
4. Se il problema persiste, verificare le seguenti impostazioni:
  - Impostazioni del protocollo sul sistema di storage
  - Impostazioni di rete su qualsiasi switch Ethernet o fabric
  - Impostazioni di rete sul sistema di storage
  - Layout dei dischi e metriche aggregate sul sistema storage
5. Se il problema persiste, contattare il supporto tecnico per assistenza.

### Utilizza il consulente digitale Active IQ per visualizzare le prestazioni del sistema

Per qualsiasi sistema ONTAP che invia la telemetria AutoSupport a NetApp, è possibile visualizzare dati completi sulle performance e sulla capacità. Active IQ mostra le performance del sistema in un periodo più lungo di quello che puoi vedere in Gestione sistema.

È possibile visualizzare grafici relativi a utilizzo della CPU, latenza, IOPS, IOPS in base al protocollo e throughput di rete. È inoltre possibile scaricare questi dati in formato .csv per l'analisi in altri strumenti.

Oltre a questi dati sulle performance, Active IQ può mostrarti l'efficienza dello storage in base al carico di lavoro e confrontarla con l'efficienza prevista per quel tipo di carico di lavoro. È possibile visualizzare le tendenze della capacità e visualizzare una stima della quantità di storage aggiuntivo che potrebbe essere

necessaria per aggiungere in un determinato intervallo di tempo.



- L'efficienza dello storage è disponibile a livello di cliente, cluster e nodo sul lato sinistro del dashboard principale.
- Le performance sono disponibili a livello di cluster e nodo sul lato sinistro del dashboard principale.

#### Informazioni correlate

- ["Documentazione di Active IQ Digital Advisor"](#)
- ["Playlist video di Active IQ Digital Advisor"](#)
- ["Portale web Active IQ"](#)

## Gestire i problemi di performance

### Workflow di gestione delle performance

Una volta identificato un problema di performance, è possibile eseguire alcuni controlli diagnostici di base dell'infrastruttura per escludere errori di configurazione evidenti. Se questi non individuano il problema, è possibile iniziare a esaminare i problemi di gestione del carico di lavoro.



### Eseguire controlli di base dell'infrastruttura

Verificare le impostazioni del protocollo sul sistema di storage

### Controllare le dimensioni massime di trasferimento TCP NFS

Per NFS, è possibile verificare se le dimensioni massime di trasferimento TCP per le operazioni di lettura e scrittura potrebbero causare problemi di performance. Se pensi che le dimensioni rallentino le performance, puoi aumentarle.



### Di cosa hai bisogno

- Per eseguire questa attività, è necessario disporre dei privilegi di amministratore del cluster.
- Per questa attività, è necessario utilizzare i comandi avanzati del livello di privilegio.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Verificare le dimensioni massime di trasferimento TCP:

```
vserver nfs show -vserver vserver_name -instance
```

3. Se la dimensione massima di trasferimento TCP è troppo piccola, aumentarne la dimensione:

```
vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
```

4. Tornare al livello di privilegi amministrativi:

```
set -privilege admin
```

### Esempio

Nell'esempio seguente viene modificata la dimensione massima di trasferimento TCP di SVM1 a 1048576:

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

### Controllare le dimensioni di lettura/scrittura TCP iSCSI

Per iSCSI, è possibile controllare le dimensioni di lettura/scrittura TCP per determinare se l'impostazione delle dimensioni sta creando un problema di prestazioni. Se le dimensioni sono la causa di un problema, è possibile correggerlo.

### Di cosa hai bisogno

Per questa attività sono necessari comandi avanzati del livello di privilegio.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Verificare l'impostazione delle dimensioni della finestra TCP:

```
vserver iscsi show -vserver vserver_name -instance
```

3. Modificare l'impostazione delle dimensioni della finestra TCP:

```
vserver iscsi modify -vserver vserver_name -tcp-window-size integer
```

4. Tornare al privilegio amministrativo:

```
set -privilege admin
```

### Esempio

Nell'esempio seguente viene modificata la dimensione della finestra TCP di SVM1 fino a 131,400 byte:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

### Controllare le impostazioni del multiplex CIFS

Se le prestazioni della rete CIFS lente causano un problema di performance, è possibile modificare le impostazioni multiplex per migliorarle e correggerle.

#### Fasi

1. Controllare l'impostazione del multiplex CIFS:

```
vserver cifs options show -vserver -vserver_name -instance
```

2. Modificare l'impostazione del multiplex CIFS:

```
vserver cifs options modify -vserver -vserver_name -max-mpx integer
```

### Esempio

Nell'esempio seguente viene modificato il numero massimo di multiplex SVM1 a 255:

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

### Controllare la velocità della porta dell'adattatore FC

La velocità della porta di destinazione dell'adattatore deve corrispondere alla velocità del dispositivo a cui si connette, per ottimizzare le prestazioni. Se la porta è impostata sulla negoziazione automatica, la riconnessione potrebbe richiedere più tempo dopo un takeover e un giveback o un'altra interruzione.

#### Di cosa hai bisogno

Tutte le LIF che utilizzano questo adattatore come porta home devono essere offline.

#### Fasi

1. Portare l'adattatore offline:

```
network fcp adapter modify -node nodename -adapter adapter -state down
```

2. Verificare la velocità massima dell'adattatore porta:

```
fcp adapter show -instance
```

3. Modificare la velocità della porta, se necessario:

```
network fcp adapter modify -node nodename -adapter adapter -speed  
{1|2|4|8|10|16|auto}
```

#### 4. Portare l'adattatore online:

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

#### 5. Porta online tutti i LIF dell'adattatore:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }  
-status-admin up
```

### Esempio

Nell'esempio seguente viene modificata la velocità della porta dell'adattatore 0d acceso node1 A 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

### Controllare le impostazioni di rete sugli switch dati

Sebbene sia necessario mantenere le stesse impostazioni MTU su client, server e sistemi di storage (ovvero endpoint di rete), i dispositivi di rete intermedi come NIC e switch devono essere impostati sui valori MTU massimi per garantire che le performance non vengano compromesse.

Per ottenere prestazioni ottimali, tutti i componenti della rete devono essere in grado di inoltrare frame jumbo (9000 byte IP, 9022 byte Ethernet inclusa). Gli switch dati devono essere impostati su almeno 9022 byte, ma con la maggior parte degli switch è possibile impostare un valore tipico di 9216.

### Procedura

Per i commutatori di dati, verificare che la dimensione MTU sia impostata su 9022 o superiore.

Per ulteriori informazioni, consultare la documentazione del fornitore dello switch.

### Controllare le impostazioni di rete MTU sul sistema di storage

È possibile modificare le impostazioni di rete sul sistema di storage se non corrispondono a quelle del client o di altri endpoint di rete. Mentre l'impostazione MTU della rete di gestione è impostata su 1500, la dimensione MTU della rete dati deve essere 9000.

### A proposito di questa attività

Tutte le porte all'interno di un dominio di broadcast hanno le stesse dimensioni MTU, ad eccezione del traffico di gestione della porta e0M. Se la porta fa parte di un dominio di broadcast, utilizzare `broadcast-domain modify` Per modificare la MTU per tutte le porte all'interno del dominio di trasmissione modificato.

Si noti che i dispositivi di rete intermedi, come NIC e switch dati, possono essere impostati su dimensioni MTU più elevate rispetto agli endpoint di rete. Per ulteriori informazioni, vedere ["Controllare le impostazioni di rete sugli switch dati"](#).

### Fasi

1. Verificare l'impostazione della porta MTU sul sistema di storage:

```
network port show -instance
```

2. Modificare l'MTU sul dominio di trasmissione utilizzato dalle porte:

```
network port broadcast-domain modify -ipspace ipspace -broadcast-domain  
broadcast_domain -mtu new_mtu
```

### Esempio

Nell'esempio seguente viene modificata l'impostazione della porta MTU su 9000:

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain  
Cluster -mtu 9000
```

### Controllare il throughput e la latenza dei dischi

È possibile controllare il throughput dei dischi e le metriche di latenza per i nodi del cluster per agevolare la risoluzione dei problemi.

#### A proposito di questa attività

Per questa attività sono necessari comandi avanzati del livello di privilegio.

#### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Controllare il throughput dei dischi e le metriche di latenza:

```
statistics disk show -sort-key latency
```

### Esempio

Nell'esempio seguente vengono visualizzati i totali di ciascuna operazione di lettura o scrittura dell'utente per node2 acceso cluster1:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
```

| Disk    | Node  | Busy (%) | Total Ops | Read Ops | Write Ops | Read (Bps) | Write (Bps) | *Latency (us) |
|---------|-------|----------|-----------|----------|-----------|------------|-------------|---------------|
| 1.10.20 | node2 | 4        | 5         | 3        | 2         | 95232      | 367616      | 23806         |
| 1.10.8  | node2 | 4        | 5         | 3        | 2         | 138240     | 386048      | 22113         |
| 1.10.6  | node2 | 3        | 4         | 2        | 2         | 48128      | 371712      | 19113         |
| 1.10.19 | node2 | 4        | 6         | 3        | 2         | 102400     | 443392      | 19106         |
| 1.10.11 | node2 | 4        | 4         | 2        | 2         | 122880     | 408576      | 17713         |

### Controllare il throughput e la latenza tra i nodi

È possibile utilizzare `network test-path` comando per identificare i colli di bottiglia della rete o per prequalificare i percorsi di rete tra i nodi. È possibile eseguire il comando tra nodi di intercluster o nodi intracluster.

#### Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono necessari comandi avanzati del livello di privilegio.
- Per un percorso intercluster, è necessario eseguire il peering dei cluster di origine e di destinazione.

#### A proposito di questa attività

Occasionalmente, le performance di rete tra i nodi potrebbero non soddisfare le aspettative per la configurazione del percorso. Una velocità di trasmissione di 1 Gbps per il tipo di trasferimenti di dati di grandi dimensioni, come ad esempio le operazioni di replica di SnapMirror, non sarebbe coerente con un collegamento a 10 GbE tra i cluster di origine e di destinazione.

È possibile utilizzare `network test-path` comando per misurare il throughput e la latenza tra i nodi. È possibile eseguire il comando tra nodi di intercluster o nodi intracluster.



Il test satura il percorso di rete con i dati, quindi è necessario eseguire il comando quando il sistema non è occupato e quando il traffico di rete tra i nodi non è eccessivo. Il test si esaurisce dopo dieci secondi. Il comando può essere eseguito solo tra i nodi ONTAP 9.

Il `session-type` L'opzione identifica il tipo di operazione in esecuzione sul percorso di rete, ad esempio "AsyncMirrorRemote" per la replica di SnapMirror su una destinazione remota. Il tipo determina la quantità di dati utilizzati nel test. La seguente tabella definisce i tipi di sessione:

| Tipo di sessione | Descrizione                                                         |
|------------------|---------------------------------------------------------------------|
| AsyncMirrorLocal | Impostazioni utilizzate da SnapMirror tra nodi nello stesso cluster |

|                    |                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AsyncMirrorRemote  | Impostazioni utilizzate da SnapMirror tra nodi in cluster diversi (tipo predefinito)                                                                                                          |
| RemoteDataTransfer | Impostazioni utilizzate da ONTAP per l'accesso remoto ai dati tra nodi nello stesso cluster (ad esempio, una richiesta NFS a un nodo per un file memorizzato in un volume su un nodo diverso) |

## Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Misurare il throughput e la latenza tra i nodi:

```
network test-path -source-node source_nodename |local -destination-cluster
destination_clustername -destination-node destination_nodename -session-type
Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
```

Il nodo di origine deve trovarsi nel cluster locale. Il nodo di destinazione può trovarsi nel cluster locale o in un cluster peered. Un valore "locale" per `-source-node` specifica il nodo su cui si esegue il comando.

Il seguente comando misura il throughput e la latenza per le operazioni di replica di tipo SnapMirror tra `node1` sul cluster locale e `node3` acceso `cluster2`:

```
cluster1::> network test-path -source-node node1 -destination-cluster
cluster2 -destination-node node3 -session-type AsyncMirrorRemote
Test Duration:      10.88 secs
Send Throughput:    18.23 MB/sec
Receive Throughput: 18.23 MB/sec
MB sent:            198.31
MB received:        198.31
Avg latency in ms:  2301.47
Min latency in ms:  61.14
Max latency in ms:  3056.86
```

3. Tornare al privilegio amministrativo:

```
set -privilege admin
```

## Al termine

Se le performance non soddisfano le aspettative per la configurazione del percorso, è necessario controllare le statistiche delle performance del nodo, utilizzare gli strumenti disponibili per isolare il problema nella rete, controllare le impostazioni dello switch e così via.

## Gestire i carichi di lavoro

## Identificare la capacità di performance rimanente

La capacità delle performance, o *headroom*, misura la quantità di lavoro che è possibile posizionare su un nodo o su un aggregato prima che le performance dei carichi di lavoro sulla risorsa comincino ad essere influenzate dalla latenza. La conoscenza della capacità di performance disponibile nel cluster consente di eseguire il provisioning e bilanciare i carichi di lavoro.

### Di cosa hai bisogno

Per questa attività sono necessari comandi avanzati del livello di privilegio.

### A proposito di questa attività

È possibile utilizzare i seguenti valori per `-object` opzione per raccogliere e visualizzare le statistiche di headroom:

- Per CPU, `resource_headroom_cpu`.
- Per gli aggregati, `resource_headroom_aggr`.

È inoltre possibile completare questa attività utilizzando Gestione di sistema e Active IQ Unified Manager.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Avvia la raccolta di statistiche in tempo reale:

```
statistics start -object resource_headroom_cpu|aggr
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

3. Visualizzare in tempo reale le informazioni statistiche di headroom:

```
statistics show -object resource_headroom_cpu|aggr
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

4. Tornare al privilegio amministrativo:

```
set -privilege admin
```

### Esempio

Nell'esempio seguente vengono visualizzate le statistiche medie orarie del headroom per i nodi del cluster.

È possibile calcolare la capacità di performance disponibile per un nodo sottraendo `current_utilization` contatore da `optimal_point_utilization` contatore. In questo esempio, la capacità di utilizzo per CPU\_sti2520-213 È -14% (72%-86%), il che suggerisce che la CPU è stata in media utilizzata in eccesso nell'ultima ora.

Potrebbe essere stato specificato `ewma_daily`, `ewma_weekly`, o `ewma_monthly` ottenere le stesse informazioni in media per periodi di tempo più lunghi.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
(statistics show)
```

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213
```

| Counter                         | Value |
|---------------------------------|-------|
| -----                           | ----- |
| ewma_hourly                     | -     |
| current_ops                     | 4376  |
| current_latency                 | 37719 |
| current_utilization             | 86    |
| optimal_point_ops               | 2573  |
| optimal_point_latency           | 3589  |
| optimal_point_utilization       | 72    |
| optimal_point_confidence_factor | 1     |

```
Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214
```

| Counter                         | Value |
|---------------------------------|-------|
| -----                           | ----- |
| ewma_hourly                     | -     |
| current_ops                     | 0     |
| current_latency                 | 0     |
| current_utilization             | 0     |
| optimal_point_ops               | 0     |
| optimal_point_latency           | 0     |
| optimal_point_utilization       | 71    |
| optimal_point_confidence_factor | 1     |

2 entries were displayed.

#### Identificare i client o i file ad alto traffico

È possibile utilizzare la tecnologia ONTAP Active Objects per identificare client o file responsabili di una quantità sproporzionata di traffico cluster. Una volta identificati questi file o client "top", è possibile ribilanciare i carichi di lavoro del cluster o intraprendere altre azioni per risolvere il problema.



## Di cosa hai bisogno

Per eseguire questa attività, è necessario essere un amministratore del cluster.

## Fasi

### 1. Visualizzare i principali client che accedono al cluster:

```
statistics top client show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

Per la sintassi completa dei comandi, vedere la pagina [man](#).

Il seguente comando visualizza i principali client che accedono cluster1:

```
cluster1::> statistics top client show
```

```
cluster1 : 3/23/2016 17:59:10
```

| Client         | Vserver | Node         | Protocol | *Total<br>Ops |
|----------------|---------|--------------|----------|---------------|
| -----          | -----   | -----        | -----    | -----         |
| 172.17.180.170 | vs4     | siderop1-vs4 | nfs      | 668           |
| 172.17.180.169 | vs3     | siderop1-vs3 | nfs      | 337           |
| 172.17.180.171 | vs3     | siderop1-vs3 | nfs      | 142           |
| 172.17.180.170 | vs3     | siderop1-vs3 | nfs      | 137           |
| 172.17.180.123 | vs3     | siderop1-vs3 | nfs      | 137           |
| 172.17.180.171 | vs4     | siderop1-vs4 | nfs      | 95            |
| 172.17.180.169 | vs4     | siderop1-vs4 | nfs      | 92            |
| 172.17.180.123 | vs4     | siderop1-vs4 | nfs      | 92            |
| 172.17.180.153 | vs3     | siderop1-vs3 | nfs      | 0             |

### 2. Visualizzare i file principali a cui si accede dal cluster:

```
statistics top file show -node node_name -sort-key sort_column -interval  
seconds_between_updates -iterations iterations -max number_of_instances
```

Per la sintassi completa dei comandi, vedere la pagina [man](#).

Il seguente comando visualizza i file principali a cui si accede cluster1:

```
cluster1::> statistics top file show
```

```
cluster1 : 3/23/2016 17:59:10
```

|                          |       |        | *Total       |       |       |
|--------------------------|-------|--------|--------------|-------|-------|
|                          | File  | Volume | Vserver      | Node  | Ops   |
| -----                    | ----- | -----  | -----        | ----- | ----- |
| /vol/vol1/vm170-read.dat | vol1  | vs4    | siderop1-vs4 | 22    |       |
| /vol/vol1/vm69-write.dat | vol1  | vs3    | siderop1-vs3 | 6     |       |
| /vol/vol2/vm171.dat      | vol2  | vs3    | siderop1-vs3 | 2     |       |
| /vol/vol2/vm169.dat      | vol2  | vs3    | siderop1-vs3 | 2     |       |
| /vol/vol2/p123.dat       | vol2  | vs4    | siderop1-vs4 | 2     |       |
| /vol/vol2/p123.dat       | vol2  | vs3    | siderop1-vs3 | 2     |       |
| /vol/vol1/vm171.dat      | vol1  | vs4    | siderop1-vs4 | 2     |       |
| /vol/vol1/vm169.dat      | vol1  | vs4    | siderop1-vs4 | 2     |       |
| /vol/vol1/vm169.dat      | vol1  | vs4    | siderop1-vs3 | 2     |       |
| /vol/vol1/p123.dat       | vol1  | vs4    | siderop1-vs4 | 2     |       |

## Throughput garantito con QoS

### Garantire il throughput con la panoramica QoS

È possibile utilizzare la qualità del servizio (QoS) dello storage per garantire che le performance dei carichi di lavoro critici non vengano degradate dai carichi di lavoro concorrenti. È possibile impostare un *soffitto* di throughput su un carico di lavoro concorrente per limitarne l'impatto sulle risorse di sistema o impostare un *piano* di throughput per un carico di lavoro critico, garantendo che soddisfi gli obiettivi di throughput minimi, indipendentemente dalla domanda dei carichi di lavoro concorrenti. È anche possibile impostare un soffitto e un pavimento per lo stesso carico di lavoro.

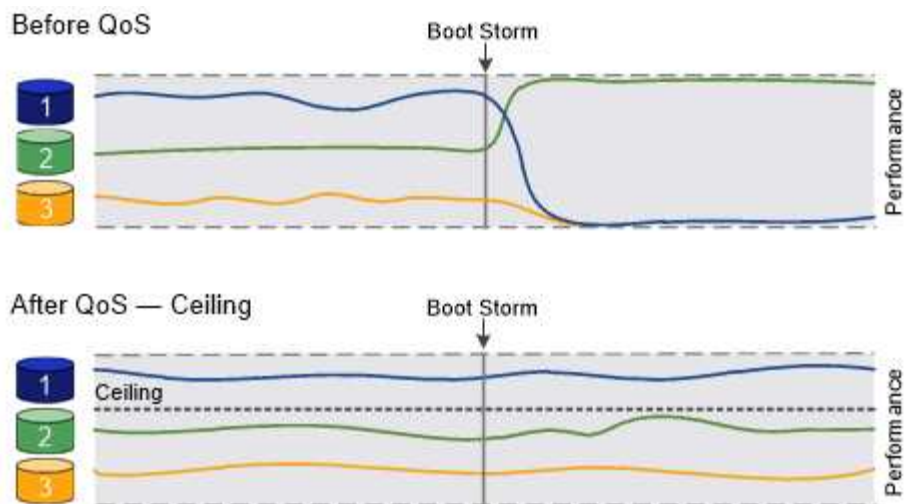
### Informazioni sui limiti di throughput (QoS Max)

Un limite massimo di throughput limita il throughput per un carico di lavoro a un numero massimo di IOPS o Mbps o IOPS e Mbps. Nella figura riportata di seguito, il limite massimo di throughput per il carico di lavoro 2 garantisce che i carichi di lavoro 1 e 3 non siano "ingombrati".

Un *gruppo di policy* definisce il limite massimo di throughput per uno o più carichi di lavoro. Un carico di lavoro rappresenta le operazioni di i/o per un *oggetto storage*: volume, file, qtree o LUN o tutti i volumi, file, qtree o LUN di una SVM. È possibile specificare il limite massimo quando si crea il gruppo di criteri oppure attendere che i carichi di lavoro vengano monitorati per specificarlo.



Il throughput per i carichi di lavoro potrebbe superare il limite massimo specificato fino al 10%, soprattutto se un carico di lavoro subisce rapidi cambiamenti nel throughput. Il limite massimo potrebbe essere superato fino al 50% per gestire i burst. I burst si verificano su singoli nodi quando i token accumulano fino al 150%



### Informazioni sui piani di throughput (QoS min)

Un piano di throughput garantisce che il throughput per un carico di lavoro non scenda al di sotto di un numero minimo di IOPS o Mbps o IOPS e Mbps. Nella figura riportata di seguito, i livelli di throughput per il carico di lavoro 1 e il carico di lavoro 3 garantiscono il raggiungimento degli obiettivi di throughput minimi, indipendentemente dalla domanda per carico di lavoro 2.



Come suggeriscono gli esempi, un limite di throughput rallenta direttamente il throughput. Un piano di throughput rallenta indirettamente il throughput, dando priorità ai carichi di lavoro per i quali è stato impostato il piano.

È possibile specificare il piano di lavoro quando si crea il gruppo di policy oppure attendere fino a quando non si monitorano i carichi di lavoro per specificarlo.

A partire da ONTAP 9.13.1, è possibile impostare i piani di throughput nell'ambito SVM con [\[adaptive-qos-templates\]](#). Nelle versioni di ONTAP precedenti alla 9.13.1, un gruppo di criteri che definisce un piano di throughput non può essere applicato a una SVM.



Nelle versioni precedenti a ONTAP 9.7, i piani di throughput sono garantiti quando è disponibile una capacità di performance sufficiente.

In ONTAP 9.7 e versioni successive, è possibile garantire il throughput anche quando la capacità delle performance è insufficiente. Questo nuovo comportamento si chiama Floors v2. Per soddisfare le garanzie, floors v2 può comportare una latenza maggiore sui carichi di lavoro senza un piano di throughput o sul lavoro che supera le impostazioni di base. Floors v2 si applica sia alla QoS che alla QoS adattiva.

L'opzione di attivazione/disattivazione del nuovo comportamento dei piani v2 è disponibile in ONTAP 9.7P6 e versioni successive. Un carico di lavoro potrebbe scendere al di sotto del piano specificato durante operazioni critiche come `volume move trigger-cutover`. Anche quando è disponibile una capacità sufficiente e non si svolgono operazioni critiche, il throughput di un workload potrebbe scendere al di sotto del piano specificato fino al 5%. Se il provisioning dei piani è eccessivo e non esiste una capacità di performance, alcuni carichi di lavoro potrebbero scendere al di sotto del piano specificato.



### Informazioni sui gruppi di policy QoS condivisi e non condivisi

A partire da ONTAP 9.4, è possibile utilizzare un gruppo di policy di qualità del servizio *non-shared* per specificare che il limite di throughput definito o il piano si applica a ogni singolo carico di lavoro membro. Il comportamento dei gruppi di policy *shared* dipende dal tipo di policy:

- Per i limiti di throughput, il throughput totale per i carichi di lavoro assegnati al gruppo di criteri condivisi non può superare il limite massimo specificato.
- Per i piani di throughput, il gruppo di policy condiviso può essere applicato solo a un singolo workload.

### Informazioni su QoS adattiva

Normalmente, il valore del gruppo di criteri assegnato a un oggetto di storage è fisso. È necessario modificare il valore manualmente quando la dimensione dell'oggetto di storage cambia. Un aumento della quantità di spazio utilizzata su un volume, ad esempio, richiede solitamente un aumento corrispondente del limite di throughput specificato per il volume.

QoS *adattiva* scala automaticamente il valore del gruppo di policy in base alle dimensioni del carico di lavoro, mantenendo il rapporto tra IOPS e TB|GB in base alle dimensioni del carico di lavoro. Si tratta di un vantaggio significativo quando si gestiscono centinaia o migliaia di carichi di lavoro in un'implementazione di grandi dimensioni.

In genere, si utilizza la QoS adattiva per regolare i limiti di throughput, ma è anche possibile utilizzarla per gestire i piani di throughput (quando le dimensioni del carico di lavoro aumentano). La dimensione del carico di lavoro viene espressa come spazio allocato per l'oggetto di storage o come spazio utilizzato dall'oggetto di storage.



Lo spazio utilizzato è disponibile per i piani di throughput in ONTAP 9.5 e versioni successive. Non è supportato per i piani di throughput in ONTAP 9.4 e versioni precedenti.

- Una policy di *spazio allocato* mantiene il rapporto IOPS/TB|GB in base alle dimensioni nominali dell'oggetto di storage. Se il rapporto è di 100 IOPS/GB, un volume da 150 GB avrà un limite di throughput di 15,000 IOPS, a condizione che il volume rimanga tale. Se il volume viene ridimensionato a 300 GB, la QoS adattiva regola il limite di throughput a 30,000 IOPS.
- Una policy *used space* (predefinita) mantiene il rapporto IOPS/TB|GB in base alla quantità di dati effettivi memorizzati prima dell'efficienza dello storage. Se il rapporto è di 100 IOPS/GB, un volume da 150 GB con 100 GB di dati memorizzati avrebbe un limite massimo di throughput di 10,000 IOPS. Man mano che la quantità di spazio utilizzato cambia, la QoS adattiva regola il limite di throughput in base al rapporto.

A partire da ONTAP 9.5, è possibile specificare una dimensione del blocco i/o per l'applicazione in uso che consenta di esprimere un limite di throughput in IOPS e Mbps. Il limite Mbps viene calcolato moltiplicando le dimensioni del blocco per il limite IOPS. Ad esempio, una dimensione del blocco i/o di 32K per un limite IOPS di 6144 IOPS/TB produce un limite di Mbps di 192 MBps.

È possibile prevedere il seguente comportamento sia per i limiti di throughput che per i piani:

- Quando un carico di lavoro viene assegnato a un gruppo di policy QoS adattivi, il soffitto o il piano vengono aggiornati immediatamente.
- Quando un carico di lavoro in un gruppo di policy QoS adattiva viene ridimensionato, il soffitto o il piano viene aggiornato in circa cinque minuti.

Il throughput deve aumentare di almeno 10 IOPS prima di eseguire gli aggiornamenti.

I gruppi di policy di QoS adattivi non sono sempre condivisi: Il limite di throughput definito o il piano si applica a ciascun carico di lavoro membro singolarmente.

A partire da ONTAP 9.6, i piani di throughput sono supportati da ONTAP Select Premium con SSD.

### Modello di gruppo di policy adattive

A partire da ONTAP 9.13.1, è possibile impostare un modello QoS adattivo su una SVM. I modelli di gruppi di policy adattivi consentono di impostare i livelli e i limiti di throughput per tutti i volumi in una SVM.

È possibile impostare i modelli di gruppi di criteri adattivi solo dopo la creazione di SVM. Utilizzare `vserver modify` con il `-qos-adaptive-policy-group-template` parametro per impostare il criterio.

Quando si imposta un modello di gruppo di criteri adattivi, i volumi creati o migrati dopo l'impostazione del criterio ereditano automaticamente il criterio. Gli eventuali volumi presenti nella SVM non vengono influenzati quando si assegna il modello di policy. Se si disattiva il criterio su SVM, qualsiasi volume successivamente migrato o creato su SVM non riceverà il criterio. La disattivazione del modello di gruppo di criteri adattivi non influisce sui volumi che hanno ereditato il modello di criteri, poiché conservano il modello di criteri.

Per ulteriori informazioni, vedere [Impostare un modello di gruppo di criteri adattivi](#).

### Supporto generale

La seguente tabella mostra le differenze nel supporto per i limiti di throughput, i piani di throughput e la QoS adattiva.

| Risorsa o funzione  | Limite di throughput | Piano di throughput                                                                                             | Throughput floor v2                                                                                         | QoS adattiva              |
|---------------------|----------------------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|---------------------------|
| Versione di ONTAP 9 | Tutto                | 9.2 e versioni successive                                                                                       | 9.7 e versioni successive                                                                                   | 9.3 e versioni successive |
| Piattaforme         | Tutto                | <ul style="list-style-type: none"><li>• AFF</li><li>• C190 *</li><li>• ONTAP Select premium con SSD *</li></ul> | <ul style="list-style-type: none"><li>• AFF</li><li>• C190</li><li>• ONTAP Select Premium con SSD</li></ul> | Tutto                     |

| Risorsa o funzione  | Limite di throughput | Piano di throughput                                                                   | Throughput floor v2                                                                   | QoS adattiva |
|---------------------|----------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|--------------|
| Protocolli          | Tutto                | Tutto                                                                                 | Tutto                                                                                 | Tutto        |
| FabricPool          | Sì                   | Sì, se la policy di tiering è impostata su "nessuno" e non ci sono blocchi nel cloud. | Sì, se la policy di tiering è impostata su "nessuno" e non ci sono blocchi nel cloud. | No           |
| SnapMirror sincrono | Sì                   | No                                                                                    | No                                                                                    | Sì           |

Il supporto di C190 e ONTAP Select è iniziato con la release ONTAP 9.6.

### Carichi di lavoro supportati per i limiti di throughput

La tabella seguente mostra il supporto dei workload per i limiti di throughput per la versione di ONTAP 9. I volumi root, i mirror di condivisione del carico e i mirror di protezione dei dati non sono supportati.

| Supporto del carico di lavoro - soffitto        | ONTAP 9.0 | ONTAP 9.1 | ONTAP 9.2 | ONTAP 9.3 | ONTAP 9.4 - 9.7 | ONTAP 9.8 e versioni successive |
|-------------------------------------------------|-----------|-----------|-----------|-----------|-----------------|---------------------------------|
| Volume                                          | sì        | sì        | sì        | sì        | sì              | sì                              |
| File                                            | sì        | sì        | sì        | sì        | sì              | sì                              |
| LUN                                             | sì        | sì        | sì        | sì        | sì              | sì                              |
| SVM                                             | sì        | sì        | sì        | sì        | sì              | sì                              |
| Volume FlexGroup                                | no        | no        | no        | sì        | sì              | sì                              |
| qtree*                                          | no        | no        | no        | no        | no              | sì                              |
| Carichi di lavoro multipli per gruppo di policy | sì        | sì        | sì        | sì        | sì              | sì                              |
| Gruppi di criteri non condivisi                 | no        | no        | no        | no        | sì              | sì                              |

A partire da ONTAP 9.8, l'accesso NFS è supportato nei qtree dei volumi FlexVol e FlexGroup con NFS attivato. A partire da ONTAP 9.9.1, l'accesso SMB è supportato anche nei qtree dei volumi FlexVol e

FlexGroup con SMB attivato.

### Carichi di lavoro supportati per i piani di throughput

La seguente tabella mostra il supporto dei workload per i piani di throughput in base alla versione di ONTAP 9. I volumi root, i mirror di condivisione del carico e i mirror di protezione dei dati non sono supportati.

| Supporto del workload - floor                   | ONTAP 9.2 | ONTAP 9.3 | ONTAP 9.4 - 9.7 | ONTAP 9.8 - 9.13.0 | ONTAP 9.13.1 e versioni successive |
|-------------------------------------------------|-----------|-----------|-----------------|--------------------|------------------------------------|
| Volume                                          | sì        | sì        | sì              | sì                 | sì                                 |
| File                                            | no        | sì        | sì              | sì                 | sì                                 |
| LUN                                             | sì        | sì        | sì              | sì                 | sì                                 |
| SVM                                             | no        | no        | no              | no                 | sì                                 |
| Volume FlexGroup                                | no        | no        | sì              | sì                 | sì                                 |
| qtree *                                         | no        | no        | no              | sì                 | sì                                 |
| Carichi di lavoro multipli per gruppo di policy | no        | no        | sì              | sì                 | sì                                 |
| Gruppi di criteri non condivisi                 | no        | no        | sì              | sì                 | sì                                 |

A partire da ONTAP 9.8, l'accesso NFS è supportato nei qtree dei volumi FlexVol e FlexGroup con NFS attivato. A partire da ONTAP 9.9.1, l'accesso SMB è supportato anche nei qtree dei volumi FlexVol e FlexGroup con SMB attivato.

### Carichi di lavoro supportati per QoS adattiva

La seguente tabella mostra il supporto dei carichi di lavoro per la QoS adattiva in base alla versione di ONTAP 9. I volumi root, i mirror di condivisione del carico e i mirror di protezione dei dati non sono supportati.

| Supporto del carico di lavoro - QoS adattiva    | ONTAP 9.3 | ONTAP 9.4 - 9.13.0 | ONTAP 9.13.1 e versioni successive |
|-------------------------------------------------|-----------|--------------------|------------------------------------|
| Volume                                          | sì        | sì                 | sì                                 |
| File                                            | no        | sì                 | sì                                 |
| LUN                                             | no        | sì                 | sì                                 |
| SVM                                             | no        | no                 | sì                                 |
| Volume FlexGroup                                | no        | sì                 | sì                                 |
| Carichi di lavoro multipli per gruppo di policy | sì        | sì                 | sì                                 |
| Gruppi di criteri non condivisi                 | sì        | sì                 | sì                                 |

## Numero massimo di workload e gruppi di policy

La seguente tabella mostra il numero massimo di workload e gruppi di policy per versione di ONTAP 9.

| Supporto dei carichi di lavoro        | ONTAP 9.3 e versioni precedenti | ONTAP 9.4 e versioni successive |
|---------------------------------------|---------------------------------|---------------------------------|
| Carichi di lavoro massimi per cluster | 12,000                          | 40,000                          |
| Carichi di lavoro massimi per nodo    | 12,000                          | 40,000                          |
| Numero massimo di gruppi di criteri   | 12,000                          | 12,000                          |

## Attiva o disattiva i piani di throughput v2

È possibile attivare o disattivare il throughput floors v2 su AFF. L'impostazione predefinita è Enabled (attivato). Con FLOors v2 abilitato, è possibile soddisfare i piani di throughput quando i controller vengono utilizzati in modo pesante a scapito di una maggiore latenza su altri carichi di lavoro. Floors v2 si applica sia a QoS che a QoS adattivo.

### Fasi

1. Passare al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Immettere uno dei seguenti comandi:

| Se si desidera...    | Utilizzare questo comando:                                   |
|----------------------|--------------------------------------------------------------|
| Disattiva piani v2   | <code>qos settings throughput-floors-v2 -enable false</code> |
| Abilitare i piani v2 | <code>qos settings throughput-floors-v2 -enable true</code>  |



Per disattivare il throughput floors v2 in un cluster MetroCluster, è necessario eseguire

```
qos settings throughput-floors-v2 -enable false
```

comando sui cluster di origine e di destinazione.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

## Workflow di QoS dello storage

Se si conoscono già i requisiti di performance per i carichi di lavoro che si desidera gestire con QoS, è possibile specificare il limite di throughput quando si crea il gruppo di



policy. In caso contrario, è possibile attendere fino a quando non si monitorano i carichi di lavoro per specificare il limite.

## Impostare un limite massimo di throughput con QoS

È possibile utilizzare `max-throughput` Campo per un gruppo di criteri per definire un limite massimo di throughput per i carichi di lavoro degli oggetti di storage (QoS Max). È possibile applicare il gruppo di criteri quando si crea o si modifica l'oggetto di storage.

### Di cosa hai bisogno

- Per creare un gruppo di criteri, è necessario essere un amministratore del cluster.
- Per applicare un gruppo di criteri a una SVM, è necessario essere un amministratore del cluster.

### A proposito di questa attività

- A partire da ONTAP 9.4, è possibile utilizzare un gruppo di policy di qualità del servizio *non-shared* per specificare che il limite di throughput definito si applica a ogni singolo carico di lavoro membro. In caso contrario, il gruppo di criteri è *shared*: il throughput totale per i carichi di lavoro assegnati al gruppo di criteri non può superare il limite massimo specificato.

Impostare `-is-shared=false` per `qos policy-group create` per specificare un gruppo di politiche non condiviso.

- È possibile specificare il limite di throughput per il limite massimo in IOPS, MB/s o IOPS, MB/s. Se si specificano IOPS e MB/s, viene applicato il limite raggiunto per primo.



Se si impostano un soffitto e un pavimento per lo stesso carico di lavoro, è possibile specificare il limite di throughput per il soffitto solo in IOPS.

- Un oggetto storage soggetto a un limite di QoS deve essere contenuto dalla SVM a cui appartiene il gruppo di criteri. Più gruppi di criteri possono appartenere alla stessa SVM.
- Non è possibile assegnare un oggetto di storage a un gruppo di criteri se l'oggetto contenente o i relativi oggetti figlio appartengono al gruppo di criteri.
- È consigliabile applicare un gruppo di criteri allo stesso tipo di oggetti di storage.

### Fasi

1. Creare un gruppo di criteri:

```
qos policy-group create -policy-group policy_group -vserver SVM -max  
-throughput number_of_iops|Mb/S|iops,Mb/S -is-shared true|false
```

Per la sintassi completa dei comandi, vedere la pagina man. È possibile utilizzare `qos policy-group modify` comando per regolare i limiti di throughput.

Il comando seguente crea il gruppo di criteri condivisi `pg-vs1` Con un throughput massimo di 5,000 IOPS:

```
cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1  
-max-throughput 5000iops -is-shared true
```

Il comando seguente crea il gruppo di criteri non condivisi `pg-vs3` Con un throughput massimo di 100 IOPS e 400 Kb/S:

```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
-max-throughput 100iops,400KB/s -is-shared false
```

Il comando seguente crea il gruppo di criteri non condivisi `pg-vs4` senza un limite di throughput:

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
-is-shared false
```

## 2. Applicare un gruppo di criteri a una SVM, a un file, a un volume o a un LUN:

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Per la sintassi completa dei comandi, vedere le pagine man. È possibile utilizzare `storage_object modify` per applicare un gruppo di criteri diverso all'oggetto di storage.

Il seguente comando applica il gruppo di criteri `pg-vs1` A SVM `vs1`:

```
cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
```

I seguenti comandi applicano il gruppo di criteri `pg-app` ai volumi `app1` e `app2`:

```
cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
-qos-policy-group pg-app
```

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app
```

## 3. Monitorare le performance dei gruppi di policy:

```
qos statistics performance show
```

Per la sintassi completa dei comandi, vedere la pagina man.



Monitorare le performance dal cluster. Non utilizzare uno strumento sull'host per monitorare le prestazioni.

Il seguente comando mostra le prestazioni del gruppo di criteri:

```
cluster1::> qos statistics performance show
```

| Policy Group        | IOPS  | Throughput | Latency   |
|---------------------|-------|------------|-----------|
| -total-             | 12316 | 47.76MB/s  | 1264.00us |
| pg_vs1              | 5008  | 19.56MB/s  | 2.45ms    |
| _System-Best-Effort | 62    | 13.36KB/s  | 4.13ms    |
| _System-Background  | 30    | 0KB/s      | 0ms       |

#### 4. Monitorare le performance dei carichi di lavoro:

```
qos statistics workload performance show
```

Per la sintassi completa dei comandi, vedere la pagina man.



Monitorare le performance dal cluster. Non utilizzare uno strumento sull'host per monitorare le prestazioni.

Il seguente comando mostra le performance del carico di lavoro:

```
cluster1::> qos statistics workload performance show
```

| Workload        | ID    | IOPS  | Throughput | Latency   |
|-----------------|-------|-------|------------|-----------|
| -total-         | -     | 12320 | 47.84MB/s  | 1215.00us |
| app1-wid7967    | 7967  | 7219  | 28.20MB/s  | 319.00us  |
| vs1-wid12279    | 12279 | 5026  | 19.63MB/s  | 2.52ms    |
| _USERSPACE_APPS | 14    | 55    | 10.92KB/s  | 236.00us  |
| _Scan_Backgro.. | 5688  | 20    | 0KB/s      | 0ms       |



È possibile utilizzare `qos statistics workload latency show` Comando per visualizzare statistiche dettagliate sulla latenza per i carichi di lavoro QoS.

#### Impostare un piano di throughput con QoS

È possibile utilizzare `min-throughput` Campo per un gruppo di policy per definire un piano di throughput per i carichi di lavoro degli oggetti storage (QoS min). È possibile applicare il gruppo di criteri quando si crea o si modifica l'oggetto di storage. A partire da ONTAP 9.8, è possibile specificare il volume di throughput in IOPS o Mbps o IOPS e Mbps.

##### Prima di iniziare

- È necessario eseguire ONTAP 9.2 o versione successiva. I piani di throughput sono disponibili a partire da ONTAP 9.2.
- Per creare un gruppo di criteri, è necessario essere un amministratore del cluster.
- A partire da ONTAP 9.13.1, è possibile applicare i piani di throughput a livello di SVM utilizzando un

[modello di gruppo di policy adattive](#). Non è possibile impostare un modello di gruppo di criteri adattativi su una SVM con un gruppo di criteri QoS.

### A proposito di questa attività

- A partire da ONTAP 9.4, è possibile utilizzare un gruppo di policy di qualità del servizio *non-shared* per specificare che il piano di throughput definito deve essere applicato a ogni singolo carico di lavoro membro. Questa è l'unica condizione in cui un gruppo di policy per un piano di throughput può essere applicato a più carichi di lavoro.

Impostare `-is-shared=false` per `qos policy-group create` per specificare un gruppo di criteri non condiviso.

- Il throughput di un carico di lavoro potrebbe scendere al di sotto del piano specificato se la capacità delle performance (spazio di crescita) del nodo o dell'aggregato è insufficiente.
- Un oggetto storage soggetto a un limite di QoS deve essere contenuto dalla SVM a cui appartiene il gruppo di criteri. Più gruppi di criteri possono appartenere alla stessa SVM.
- È consigliabile applicare un gruppo di criteri allo stesso tipo di oggetti di storage.
- Un gruppo di criteri che definisce un piano di throughput non può essere applicato a una SVM.

### Fasi

1. Controllare che le prestazioni sul nodo o sull'aggregato siano adeguate, come descritto nella ["Identificazione della capacità di prestazioni rimanente"](#).
2. Creare un gruppo di criteri:

```
qos policy-group create -policy group policy_group -vserver SVM -min  
-throughput qos_target -is-shared true|false
```

Per una sintassi completa dei comandi, consulta la pagina man della tua release ONTAP. È possibile utilizzare `qos policy-group modify` comando per regolare i piani di throughput.

Il comando seguente crea il gruppo di criteri condivisi `pg-vs2` Con un throughput minimo di 1,000 IOPS:

```
cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2  
-min-throughput 1000iops -is-shared true
```

Il comando seguente crea il gruppo di criteri non condivisi `pg-vs4` senza un limite di throughput:

```
cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4  
-is-shared false
```

3. Applicare un gruppo di criteri a un volume o a un LUN:

```
storage_object create -vserver SVM -qos-policy-group policy_group
```

Per la sintassi completa dei comandi, vedere le pagine man. È possibile utilizzare `_storage_object_modify` per applicare un gruppo di criteri diverso all'oggetto di storage.

Il seguente comando applica il gruppo di criteri `pg-app2` al volume `app2`:

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app2
```

#### 4. Monitorare le performance dei gruppi di policy:

```
qos statistics performance show
```

Per la sintassi completa dei comandi, vedere la pagina man.



Monitorare le performance dal cluster. Non utilizzare uno strumento sull'host per monitorare le prestazioni.

Il seguente comando mostra le prestazioni del gruppo di criteri:

```
cluster1::> qos statistics performance show
```

| Policy Group        | IOPS  | Throughput | Latency   |
|---------------------|-------|------------|-----------|
| -total-             | 12316 | 47.76MB/s  | 1264.00us |
| pg_app2             | 7216  | 28.19MB/s  | 420.00us  |
| _System-Best-Effort | 62    | 13.36KB/s  | 4.13ms    |
| _System-Background  | 30    | 0KB/s      | 0ms       |

#### 5. Monitorare le performance dei carichi di lavoro:

```
qos statistics workload performance show
```

Per la sintassi completa dei comandi, vedere la pagina man.



Monitorare le performance dal cluster. Non utilizzare uno strumento sull'host per monitorare le prestazioni.

Il seguente comando mostra le performance del carico di lavoro:

```
cluster1::> qos statistics workload performance show
```

| Workload        | ID    | IOPS  | Throughput | Latency   |
|-----------------|-------|-------|------------|-----------|
| -total-         | -     | 12320 | 47.84MB/s  | 1215.00us |
| app2-wid7967    | 7967  | 7219  | 28.20MB/s  | 319.00us  |
| vs1-wid12279    | 12279 | 5026  | 19.63MB/s  | 2.52ms    |
| _USERSPACE_APPS | 14    | 55    | 10.92KB/s  | 236.00us  |
| _Scan_Backgro.. | 5688  | 20    | 0KB/s      | 0ms       |



È possibile utilizzare `qos statistics workload latency show` Comando per visualizzare statistiche dettagliate sulla latenza per i carichi di lavoro QoS.

## Utilizzare gruppi di policy QoS adattivi

È possibile utilizzare un gruppo di policy *Adaptive QoS* per scalare automaticamente un limite di throughput o le dimensioni da pavimento a volume, mantenendo il rapporto tra IOPS e TB|GB al variare delle dimensioni del volume. Si tratta di un vantaggio significativo quando si gestiscono centinaia o migliaia di carichi di lavoro in un'implementazione di grandi dimensioni.

### Prima di iniziare

- È necessario eseguire ONTAP 9.3 o versione successiva. I gruppi di policy QoS adattivi sono disponibili a partire da ONTAP 9.3.
- Per creare un gruppo di criteri, è necessario essere un amministratore del cluster.

### A proposito di questa attività

Un oggetto storage può essere membro di un gruppo di criteri adattivi o non adattivi, ma non di entrambi. La SVM dell'oggetto di storage e il criterio devono essere identici. L'oggetto di storage deve essere in linea.

I gruppi di policy di QoS adattivi non sono sempre condivisi: Il limite di throughput definito o il piano si applica a ciascun carico di lavoro membro singolarmente.

Il rapporto tra i limiti di throughput e le dimensioni degli oggetti di storage è determinato dall'interazione dei seguenti campi:

- `expected-iops` È il minimo IOPS previsto per TB|GB allocati.



``expected-iops`` È garantito solo sulle piattaforme AFF.  
``expected-iops`` È garantito per FabricPool solo se la policy di tiering è impostata su "nessuno" e non ci sono blocchi nel cloud. ``expected-iops`` È garantito per i volumi che non sono in una relazione sincrona di SnapMirror.

- `peak-iops` È il massimo IOPS possibile per TB|GB allocati o utilizzati.
- `expected-iops-allocation` specifica se per gli iops previsti viene utilizzato lo spazio allocato (impostazione predefinita) o lo spazio utilizzato.



`expected-iops-allocation` È disponibile in ONTAP 9.5 e versioni successive. Non è supportato in ONTAP 9.4 e versioni precedenti.

- `peak-iops-allocation` specifica se viene utilizzato lo spazio allocato o lo spazio utilizzato (impostazione predefinita) per `peak-iops`.
- `absolute-min-iops` È il numero minimo assoluto di IOPS. È possibile utilizzare questo campo con oggetti di storage molto piccoli. Sovrascrive entrambi `peak-iops` e/o. `expected-iops` quando `absolute-min-iops` è maggiore del valore calcolato `expected-iops`.

Ad esempio, se si imposta `expected-iops` Fino a 1,000 IOPS/TB e le dimensioni del volume sono inferiori a 1 GB, il valore calcolato `expected-iops` Sarà un IOP frazionario. Il valore calcolato `peak-iops` sarà una frazione ancora più piccola. Per evitare questo problema, impostare `absolute-min-iops` a un

valore realistico.

- **block-size** Specifica la dimensione del blocco i/o dell'applicazione. L'impostazione predefinita è 32K. I valori validi sono 8K, 16K, 32K, 64K, QUALSIASI. QUALSIASI indica che la dimensione del blocco non viene applicata.

Sono disponibili tre gruppi di criteri QoS adattivi predefiniti, come mostrato nella tabella seguente. È possibile applicare questi gruppi di criteri direttamente a un volume.

| Gruppo di criteri predefinito | IOPS/TB previsti | IOPS/TB di picco | IOPS minimo assoluto |
|-------------------------------|------------------|------------------|----------------------|
| extreme                       | 6,144            | 12,288           | 1000                 |
| performance                   | 2,048            | 4,096            | 500                  |
| value                         | 128              | 512              | 75                   |

Non è possibile assegnare un oggetto di storage a un gruppo di criteri se l'oggetto contenente o i relativi oggetti figlio appartengono a un gruppo di criteri. Nella tabella seguente sono elencate le restrizioni.

| Se si assegna...           | Quindi non è possibile assegnare...                                     |
|----------------------------|-------------------------------------------------------------------------|
| SVM a un gruppo di criteri | Qualsiasi oggetto di storage contenuto dalla SVM a un gruppo di criteri |
| Su un gruppo di criteri    | Volumi contenenti SVM o LUN figlio di un gruppo di criteri              |
| LUN a un gruppo di criteri | I LUN contenenti un volume o una SVM in un gruppo di criteri            |
| Su un gruppo di criteri    | Il file contenente un volume o una SVM in un gruppo di criteri          |

## Fasi

### 1. Creare un gruppo di criteri QoS adattivi:

```
qos adaptive-policy-group create -policy group policy_group -vserver SVM
-expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
-iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
```

Per la sintassi completa dei comandi, vedere la pagina man.



-expected-iops-allocation e. -block-size È disponibile in ONTAP 9.5 e versioni successive. Queste opzioni non sono supportate in ONTAP 9.4 e versioni precedenti.

Il seguente comando crea un gruppo di criteri QoS adattivi `adpg-app1` con `-expected-iops` impostato

su 300 IOPS/TB, `-peak-iops` Impostato su 1,000 IOPS/TB, `-peak-iops-allocation` impostare su `used-space`, e. `-absolute-min-iops` Impostato su 50 IOPS:

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

## 2. Applicare un gruppo di criteri QoS adattivi a un volume:

```
volume create -vserver SVM -volume volume -aggregate aggregate -size number_of
TB|GB -qos-adaptive-policy-group policy_group
```

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando applica il gruppo di criteri QoS adattivi `adpg-app1` al volume `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

I seguenti comandi applicano il gruppo di criteri QoS adattivi predefinito `extreme` al nuovo volume `app4` e al volume esistente `app5`. Il limite di throughput definito per il gruppo di criteri si applica ai volumi `app4` e `app5` singolarmente:

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

## Impostare un modello di gruppo di criteri adattativi

A partire da ONTAP 9.13.1, è possibile applicare i livelli e i limiti di throughput a livello di SVM utilizzando un modello di gruppo di policy adattivo.

### A proposito di questa attività

- Il modello di gruppo di criteri adattivi è un criterio predefinito `apg1`. Il criterio può essere modificato in qualsiasi momento. Può essere impostato solo con l'API REST CLI o ONTAP e può essere applicato solo alle SVM esistenti.
- Il modello di gruppo di policy adattive influisce solo sui volumi creati o migrati sulla SVM dopo aver impostato il criterio. I volumi esistenti sulla SVM mantengono lo stato esistente.

Se si disattiva il modello di gruppo di criteri adattivi, i volumi su SVM conservano i criteri esistenti. Solo i volumi successivamente creati o migrati sulla SVM saranno influenzati dalla disabilitazione.



- Non è possibile impostare un modello di gruppo di criteri adattativi su una SVM con un gruppo di criteri QoS.
- I modelli di gruppi di policy adattivi sono progettati per le piattaforme AFF. È possibile impostare un modello di gruppo di policy adattivo su altre piattaforme, ma il criterio potrebbe non applicare un throughput minimo. Allo stesso modo, è possibile aggiungere un modello di gruppo di policy adattivo a una SVM in un aggregato FabricPool o in un aggregato che non supporta un throughput minimo, tuttavia il throughput non verrà applicato.
- Se la SVM si trova in una configurazione MetroCluster o in una relazione SnapMirror, il modello di gruppo di criteri adattativi verrà applicato alla SVM mirrorata.

## Fasi

1. Modificare la SVM per applicare il modello di gruppo di criteri adattativi:  

```
vserver modify -qos-adaptive-policy-group-template apg1
```
2. Verificare che il criterio sia stato impostato:  

```
vserver show -fields qos-adaptive-policy-group
```

## Monitorare le performance del cluster con Unified Manager

Con Active IQ Unified Manager, puoi massimizzare la disponibilità e mantenere il controllo della tua infrastruttura storage NetApp AFF e FAS per migliorare scalabilità, supportabilità, performance e sicurezza.

Active IQ Unified Manager monitora continuamente lo stato del sistema e invia avvisi, in modo che la tua organizzazione possa liberare risorse del personale IT. È possibile visualizzare istantaneamente lo stato dello storage da una singola dashboard e risolvere rapidamente i problemi attraverso le azioni consigliate.

La gestione dei dati è semplificata perché è possibile rilevare, monitorare e ricevere notifiche per gestire in modo proattivo lo storage e risolvere rapidamente i problemi. L'efficienza degli amministratori è migliorata grazie alla possibilità di monitorare petabyte di dati da un singolo dashboard e gestire i dati in modo scalabile.

Con Active IQ Unified Manager, puoi restare al passo con le esigenze di business fluttuanti, ottimizzando le performance utilizzando dati sulle performance e analytics avanzati. Le funzionalità di reporting consentono di accedere a report standard o creare report operativi personalizzati per soddisfare le esigenze specifiche del business.

Link correlati:

- ["Scopri di più su Active IQ Unified Manager"](#)
- ["Inizia subito con Active IQ Unified Manager per VMware"](#)
- ["Inizia subito con Active IQ Unified Manager per Linux"](#)
- ["Introduzione a Active IQ Unified Manager per Windows"](#)

## Monitorare le performance del cluster con Cloud Insights

NetApp Cloud Insights è uno strumento di monitoraggio che offre visibilità sull'intera infrastruttura. Con Cloud Insights, puoi monitorare, risolvere i problemi e ottimizzare tutte le risorse, inclusi i cloud pubblici e i data center privati.

## Cloud Insights è disponibile in due edizioni

L'edizione di base di Cloud Insights è progettata appositamente per monitorare e ottimizzare le risorse del data fabric NetApp. Fornisce analisi avanzate per le connessioni tra tutte le risorse NetApp, tra cui HCI e All Flash FAS (AFF) all'interno dell'ambiente, gratuitamente.

L'edizione standard di Cloud Insights si concentra non solo sui componenti dell'infrastruttura abilitati per il data fabric, ma anche sugli ambienti multi-vendor e multi-cloud. Grazie alle sue funzionalità avanzate, puoi accedere al supporto di oltre 100 servizi e risorse.

Nel mondo odierno, con risorse in gioco dai data center on-premise a più cloud pubblici, è fondamentale avere un quadro completo dell'applicazione stessa al disco back-end dello storage array. Il supporto aggiuntivo per il monitoraggio delle applicazioni (come Kafka, MongoDB e Nginx) fornisce le informazioni e le conoscenze necessarie per operare al livello di utilizzo ottimale e con il buffer di rischio perfetto.

Entrambe le edizioni (di base e standard) possono integrarsi con NetApp Active IQ Unified Manager. I clienti che utilizzano Active IQ Unified Manager possono visualizzare le informazioni di Unione all'interno dell'interfaccia utente di Cloud Insights. Le notifiche pubblicate su Active IQ Unified Manager non vengono trascurate e possono essere correlate agli eventi in Cloud Insights. In altre parole, otterrai il meglio di entrambi i mondi.

## Monitorare, risolvere i problemi e ottimizzare tutte le risorse

Cloud Insights ti aiuta a ridurre significativamente il tempo necessario per risolvere i problemi e a evitare che incidano sugli utenti finali. Inoltre, ti aiuta a ridurre i costi dell'infrastruttura cloud. La tua esposizione alle minacce interne è ridotta proteggendo i tuoi dati con informazioni pratiche.

Cloud Insights ti offre visibilità sull'intera infrastruttura ibrida in un'unica posizione, dal cloud pubblico al data center. Puoi creare istantaneamente dashboard pertinenti che possono essere personalizzati in base alle tue esigenze specifiche. È inoltre possibile creare avvisi mirati e condizionali specifici e pertinenti alle esigenze dell'organizzazione.

Il rilevamento avanzato delle anomalie consente di risolvere in modo proattivo i problemi prima che si verifichino. È possibile visualizzare automaticamente i conflitti e il degrado delle risorse per ripristinare rapidamente i carichi di lavoro interessati. Il troubleshooting viene eseguito più rapidamente grazie alla gerarchia di relazioni creata automaticamente tra i diversi componenti dello stack.

Puoi identificare le risorse inutilizzate o abbandonate nel tuo ambiente, che ti aiuta a scoprire le opportunità di dimensionare correttamente l'infrastruttura e ottimizzare l'intera spesa.

Cloud Insights visualizza la topologia del sistema per comprendere l'architettura di Kubernetes. È possibile monitorare lo stato dei cluster Kubernetes, inclusi i nodi in difficoltà, e ingrandire quando si verifica un problema.

Cloud Insights ti aiuta a proteggere i dati dell'organizzazione dall'utilizzo improprio da parte di utenti malintenzionati o compromessi attraverso l'apprendimento automatico avanzato e il rilevamento delle anomalie che ti offrono informazioni pratiche sulle minacce interne.

Cloud Insights ti aiuta a visualizzare le metriche di Kubernetes in modo da poter comprendere appieno le relazioni tra pod, nodi e cluster. È possibile valutare lo stato di salute di un cluster o di un pod di lavoro, nonché il carico attualmente in elaborazione, consentendo di assumere il controllo del cluster K8S e di controllare sia lo stato di salute che il costo dell'implementazione.

### Link correlati

- ["Scopri di più su Cloud Insights"](#)
- ["Inizia subito con Cloud Insights"](#)

## Registrazione dell'audit

### Come ONTAP implementa la registrazione dell'audit

Le attività di gestione registrate nel registro di audit sono incluse nei report standard di AutoSupport e alcune attività di registrazione sono incluse nei messaggi EMS. È inoltre possibile inoltrare il registro di controllo alle destinazioni specificate e visualizzare i file di registro di controllo utilizzando la CLI o un browser Web.

A partire da ONTAP 9.11.1, è possibile visualizzare il contenuto del registro di controllo utilizzando Gestione di sistema.

A partire da ONTAP 9.12.1, ONTAP fornisce avvisi di manomissione per i registri di controllo. ONTAP esegue un lavoro giornaliero in background per verificare la presenza di manomissioni di file audit.log e invia un avviso EMS se trova file di registro modificati o manomessi.

ONTAP registra le attività di gestione eseguite sul cluster, ad esempio la richiesta emessa, l'utente che ha attivato la richiesta, il metodo di accesso dell'utente e l'ora della richiesta.

Le attività di gestione possono essere di uno dei seguenti tipi:

- **IMPOSTARE** le richieste, che in genere si applicano a comandi o operazioni non di visualizzazione
  - Queste richieste vengono emesse quando si esegue un `create`, `modify`, o `delete` ad esempio.
  - Le richieste di `set` vengono registrate per impostazione predefinita.
- **OTTENERE** richieste che recuperano le informazioni e le visualizzano nell'interfaccia di gestione
  - Queste richieste vengono emesse quando si esegue un `show` ad esempio.
  - LE richieste `GET` non vengono registrate per impostazione predefinita, ma è possibile controllare se LE richieste `GET` inviate dall'interfaccia CLI ONTAP (`-cli get`), dall'API ONTAP (`-ontapi get`) O dall'API REST (`-http get`) sono registrati nel file.

ONTAP registra le attività di gestione in `/mroot/etc/log/mlog/audit.log` file di un nodo. I comandi delle tre shell per i comandi CLI—la `clustershell`, il `nodeshell` e la shell di sistema non interattiva (i comandi interattivi della shell di sistema non sono registrati)—così come i comandi API sono registrati qui. I registri di audit includono timestamp per mostrare se tutti i nodi di un cluster sono sincronizzati in base all'ora.

Il `audit.log` Il file viene inviato dallo strumento AutoSupport ai destinatari specificati. È inoltre possibile inoltrare il contenuto in modo sicuro alle destinazioni esterne specificate, ad esempio un server Splunk o syslog.

Il `audit.log` il file viene ruotato ogni giorno. La rotazione si verifica anche quando raggiunge 100 MB di dimensione e le precedenti 48 copie vengono conservate (con un totale massimo di 49 file). Quando il file di audit esegue la rotazione giornaliera, non viene generato alcun messaggio EMS. Se il file di audit ruota a causa del superamento del limite di dimensione del file, viene generato un messaggio EMS.

## Modifiche alla registrazione dell'audit in ONTAP 9

A partire da ONTAP 9 `command-history.log` il file viene sostituito da `audit.log` e il `mgwd.log` il file non contiene più informazioni di audit. Se si esegue l'aggiornamento a ONTAP 9, è necessario esaminare gli script o gli strumenti che fanno riferimento ai file legacy e al loro contenuto.

Dopo l'aggiornamento a ONTAP 9, esistente `command-history.log` i file vengono conservati. Vengono ruotati verso l'esterno (cancellati) come nuovi `audit.log` i file vengono ruotati in (creati).

Strumenti e script che controllano `command-history.log` il file potrebbe continuare a funzionare, perché un collegamento soft da `command-history.log` a `audit.log` viene creato al momento dell'aggiornamento. Tuttavia, strumenti e script che controllano `mgwd.log` il file non riesce, perché non contiene più informazioni di audit.

Inoltre, i registri di controllo di ONTAP 9 e versioni successive non includono più le seguenti voci, in quanto non sono considerate utili e causano attività di registrazione non necessarie:

- Comandi interni eseguiti da ONTAP (ovvero, dove `username=root`)
- Alias dei comandi (separatamente dal comando a cui puntano)

A partire da ONTAP 9, è possibile trasmettere i registri di controllo in modo sicuro a destinazioni esterne utilizzando i protocolli TCP e TLS.

## Visualizzare il contenuto del registro di controllo

È possibile visualizzare il contenuto dei cluster `/mroot/etc/log/mlog/audit.log` Utilizzando l'interfaccia utente di ONTAP, Gestore di sistema o un browser Web.

Le voci del file di log del cluster includono quanto segue:

### Ora

Data e ora della voce di registro.

### Applicazione

L'applicazione utilizzata per connettersi al cluster. Esempi di valori possibili sono `internal`, `console`, `ssh`, `http`, `ontapi`, `snmp`, `rsh`, `telnet`, e `service-processor`.

### Utente

Il nome utente dell'utente remoto.

### Stato

Lo stato corrente della richiesta di audit, che potrebbe essere `success`, `pending`, oppure `error`.

### Messaggio

Campo facoltativo che potrebbe contenere informazioni aggiuntive o errori sullo stato di un comando.

### ID sessione

L'ID della sessione in cui viene ricevuta la richiesta. A ogni *sessione* SSH viene assegnato un ID sessione, mentre a ogni *richiesta* HTTP, ONTAPI o SNMP viene assegnato un ID sessione univoco.

## VM di storage

SVM attraverso cui l'utente si è connesso.

## Scopo

Viene visualizzato `svm` Quando la richiesta si trova su una macchina virtuale per lo storage dei dati, altrimenti viene visualizzato `cluster`.

## ID comando

L'ID di ciascun comando ricevuto in una sessione CLI. In questo modo è possibile correlare una richiesta e una risposta. Le richieste ZAPI, HTTP e SNMP non dispongono di ID comando.

È possibile visualizzare le voci di registro del cluster dall'interfaccia utente di ONTAP, da un browser Web e a partire da ONTAP 9.11.1, da Gestore di sistema.

### System Manager

- Per visualizzare l'inventario, selezionare **Eventi e processi > registri di controllo**. + ogni colonna dispone di controlli per filtrare, ordinare, cercare, mostrare e inventariare le categorie. I dettagli dell'inventario possono essere scaricati come guida Excel.
- Per impostare i filtri, fare clic sul pulsante **Filter** (filtro) in alto a destra, quindi selezionare i campi desiderati. + è inoltre possibile visualizzare tutti i comandi eseguiti nella sessione in cui si è verificato un errore facendo clic sul collegamento Session ID (ID sessione).

### CLI

Per visualizzare le voci di audit unite da più nodi nel cluster, immettere:

```
security audit log show [parameters]
```

È possibile utilizzare `security audit log show` comando per visualizzare le voci di audit per i singoli nodi o unite da più nodi nel cluster. È inoltre possibile visualizzare il contenuto di `/mroot/etc/log/mlog` directory su un singolo nodo utilizzando un browser web. Per ulteriori informazioni, consulta la pagina man.

### Browser Web


È possibile visualizzare il contenuto di `/mroot/etc/log/mlog` directory su un singolo nodo utilizzando un browser web. ["Scopri come accedere ai file di log, core dump e MIB di un nodo utilizzando un browser Web"](#).

## Gestire le impostazioni di richiesta DI VERIFICA GET

Sebbene LE richieste SET siano registrate per impostazione predefinita, le richieste GET non lo sono. Tuttavia, è possibile controllare se LE richieste GET inviate dall'HTML di ONTAP (`-httpget`), l'interfaccia utente di ONTAP (`-cliget`), o dalle API ONTAP (`-ontapiget`) sono registrati nel file.

È possibile modificare le impostazioni di registrazione dell'audit dalla CLI di ONTAP e, a partire da ONTAP 9.11.1, da Gestore di sistema.

## System Manager

1. Selezionare **Eventi e processi > registri di controllo**.
2. Fare clic su  nell'angolo in alto a destra, scegliere le richieste da aggiungere o rimuovere.

## CLI

- Per specificare che le richieste GET dall'interfaccia utente o dalle API ONTAP devono essere registrate nel registro di controllo (il file audit.log), oltre alle richieste set predefinite, immettere:  
`security audit modify [-cliget {on|off}][--httpget {on|off}][--ontapiget {on|off}]`
- Per visualizzare le impostazioni correnti, immettere:  
`security audit show`

Per ulteriori informazioni, consulta le pagine man.

## Gestire le destinazioni del registro di controllo

È possibile inoltrare il registro di controllo a un massimo di 10 destinazioni. Ad esempio, è possibile inoltrare il log a un server Splunk o syslog per scopi di monitoraggio, analisi o backup.

### A proposito di questa attività

Per configurare l'inoltro, è necessario fornire l'indirizzo IP dell'host syslog o Splunk, il relativo numero di porta, un protocollo di trasmissione e la funzione syslog da utilizzare per i registri inoltrati. ["Scopri le funzionalità di syslog"](#).

È possibile selezionare uno dei seguenti valori di trasmissione:

### UDP non crittografato

User Datagram Protocol senza sicurezza (impostazione predefinita)

### TCP non crittografato




Transmission Control Protocol senza sicurezza

### Crittografia TCP

Transmission Control Protocol with Transport Layer Security (TLS) + Un'opzione **verify server** è disponibile quando si seleziona il protocollo crittografato TCP.

È possibile inoltrare i registri di controllo dall'interfaccia utente di ONTAP e, a partire da ONTAP 9.11.1, da Gestore di sistema.

## System Manager

- Per visualizzare le destinazioni del registro di controllo, selezionare **Cluster > Impostazioni**. + Un numero di destinazioni del registro viene visualizzato nel riquadro **Gestione notifiche**. Fare clic su  per visualizzare i dettagli.
- Per aggiungere, modificare o eliminare le destinazioni del registro di controllo, selezionare **Eventi e processi > registri di controllo**, quindi fare clic su **Gestisci destinazioni di controllo** nella parte superiore destra della schermata. + clic  **Add** oppure fare clic su  Nella colonna **Indirizzo host** per modificare o eliminare le voci.

## CLI

1. Per ciascuna destinazione a cui si desidera inoltrare il registro di controllo, specificare l'indirizzo IP o il nome host di destinazione e le opzioni di sicurezza.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

- Se il `cluster log-forwarding create` impossibile eseguire il ping dell'host di destinazione per verificare la connettività, il comando non riesce e viene visualizzato un errore. Anche se non consigliato, utilizzare `-force` il parametro con il comando ignora la verifica della connettività.
  - Quando si imposta `-verify-server` parametro a `true`, l'identità della destinazione di inoltro del log viene verificata convalidando il relativo certificato. È possibile impostare il valore su `true` solo quando si seleziona `tcp-encrypted` valore in `-protocol` campo.
2. Verificare che i record di destinazione siano corretti utilizzando `cluster log-forwarding show` comando.

```
cluster1::> cluster log-forwarding show
```

| Destination Host | Port | Protocol        | Verify Server | Syslog Facility |
|------------------|------|-----------------|---------------|-----------------|
| 192.168.123.96   | 514  | udp-unencrypted | false         | user            |
| 192.168.123.98   | 514  | tcp-encrypted   | true          | user            |

2 entries were displayed.

Per ulteriori informazioni, consulta le pagine man.

# AutoSupport

## Gestisci le impostazioni AutoSupport con Gestione di sistema

È possibile utilizzare Gestione di sistema per gestire le impostazioni dell'account AutoSupport.

È possibile eseguire le seguenti procedure:

### Consente di visualizzare le impostazioni AutoSupport

È possibile utilizzare Gestione sistema per visualizzare le impostazioni dell'account AutoSupport.

#### Fasi

1. In System Manager, fare clic su **Cluster > Settings** (Cluster > Impostazioni).

Nella sezione **AutoSupport** vengono visualizzate le seguenti informazioni:

- Stato
- Protocollo di trasporto
- Server proxy
- Da indirizzo e-mail


2. Nella sezione **AutoSupport**, selezionare , Quindi selezionare **altre opzioni**.

Vengono visualizzate ulteriori informazioni sulla connessione a AutoSupport e sulle impostazioni e-mail. Inoltre, viene elencata la cronologia di trasferimento dei messaggi.

## Generare e inviare dati AutoSupport

In Gestore di sistema, è possibile avviare la generazione di messaggi AutoSupport e scegliere tra i nodi del cluster da cui vengono raccolti i dati.


#### Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Nella sezione **AutoSupport**, selezionare , Quindi selezionare **genera e Invia**.
3. Inserire un oggetto.
4. Selezionare la casella di controllo in **Raccogli dati da** per specificare i nodi da cui raccogliere i dati.

## Verificare la connessione a AutoSupport

Da Gestione sistema, è possibile inviare un messaggio di prova per verificare la connessione a AutoSupport.

#### Fasi

1. In System Manager, fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare , Quindi selezionare **Test connettività**.
3. Inserire un oggetto per il messaggio.



## Attiva o disattiva AutoSupport



AutoSupport garantisce ai clienti NetApp benefici di business comprovati, tra cui l'identificazione proattiva dei possibili problemi di configurazione e una risoluzione più rapida dei casi di supporto. Nei nuovi sistemi, AutoSupport è abilitato per impostazione predefinita. Se necessario, puoi utilizzare System Manager per disabilitare AutoSupport per monitorare lo stato di salute del tuo sistema storage e inviare messaggi di notifica. È possibile attivare nuovamente AutoSupport dopo averlo disattivato.

### A proposito di questa attività

Prima di disattivare AutoSupport, tenere presente che si sta disattivando il sistema call-home di NetApp e che si perdono i seguenti benefici:

- **Monitoraggio dello stato:** AutoSupport monitora lo stato del sistema di archiviazione e invia notifiche al supporto tecnico e all'organizzazione di supporto interna.
- **Automazione:** AutoSupport automatizza il reporting dei casi di supporto. La maggior parte dei casi di supporto viene aperta automaticamente prima che i clienti si rendano conto che si è verificato un problema.
- **Risoluzione più rapida:** I sistemi che inviano dati AutoSupport hanno risolto i loro casi di supporto in metà del tempo rispetto ai casi dei sistemi che non inviano dati AutoSupport.
- **Aggiornamenti più veloci:** AutoSupport supporta i flussi di lavoro self-service dei clienti, come upgrade di versioni, componenti aggiuntivi, rinnovi e automazione degli aggiornamenti firmware in Gestione sistema.
- **Altre funzioni:** Alcune funzioni di altri strumenti funzionano solo quando AutoSupport è abilitato, ad esempio alcuni flussi di lavoro in BlueXP.

### Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare , Quindi selezionare **Disabilita**.
3. Se si desidera riattivare AutoSupport, nella sezione **AutoSupport**, selezionare , Quindi selezionare **Abilita**.

## Elimina la generazione di casi di supporto


A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per inviare una richiesta a AutoSupport per eliminare la generazione di casi di supporto.

### A proposito di questa attività

Per eliminare la generazione di casi di supporto, specificare i nodi e il numero di ore per cui si desidera che venga eseguita la soppressione.

La soppressione dei casi di supporto può essere particolarmente utile se non si desidera che AutoSupport crei casi automatizzati durante la manutenzione dei sistemi.


### Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare , Quindi selezionare **Sospendi generazione caso di supporto**.
3. Inserire il numero di ore in cui si desidera che venga eseguita la soppressione.
4. Selezionare i nodi per i quali si desidera eseguire la soppressione.

## Riprendere la generazione di casi di supporto

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per riprendere la generazione di casi di supporto da AutoSupport, se questa è stata soppressa.



### Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare , Quindi selezionare **Riprendi generazione caso di supporto**.
3. Selezionare i nodi per i quali si desidera riprendere la generazione.

## Modificare le impostazioni AutoSupport

È possibile utilizzare Gestione sistema per modificare le impostazioni di connessione e di posta elettronica dell'account AutoSupport.

### Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare , Quindi selezionare **altre opzioni**.
3. Nella sezione **connessioni** o nella sezione **e-mail**, selezionare  **Edit** consente di modificare le impostazioni di una delle sezioni.

## Gestire AutoSupport con l'interfaccia CLI

### Panoramica di Manage AutoSupport

AutoSupport è un meccanismo che monitora in modo proattivo lo stato di salute del sistema e invia automaticamente messaggi al supporto tecnico NetApp, all'organizzazione di supporto interna e a un partner di supporto. Sebbene i messaggi AutoSupport per il supporto tecnico siano attivati per impostazione predefinita, è necessario impostare le opzioni corrette e disporre di un host di posta valido per l'invio dei messaggi all'organizzazione di supporto interna.

Solo l'amministratore del cluster può eseguire la gestione di AutoSupport. L'amministratore della macchina virtuale per lo storage (SVM) non ha accesso a AutoSupport.

AutoSupport è attivato per impostazione predefinita quando si configura il sistema di storage per la prima volta. AutoSupport inizia a inviare messaggi al supporto tecnico 24 ore dopo l'attivazione di AutoSupport. È possibile ridurre il periodo di 24 ore aggiornando o ripristinando il sistema, modificando la configurazione AutoSupport o modificando l'ora del sistema in modo che non sia un periodo di 24 ore.



È possibile disattivare AutoSupport in qualsiasi momento, ma si consiglia di lasciarlo attivato. L'abilitazione di AutoSupport può contribuire a velocizzare in modo significativo la determinazione e la risoluzione dei problemi in caso di problemi nel sistema storage. Per impostazione predefinita, il sistema raccoglie le informazioni AutoSupport e le memorizza localmente, anche se si disattiva AutoSupport.

Per ulteriori informazioni su AutoSupport, visitare il sito del supporto NetApp.

### Informazioni correlate

- ["Supporto NetApp"](#)

- ["Scopri di più sui comandi AutoSupport nella CLI di ONTAP"](#)

## Utilizza AutoSupport e Active IQ Digital Advisor

Il componente AutoSupport di ONTAP raccoglie la telemetria e la invia per l'analisi. Il consulente digitale Active IQ analizza i dati di AutoSupport e offre un'assistenza e un'ottimizzazione proattive. Utilizzando l'intelligenza artificiale, Active IQ è in grado di identificare i potenziali problemi e di risolverli prima che influiscano sul tuo business.

Active IQ ti consente di ottimizzare la tua infrastruttura dati nel tuo cloud ibrido globale offrendo analisi predittive e supporto proattivo attraverso un portale basato sul cloud e un'app mobile. Le informazioni e i consigli di Active IQ basati sui dati sono disponibili per tutti i clienti NetApp con un contratto SupportEdge attivo (le funzionalità variano in base al prodotto e al livello di supporto).

Ecco alcune cose che puoi fare con Active IQ:

- Pianificare gli aggiornamenti. Active IQ identifica i problemi dell'ambiente che possono essere risolti eseguendo l'aggiornamento a una versione più recente di ONTAP e il componente preparazione aggiornamento consente di pianificare un aggiornamento corretto.
- Visualizza lo stato di salute del sistema. La dashboard di Active IQ segnala eventuali problemi relativi allo stato di salute e ti aiuta a correggerli. Monitorare la capacità del sistema per assicurarsi di non esaurire mai lo spazio di storage. Visualizza i casi di supporto per il tuo sistema.
- Gestire le performance. Active IQ mostra le performance del sistema in un periodo più lungo di quello che puoi vedere in Gestione sistema. Identificare i problemi di configurazione e di sistema che influiscono sulle performance.
- Massimizza l'efficienza. Visualizza le metriche di efficienza dello storage e identifica i modi per memorizzare più dati in meno spazio.
- Visualizza l'inventario e la configurazione. Active IQ visualizza l'inventario completo e le informazioni di configurazione software e hardware. Controlla quando i contratti di servizio stanno per scadere e rinnovarli per assicurarti di rimanere supportati.

## Informazioni correlate

["Documentazione NetApp: Consulente digitale Active IQ"](#)

["Avviare Active IQ"](#)

["Servizi SupportEdge"](#)

## Quando e dove vengono inviati i messaggi AutoSupport

AutoSupport invia messaggi a destinatari diversi, a seconda del tipo di messaggio. Imparare quando e dove AutoSupport invia i messaggi può aiutarti a comprendere i messaggi ricevuti tramite e-mail o a visualizzarli sul sito Web di Active IQ (precedentemente noto come My AutoSupport).

Se non diversamente specificato, le impostazioni nelle seguenti tabelle sono parametri di `system node autosupport modify` comando.

### Messaggi attivati dagli eventi

Quando si verificano eventi nel sistema che richiedono un'azione correttiva, AutoSupport invia automaticamente un messaggio attivato da un evento.

| Quando il messaggio viene inviato                        | Dove viene inviato il messaggio                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AutoSupport risponde a un evento di attivazione nell'EMS | <p>Indirizzi specificati in <code>-to</code> e <code>-noteto</code>. (Vengono inviati solo eventi critici che influiscono sul servizio).</p> <p>Indirizzi specificati in <code>-partner-address</code></p> <p>Supporto tecnico, se <code>-support</code> è impostato su <code>enable</code></p> |

### Messaggi pianificati

AutoSupport invia automaticamente diversi messaggi in base a una pianificazione regolare.

| Quando il messaggio viene inviato                                                                                                                                               | Dove viene inviato il messaggio                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Giornaliero (per impostazione predefinita, inviato tra le 12:00 e alle 1:00 come messaggio di log)                                                                              | <p>Indirizzi specificati in <code>-partner-address</code></p> <p>Supporto tecnico, se <code>-support</code> è impostato su <code>enable</code></p>  |
| Giornaliero (per impostazione predefinita, inviato tra le 12:00 e alle 1:00 come messaggio di performance), se <code>-perf</code> il parametro è impostato su <code>true</code> | <p>Indirizzi specificati in <code>-partner-address`</code></p> <p>Supporto tecnico, se <code>-support</code> è impostato su <code>enable</code></p> |
| Settimanale (per impostazione predefinita, la domenica viene inviata tra le 12:00 e 1:00)                                                                                       | <p>Indirizzi specificati in <code>-partner-address</code></p> <p>Supporto tecnico, se <code>-support</code> è impostato su <code>enable</code></p>  |

### Messaggi attivati manualmente

È possibile avviare o inviare di nuovo un messaggio AutoSupport manualmente.

| Quando il messaggio viene inviato                                                                                          | Dove viene inviato il messaggio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Viene avviato manualmente un messaggio utilizzando <code>system node autosupport invoke</code> comando                     | <p>Se viene specificato un URI utilizzando <code>-uri</code> nel <code>system node autosupport invoke</code> Il messaggio viene inviato all'URI.</p> <p>Se <code>-uri</code> viene omissso, il messaggio viene inviato agli indirizzi specificati in <code>-to</code> e. <code>-partner-address</code>. Il messaggio viene inviato anche al supporto tecnico se <code>-support</code> è impostato su <code>enable</code>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Viene avviato manualmente un messaggio utilizzando <code>system node autosupport invoke-core-upload</code> comando         | <p>Se viene specificato un URI utilizzando <code>-uri</code> nel <code>system node autosupport invoke-core-upload</code> Il messaggio viene inviato a quell'URI e il file core dump viene caricato nell'URI.</p> <p>Se <code>-uri</code> viene omissso in <code>system node autosupport invoke-core-upload</code> il messaggio viene inviato al supporto tecnico e il file core dump viene caricato nel sito del supporto tecnico.</p> <p>Entrambi gli scenari lo richiedono <code>-support</code> è impostato su <code>enable</code> e. <code>-transport</code> è impostato su <code>https</code> oppure <code>http</code>.</p> <p>A causa delle grandi dimensioni dei file core dump, il messaggio non viene inviato agli indirizzi specificati in <code>-to</code> e. <code>-partner-addresses</code> parametri.</p>                                                                                   |
| Viene avviato manualmente un messaggio utilizzando <code>system node autosupport invoke-performance-archive</code> comando | <p>Se viene specificato un URI utilizzando <code>-uri</code> nel <code>system node autosupport invoke-performance-archive</code> Il messaggio viene inviato a quell'URI e il file di archivio delle prestazioni viene caricato nell'URI.</p> <p>Se <code>-uri</code> viene omissso in <code>system node autosupport invoke-performance-archive</code>, il messaggio viene inviato al supporto tecnico e il file di archivio delle performance viene caricato sul sito del supporto tecnico.</p> <p>Entrambi gli scenari lo richiedono <code>-support</code> è impostato su <code>enable</code> e. <code>-transport</code> è impostato su <code>https</code> oppure <code>http</code>.</p> <p>A causa delle grandi dimensioni dei file di archiviazione delle prestazioni, il messaggio non viene inviato agli indirizzi specificati in <code>-to</code> e. <code>-partner-addresses</code> parametri.</p> |

| Quando il messaggio viene inviato                                                                                                            | Dove viene inviato il messaggio                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| È possibile inviare di nuovo manualmente un messaggio precedente utilizzando <code>system node autosupport history retransmit</code> comando | Solo all'URI specificato in <code>-uri</code> del parametro <code>system node autosupport history retransmit</code> comando |

### Messaggi attivati dal supporto tecnico

Il supporto tecnico può richiedere messaggi a AutoSupport utilizzando la funzione AutoSupport su richiesta.

| Quando il messaggio viene inviato                                                                                                                          | Dove viene inviato il messaggio                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Quando AutoSupport ottiene le istruzioni di consegna per generare nuovi messaggi AutoSupport                                                               | Indirizzi specificati in <code>-partner-address</code><br><br>Supporto tecnico, se <code>-support</code> è impostato su <code>enable</code> e <code>-transport</code> è impostato su <code>https</code>                                        |
| Quando AutoSupport ottiene le istruzioni di consegna per inviare nuovamente i messaggi AutoSupport precedenti                                              | Supporto tecnico, se <code>-support</code> è impostato su <code>enable</code> e <code>-transport</code> è impostato su <code>https</code>                                                                                                      |
| Quando AutoSupport ottiene le istruzioni di consegna per generare nuovi messaggi AutoSupport che caricano i file core dump o di archivio delle performance | Supporto tecnico, se <code>-support</code> è impostato su <code>enable</code> e <code>-transport</code> è impostato su <code>https</code> . Il core dump o il file di archivio delle performance viene caricato sul sito del supporto tecnico. |

### Modalità di creazione e invio dei messaggi attivati dagli eventi da parte di AutoSupport

AutoSupport crea messaggi AutoSupport attivati da eventi quando il servizio di emergenza elabora un evento di attivazione. Un messaggio AutoSupport attivato dall'evento avvisa i destinatari dei problemi che richiedono un'azione correttiva e contiene solo informazioni rilevanti per il problema. È possibile personalizzare i contenuti da includere e chi riceve i messaggi.

AutoSupport utilizza il seguente processo per creare e inviare messaggi AutoSupport attivati dagli eventi:

1. Quando EMS elabora un evento di attivazione, EMS invia una richiesta a AutoSupport.

Un evento trigger è un evento EMS con una destinazione AutoSupport e un nome che inizia con `a.callhome.` prefisso.

2. AutoSupport crea un messaggio AutoSupport attivato dall'evento.

AutoSupport raccoglie le informazioni di base e di troubleshooting dai sottosistemi associati al trigger per creare un messaggio che includa solo le informazioni pertinenti all'evento di trigger.

A ciascun trigger viene associato un set predefinito di sottosistemi. Tuttavia, è possibile scegliere di associare altri sottosistemi a un trigger utilizzando `system node autosupport trigger modify` comando.

3. AutoSupport invia il messaggio AutoSupport attivato dagli eventi ai destinatari definiti da `system node autosupport modify` con il `-to`, `-noteto`, `-partner-address`, e. `-support` parametri.

È possibile attivare e disattivare l'invio dei messaggi AutoSupport per trigger specifici utilizzando `system node autosupport trigger modify` con il `-to` e. `-noteto` parametri.

### Esempio di dati inviati per un evento specifico

Il `storage shelf PSU failed` Evento EMS attiva un messaggio che contiene dati di base da obbligatorio, file di log, storage, RAID, ha, Piattaforma e sistemi secondari di rete e dati di troubleshooting dai sottosistemi obbligatori, file di log e storage.

Decidi di includere i dati relativi a NFS in qualsiasi messaggio AutoSupport inviato in risposta a un futuro `storage shelf PSU failed` evento. Immettere il seguente comando per attivare i dati a livello di risoluzione dei problemi per NFS per `callhome.shlf.ps.fault` evento:

```
cluster1::\>
system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Tenere presente che il `callhome.` il prefisso viene eliminato da `callhome.shlf.ps.fault` quando si utilizza `system node autosupport trigger` O quando viene fatto riferimento da eventi AutoSupport e EMS nella CLI.

### Tipi di messaggi AutoSupport e relativi contenuti

I messaggi AutoSupport contengono informazioni sullo stato dei sottosistemi supportati. L'apprendimento dei messaggi AutoSupport consente di interpretare o rispondere ai messaggi ricevuti tramite e-mail o di visualizzarli sul sito Web di Active IQ (in precedenza denominato My AutoSupport).

| Tipo di messaggio  | Tipo di dati contenuti nel messaggio                                                                          |
|--------------------|---------------------------------------------------------------------------------------------------------------|
| Attivato da eventi | File contenenti dati sensibili al contesto relativi al sottosistema specifico in cui si è verificato l'evento |
| Ogni giorno        | File di log                                                                                                   |
| Performance        | Dati sulle performance campionati durante le 24 ore precedenti                                                |
| Settimanale        | Dati di configurazione e stato                                                                                |

| Tipo di messaggio                                                                   | Tipo di dati contenuti nel messaggio                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Attivato da <code>system node autosupport invoke comando</code>                     | <p>Dipende dal valore specificato in <code>-type</code> parametro:</p> <ul style="list-style-type: none"> <li><code>test</code> invia un messaggio attivato dall'utente con alcuni dati di base.</li> </ul> <p>Questo messaggio attiva anche una risposta email automatica dal supporto tecnico a qualsiasi indirizzo email specificato, utilizzando <code>-to</code>. Per confermare la ricezione dei messaggi AutoSupport.</p> <ul style="list-style-type: none"> <li><code>performance</code> invia i dati delle performance.</li> <li><code>all</code> invia un messaggio attivato dall'utente con una serie completa di dati simili al messaggio settimanale, inclusi i dati di risoluzione dei problemi di ciascun sottosistema.</li> </ul> <p>Il supporto tecnico in genere richiede questo messaggio.</p> |
| Attivato da <code>system node autosupport invoke-core-upload comando</code>         | File core dump per un nodo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Attivato da <code>system node autosupport invoke-performance-archive comando</code> | File di archiviazione delle performance per un periodo di tempo specificato                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Attivato da AutoSupport OnDemand                                                    | <p>AutoSupport OnDemand può richiedere nuovi messaggi o messaggi precedenti:</p> <ul style="list-style-type: none"> <li>I nuovi messaggi, a seconda del tipo di raccolta AutoSupport, possono essere <code>test</code>, <code>all</code>, o <code>performance</code>.</li> <li>I messaggi passati dipendono dal tipo di messaggio che viene inviato nuovamente.</li> </ul> <p>AutoSupport OnDemand può richiedere nuovi messaggi che caricano i seguenti file sul sito del supporto NetApp all'indirizzo <a href="https://mysupport.netapp.com">"mysupport.netapp.com"</a>:</p> <ul style="list-style-type: none"> <li>Core dump</li> <li>Archivio delle performance</li> </ul>                                                                                                                                   |

### Che cosa sono i sottosistemi AutoSupport

Ogni sottosistema fornisce informazioni di base e di risoluzione dei problemi che AutoSupport utilizza per i propri messaggi. Ogni sottosistema è inoltre associato a eventi



di trigger che consentono a AutoSupport di raccogliere solo informazioni relative all'evento di trigger dai sottosistemi.

AutoSupport raccoglie contenuti sensibili al contesto. È possibile visualizzare informazioni sui sottosistemi e sugli eventi di attivazione utilizzando `system node autosupport trigger show` comando.

### **Dimensioni AutoSupport e budget temporali**

AutoSupport raccoglie le informazioni, organizzate in base al sottosistema, e applica un budget di tempo e dimensioni sui contenuti per ciascun sottosistema. Con la crescita dei sistemi storage, i budget AutoSupport forniscono il controllo sul payload AutoSupport, che a sua volta fornisce un'erogazione scalabile dei dati AutoSupport.

AutoSupport interrompe la raccolta di informazioni e tronca il contenuto AutoSupport se il contenuto del sottosistema supera le dimensioni o il budget di tempo. Se il contenuto non può essere troncato facilmente (ad esempio, file binari), AutoSupport omette il contenuto.

È necessario modificare le dimensioni predefinite e i budget temporali solo se richiesto dal supporto NetApp. È inoltre possibile rivedere le dimensioni predefinite e i budget temporali dei sottosistemi utilizzando `autosupport manifest show` comando.

### **File inviati in messaggi AutoSupport attivati dagli eventi**

I messaggi AutoSupport attivati dagli eventi contengono solo informazioni di base e di risoluzione dei problemi provenienti dai sottosistemi associati all'evento che ha causato la generazione del messaggio da parte di AutoSupport. I dati specifici aiutano i partner di supporto e supporto NetApp a risolvere il problema.

AutoSupport utilizza i seguenti criteri per controllare il contenuto dei messaggi AutoSupport attivati dagli eventi:

- Quali sottosistemi sono inclusi

I dati sono raggruppati in sottosistemi, inclusi sottosistemi comuni, come file di registro, e sottosistemi specifici, come RAID. Ogni evento attiva un messaggio che contiene solo i dati di specifici sottosistemi.

- Il livello di dettaglio di ciascun sottosistema incluso

I dati per ciascun sottosistema incluso vengono forniti a livello di base o di troubleshooting.

È possibile visualizzare tutti gli eventi possibili e determinare quali sottosistemi sono inclusi nei messaggi relativi a ciascun evento utilizzando `system node autosupport trigger show` con il `-instance` parametro.

Oltre ai sottosistemi inclusi per impostazione predefinita per ciascun evento, è possibile aggiungere altri sottosistemi a livello di base o di risoluzione dei problemi utilizzando `system node autosupport trigger modify` comando.

### **File di log inviati in messaggi AutoSupport**

I messaggi AutoSupport possono contenere diversi file di log delle chiavi che consentono al personale del supporto tecnico di esaminare le recenti attività del sistema.

Tutti i tipi di messaggi AutoSupport possono includere i seguenti file di registro quando il sottosistema file di registro è attivato:

| File di log                                                                                                                                                                                                                                                     | Quantità di dati inclusi nel file                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• File di registro da <code>/mroot/etc/log/mlog/</code> directory</li><li>• Il file di log DEI MESSAGGI</li></ul>                                                                                                         | <p>Solo le nuove righe aggiunte ai registri dall'ultimo messaggio AutoSupport fino a un massimo specificato. Ciò garantisce che i messaggi AutoSupport abbiano dati univoci, rilevanti, non sovrapposti.</p> <p>(I file di log dei partner rappresentano un'eccezione; per i partner sono inclusi i dati massimi consentiti).</p> |
| <ul style="list-style-type: none"><li>• File di registro da <code>/mroot/etc/log/shelflog/</code> directory</li><li>• File di registro da <code>/mroot/etc/log/acp/</code> directory</li><li>• Dati di log del sistema di gestione degli eventi (EMS)</li></ul> | <p>Le righe di dati più recenti fino a un massimo specificato.</p>                                                                                                                                                                                                                                                                |

Il contenuto dei messaggi AutoSupport può cambiare tra una versione e l'altra di ONTAP.

### File inviati in messaggi AutoSupport settimanali

I messaggi AutoSupport settimanali contengono dati di configurazione e stato aggiuntivi utili per tenere traccia delle modifiche nel sistema nel tempo.

Le seguenti informazioni vengono inviate in messaggi AutoSupport settimanali:

- Informazioni di base su ogni sottosistema
- Contenuto di selezionato `/mroot/etc` file di directory
- File di log
- Output di comandi che forniscono informazioni di sistema
- Informazioni aggiuntive, tra cui le informazioni del database replicato (RDB), le statistiche di servizio e molto altro ancora

### In che modo AutoSupport OnDemand ottiene le istruzioni di consegna dal supporto tecnico

AutoSupport OnDemand comunica periodicamente con il supporto tecnico per ottenere istruzioni di consegna per l'invio, il reinvio e il rifiuto di messaggi AutoSupport, nonché per il caricamento di file di grandi dimensioni sul sito di supporto NetApp. AutoSupport OnDemand consente l'invio on-demand dei messaggi AutoSupport invece di attendere l'esecuzione del processo AutoSupport settimanale.

AutoSupport OnDemand è costituito dai seguenti componenti:

- Client AutoSupport OnDemand eseguito su ciascun nodo

- Servizio AutoSupport OnDemand che risiede nel supporto tecnico

Il client AutoSupport OnDemand esegue periodicamente il polling del servizio AutoSupport OnDemand per ottenere le istruzioni di consegna dal supporto tecnico. Ad esempio, il supporto tecnico può utilizzare il servizio AutoSupport OnDemand per richiedere la generazione di un nuovo messaggio AutoSupport. Quando il client AutoSupport OnDemand esegue il polling del servizio AutoSupport OnDemand, il client ottiene le istruzioni di consegna e invia il nuovo messaggio AutoSupport on-demand come richiesto.

AutoSupport OnDemand è attivato per impostazione predefinita. Tuttavia, AutoSupport OnDemand si affida ad alcune impostazioni AutoSupport per continuare a comunicare con il supporto tecnico. AutoSupport OnDemand comunica automaticamente con il supporto tecnico quando vengono soddisfatti i seguenti requisiti:

- AutoSupport è attivato.
- AutoSupport è configurato per inviare messaggi al supporto tecnico.
- AutoSupport è configurato per utilizzare il protocollo di trasporto HTTPS.

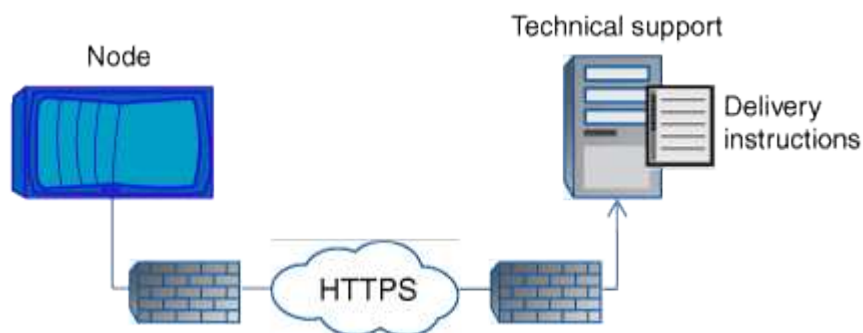
Il client AutoSupport OnDemand invia le richieste HTTPS alla stessa posizione del supporto tecnico a cui vengono inviati i messaggi AutoSupport. Il client AutoSupport OnDemand non accetta connessioni in entrata.



AutoSupport OnDemand utilizza l'account utente "AutoSupport" per comunicare con il supporto tecnico. ONTAP impedisce di eliminare questo account.

Se si desidera disattivare AutoSupport OnDemand, ma mantenere AutoSupport attivato, utilizzare il comando:  
 Link:[https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters\[system node autosupport modify -ondemand-state disable\]](https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters[system node autosupport modify -ondemand-state disable]).

La figura seguente mostra come AutoSupport OnDemand invia le richieste HTTPS al supporto tecnico per ottenere le istruzioni di consegna.



Le istruzioni di consegna possono includere richieste di AutoSupport per effettuare le seguenti operazioni:

- Generare nuovi messaggi AutoSupport.

Il supporto tecnico potrebbe richiedere nuovi messaggi AutoSupport per risolvere i problemi.

- Generare nuovi messaggi AutoSupport che caricano i file di dump core o i file di archivio delle performance sul sito di supporto NetApp.

Il supporto tecnico potrebbe richiedere il core dump o i file di archivio delle performance per risolvere i problemi di triage.

- Ritrasmettere i messaggi AutoSupport generati in precedenza.

Questa richiesta si verifica automaticamente se non è stato ricevuto un messaggio a causa di un errore di consegna.

- Disattiva l'invio dei messaggi AutoSupport per eventi trigger specifici.

Il supporto tecnico potrebbe disattivare la consegna dei dati non utilizzati.

## Struttura dei messaggi AutoSupport inviati via email

Quando un messaggio AutoSupport viene inviato via email, il messaggio ha un oggetto standard, un corpo breve e un grande allegato in formato file 7z che contiene i dati.



Se AutoSupport è configurato per nascondere i dati privati, alcune informazioni, come il nome host, vengono omesse o mascherate nell'intestazione, nell'oggetto, nel corpo e negli allegati.

### Soggetto

La riga dell'oggetto dei messaggi inviati dal meccanismo AutoSupport contiene una stringa di testo che identifica il motivo della notifica. Il formato dell'oggetto è il seguente:

Notifica gruppo HA da *Nome\_sistema* (*messaggio*) *severità*

- *Nome\_sistema* è il nome host o l'ID di sistema, a seconda della configurazione di AutoSupport

### Corpo

Il corpo del messaggio AutoSupport contiene le seguenti informazioni:

- Data e ora del messaggio
- Versione di ONTAP sul nodo che ha generato il messaggio
- ID di sistema, numero di serie e nome host del nodo che ha generato il messaggio
- Numero di sequenza AutoSupport
- Nome e posizione del contatto SNMP, se specificati
- ID di sistema e nome host del partnernode ha

### File allegati

Le informazioni chiave in un messaggio AutoSupport sono contenute in file compressi in un file 7z chiamato `body.7z` e allegato al messaggio.

I file contenuti nell'allegato sono specifici del tipo di messaggio AutoSupport.

### Tipi di severità AutoSupport

I messaggi AutoSupport hanno tipi di severità che aiutano a comprendere lo scopo di ciascun messaggio, ad esempio per attirare l'attenzione immediata su un problema di emergenza o solo per fornire informazioni.

I messaggi hanno una delle seguenti severità:

- **Alert:** I messaggi di avviso indicano che potrebbe verificarsi un evento di livello superiore se non si esegue alcuna azione.

È necessario intraprendere un'azione contro i messaggi di avviso entro 24 ore.

- **Emergenza:** I messaggi di emergenza vengono visualizzati quando si verifica un'interruzione.

È necessario intraprendere immediatamente un'azione contro i messaggi di emergenza.

- **Error:** Le condizioni di errore indicano cosa potrebbe accadere se si ignora.
- **Avviso:** Condizione normale ma significativa.
- **Info:** Il messaggio informativo fornisce dettagli sul problema, che è possibile ignorare.
- **Debug:** I messaggi a livello di debug forniscono le istruzioni da eseguire.

Se l'organizzazione di supporto interna riceve messaggi AutoSupport tramite e-mail, la severità viene visualizzata nella riga dell'oggetto del messaggio.

### Requisiti per l'utilizzo di AutoSupport

È necessario utilizzare HTTPS con TLSv1.2 o SMTP sicuro per l'invio dei messaggi AutoSupport per garantire la massima sicurezza e per supportare tutte le funzionalità AutoSupport più recenti. I messaggi AutoSupport inviati con qualsiasi altro protocollo verranno rifiutati.

### Protocolli supportati

Tutti questi protocolli vengono eseguiti su IPv4 o IPv6, in base alla famiglia di indirizzi a cui il nome viene risolto.

| Protocollo e porta    | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTPS sulla porta 443 | <p>Questo è il protocollo predefinito. Se possibile, utilizzare questa opzione.</p> <p>Questo protocollo supporta AutoSupport OnDemand e upload di file di grandi dimensioni.</p> <p>Il certificato proveniente dal server remoto viene convalidato in base al certificato root, a meno che non venga disattivata la convalida.</p> <p>Il recapito utilizza una richiesta HTTPS PUT. Con PUT, se la richiesta non riesce durante la trasmissione, la richiesta viene riavviata da dove è stata interrotta. Se il server che riceve la richiesta non supporta PUT, il recapito utilizza una richiesta HTTPS POST.</p> |

| Protocollo e porta                      | Descrizione                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP sulla porta 80                     | <p>Questo protocollo è preferito rispetto a SMTP.</p> <p>Questo protocollo supporta il caricamento di file di grandi dimensioni, ma non AutoSupport OnDemand.</p> <p>Il recapito utilizza una richiesta HTTPS PUT. Con PUT, se la richiesta non riesce durante la trasmissione, la richiesta viene riavviata da dove è stata interrotta. Se il server che riceve la richiesta non supporta PUT, il recapito utilizza una richiesta HTTPS POST.</p>                                                                                                                                                                                                                                                                                     |
| SMTP sulla porta 25 o su un'altra porta | <p>Utilizzare questo protocollo solo se la connessione di rete non consente HTTPS.</p> <p>Il valore predefinito della porta è 25, ma è possibile configurare AutoSupport in modo che utilizzi una porta diversa.</p> <p>Tenere presenti le seguenti limitazioni quando si utilizza SMTP:</p> <ul style="list-style-type: none"> <li>• AutoSupport OnDemand e upload di file di grandi dimensioni non sono supportati.</li> <li>• I dati non sono crittografati.</li> </ul> <p>SMTP invia i dati in testo chiaro, rendendo il testo nel messaggio AutoSupport facile da intercettare e leggere.</p> <ul style="list-style-type: none"> <li>• È possibile introdurre limitazioni sulla lunghezza del messaggio e della linea.</li> </ul> |

Se si configura AutoSupport con indirizzi e-mail specifici per l'organizzazione di supporto interna o per un'organizzazione di partner di supporto, tali messaggi vengono sempre inviati tramite SMTP.

Ad esempio, se si utilizza il protocollo consigliato per inviare messaggi al supporto tecnico e si desidera anche inviare messaggi all'organizzazione di supporto interna, i messaggi verranno trasportati utilizzando sia HTTPS che SMTP, rispettivamente.

AutoSupport limita le dimensioni massime dei file per ciascun protocollo. L'impostazione predefinita per i trasferimenti HTTP e HTTPS è 25 MB. L'impostazione predefinita per i trasferimenti SMTP è 5 MB. Se le dimensioni del messaggio AutoSupport superano il limite configurato, AutoSupport recapita la maggior parte del messaggio possibile. È possibile modificare le dimensioni massime modificando la configurazione di AutoSupport. Vedere `system node autosupport modify` pagina man per ulteriori informazioni.



AutoSupport sovrascrive automaticamente il limite massimo delle dimensioni dei file per i protocolli HTTPS e HTTP quando si generano e inviano messaggi AutoSupport che caricano i file core dump o di archivio delle performance al sito di supporto NetApp o a un URI specificato. L'override automatica si applica solo quando si caricano i file utilizzando `system node autosupport invoke-core-upload` o il `system node autosupport invoke-performance-archive` comandi.

## Requisiti di configurazione

A seconda della configurazione di rete, il protocollo HTTPS potrebbe richiedere un'ulteriore configurazione di un URL proxy. Se HTTPS invia messaggi AutoSupport al supporto tecnico e si dispone di un proxy, è necessario identificare l'URL per tale proxy. Se il proxy utilizza una porta diversa da quella predefinita, ovvero 3128, è possibile specificare la porta per tale proxy. È inoltre possibile specificare un nome utente e una password per l'autenticazione del proxy.

Se si utilizza SMTP per inviare messaggi AutoSupport all'organizzazione di supporto interna o al supporto tecnico, è necessario configurare un server di posta esterno. Il sistema di storage non funziona come server di posta, ma richiede un server di posta esterno per l'invio della posta. Il server di posta deve essere un host in attesa sulla porta SMTP (25) o su un'altra porta e deve essere configurato per inviare e ricevere la codifica MIME (Multipurpose Internet Mail Extensions) a 8 bit. Gli host di posta di esempio includono un host UNIX che esegue un server SMTP come il programma sendmail e un server Windows che esegue il server Microsoft Exchange. È possibile disporre di uno o più host di posta.

## Configurare AutoSupport

È possibile controllare se e come le informazioni AutoSupport vengono inviate al supporto tecnico e all'organizzazione di supporto interna, quindi verificare che la configurazione sia corretta.

### A proposito di questa attività

In ONTAP 9.5 e versioni successive, è possibile attivare AutoSupport e modificarne la configurazione su tutti i nodi del cluster contemporaneamente. Quando un nuovo nodo si unisce al cluster, il nodo eredita automaticamente la configurazione del cluster AutoSupport. Non è necessario aggiornare la configurazione su ciascun nodo separatamente.



A partire da ONTAP 9.5, lo scopo di `system node autosupport modify` il comando è esteso a tutto il cluster. La configurazione AutoSupport viene modificata su tutti i nodi del cluster, anche quando `-node` opzione specificata. L'opzione viene ignorata, ma è stata mantenuta per la compatibilità con le versioni precedenti di CLI.

In ONTAP 9.4 e versioni precedenti, lo scopo di `system node autosupport modify` il comando è specifico del nodo. La configurazione AutoSupport deve essere modificata su ciascun nodo del cluster.

Per impostazione predefinita, AutoSupport è attivato su ciascun nodo per inviare messaggi al supporto tecnico utilizzando il protocollo di trasporto HTTPS.

È necessario utilizzare HTTPS con TLSv1.2 o SMTP sicuro per l'invio dei messaggi AutoSupport per garantire la massima sicurezza e per supportare tutte le funzionalità AutoSupport più recenti.

## Fasi

1. Assicurarsi che AutoSupport sia attivato:

```
system node autosupport modify -state enable
```

2. Se si desidera che il supporto tecnico riceva messaggi AutoSupport, utilizzare il seguente comando:

```
system node autosupport modify -support enable
```

È necessario attivare questa opzione se si desidera attivare AutoSupport per lavorare con AutoSupport OnDemand o se si desidera caricare file di grandi dimensioni, come i file di archiviazione delle performance e dei core dump, sul supporto tecnico o su un URL specificato.

3. Se il supporto tecnico è abilitato a ricevere messaggi AutoSupport, specificare il protocollo di trasporto da utilizzare per i messaggi.

È possibile scegliere tra le seguenti opzioni:

| Se si desidera...                          | Quindi, impostare i seguenti parametri di <code>system node autosupport modify</code> comando...                                                                                                                                                                      |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Utilizzare il protocollo HTTPS predefinito | <p>a. Impostare <code>-transport a. https</code>.</p> <p>b. Se si utilizza un proxy, impostare <code>-proxy-url</code> All'URL del proxy. Questa configurazione supporta la comunicazione con AutoSupport OnDemand e il caricamento di file di grandi dimensioni.</p> |
| USA SMTP                                   | <p>Impostare <code>-transport a. smtp</code>.</p> <p>Questa configurazione non supporta AutoSupport OnDemand o upload di file di grandi dimensioni.</p>                                                                                                               |

4. Se si desidera che l'organizzazione di supporto interna o un partner di supporto riceva messaggi AutoSupport, eseguire le seguenti operazioni:

- a. Identificare i destinatari dell'organizzazione impostando i seguenti parametri di `system node autosupport modify` comando:

| Imposta questo parametro... | A questo...                                                                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-to</code>            | Fino a cinque indirizzi e-mail o liste di distribuzione separati da virgole nell'organizzazione di supporto interna che riceveranno messaggi AutoSupport chiave |



|                  |                                                                                                                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -noteto          | Fino a cinque indirizzi e-mail o liste di distribuzione separati da virgole nell'organizzazione di supporto interna che riceveranno una versione abbreviata dei messaggi AutoSupport chiave progettati per telefoni cellulari e altri dispositivi mobili |
| -partner-address | Fino a cinque indirizzi e-mail o liste di distribuzione separati da virgole nell'organizzazione del partner di supporto che riceveranno tutti i messaggi AutoSupport                                                                                     |

b. Verificare che gli indirizzi siano configurati correttamente elencando le destinazioni utilizzando `system node autosupport destinations show` comando.

5. Se si inviano messaggi all'organizzazione di supporto interna o si sceglie il trasporto SMTP per i messaggi all'assistenza tecnica, configurare SMTP impostando i seguenti parametri di `system node autosupport modify` comando:

- Impostare `-mail-hosts` a uno o più mail host, separati da virgole.

È possibile impostare un massimo di cinque.

È possibile configurare un valore di porta per ciascun host di posta specificando i due punti e il numero di porta dopo il nome host della posta: Ad esempio, `mymailhost.example.com:5678`, dove 5678 è la porta per l'host di posta.

- Impostare `-from` All'indirizzo e-mail che invia il messaggio AutoSupport.

6. Configurare il DNS.

7. Se si desidera modificare impostazioni specifiche, aggiungere opzioni di comando:

|                                                                                               |                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se si desidera eseguire questa operazione...                                                  | Quindi, impostare i seguenti parametri di <code>system node autosupport modify</code> comando...                                                                                                                  |
| Nascondere i dati privati rimuovendo, mascherando o codificando i dati sensibili nei messaggi | Impostare <code>-remove-private-data</code> a <code>true</code> . Se si cambia da <code>false</code> a <code>true</code> , Vengono cancellati tutti i file della cronologia AutoSupport e tutti i file associati. |
| Interrompere l'invio dei dati relativi alle prestazioni nei messaggi AutoSupport periodici    | Impostare <code>-perf</code> a <code>false</code> .                                                                                                                                                               |

8. Controllare la configurazione generale utilizzando `system node autosupport show` con il `-node` parametro.

9. Verificare il funzionamento di AutoSupport utilizzando `system node autosupport check show` comando.

Se vengono segnalati problemi, utilizzare `system node autosupport check show-details` per visualizzare ulteriori informazioni.

## 10. Verifica dell'invio e della ricezione dei messaggi AutoSupport:

- a. Utilizzare `system node autosupport invoke` con il `-type` parametro impostato su `test`.

```
cluster1::> system node autosupport invoke -type test -node node1
```

- b. Conferma che NetApp sta ricevendo i tuoi messaggi AutoSupport:

la cronologia AutoSupport del nodo di sistema mostra `-node local`

Lo stato dell'ultimo messaggio AutoSupport in uscita dovrebbe cambiare in `sent-successful` per tutte le destinazioni del protocollo appropriate.

- a. Se lo si desidera, verificare che il messaggio AutoSupport venga inviato all'organizzazione di supporto interna o al partner di supporto controllando l'indirizzo e-mail di qualsiasi indirizzo configurato per `-to`, `-noteto`, o `-partner-address` parametri di `system node autosupport modify` comando.

### Caricare i file core dump

Quando viene salvato un file core dump, viene generato un messaggio di evento. Se il servizio AutoSupport è abilitato e configurato per l'invio di messaggi al supporto NetApp, viene trasmesso un messaggio AutoSupport e viene inviato un messaggio e-mail di conferma automatico.

### Di cosa hai bisogno

- È necessario configurare AutoSupport con le seguenti impostazioni:
  - AutoSupport è attivato sul nodo.
  - AutoSupport è configurato per inviare messaggi al supporto tecnico.
  - AutoSupport è configurato per utilizzare il protocollo di trasporto HTTP o HTTPS.

Il protocollo di trasporto SMTP non è supportato quando si inviano messaggi che includono file di grandi dimensioni, come i file core dump.

### A proposito di questa attività

È inoltre possibile caricare il file core dump tramite il servizio AutoSupport su HTTPS utilizzando `system node autosupport invoke-core-upload` Comando, se richiesto dal supporto NetApp.

### "Come caricare un file su NetApp"

#### Fasi

1. Visualizzare i file di dump principali per un nodo utilizzando `system node coredump show` comando.

Nell'esempio seguente, i file core dump vengono visualizzati per il nodo locale:

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
-----
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Generare un messaggio AutoSupport e caricare un file core dump utilizzando `system node autosupport invoke-core-upload` comando.

Nell'esempio seguente, viene generato un messaggio AutoSupport e inviato alla posizione predefinita, ovvero il supporto tecnico, e il file core dump viene caricato nella posizione predefinita, ovvero il sito di supporto NetApp:

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

Nell'esempio seguente, viene generato e inviato un messaggio AutoSupport nella posizione specificata nell'URI e il file dump core viene caricato nell'URI:

```
cluster1::> system node autosupport invoke-core-upload -uri
https://files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

## Caricare i file di archivio delle performance

È possibile generare e inviare un messaggio AutoSupport contenente un archivio delle performance. Per impostazione predefinita, il supporto tecnico di NetApp riceve il messaggio AutoSupport e l'archivio delle performance viene caricato sul sito di supporto NetApp. È possibile specificare una destinazione alternativa per il messaggio e il caricamento.

### Di cosa hai bisogno

- È necessario configurare AutoSupport con le seguenti impostazioni:
  - AutoSupport è attivato sul nodo.
  - AutoSupport è configurato per inviare messaggi al supporto tecnico.
  - AutoSupport è configurato per utilizzare il protocollo di trasporto HTTP o HTTPS.

Il protocollo di trasporto SMTP non è supportato quando si inviano messaggi che includono file di grandi dimensioni, ad esempio file di archiviazione delle prestazioni.

### A proposito di questa attività

È necessario specificare una data di inizio per i dati dell'archivio delle performance che si desidera caricare. La maggior parte dei sistemi storage conserva gli archivi delle performance per due settimane, consentendoti di

specificare una data di inizio fino a due settimane fa. Ad esempio, se oggi è il 15 gennaio, è possibile specificare una data di inizio del 2 gennaio.

**Fase**

1. Generare un messaggio AutoSupport e caricare il file di archivio delle performance utilizzando `system node autosupport invoke-performance-archive` comando.

Nell'esempio seguente, 4 ore di file di archivio delle performance dal 12 gennaio 2015 vengono aggiunti a un messaggio AutoSupport e caricati nella posizione predefinita, che è il sito di supporto NetApp:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h
```

Nell'esempio seguente, 4 ore di file di archivio delle performance dal 12 gennaio 2015 vengono aggiunti a un messaggio AutoSupport e caricati nella posizione specificata dall'URI:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

**Ottenere le descrizioni dei messaggi AutoSupport**

Le descrizioni dei messaggi AutoSupport ricevuti sono disponibili tramite il convertitore Syslog di ONTAP.

**Fasi**

1. Accedere alla ["Syslog Translator"](#).
2. Nel campo **Release**, immettere la versione di ONTAP in uso. Nel campo **stringa di ricerca**, immettere "callhome". Selezionare **Translate** (Traduci).
3. Syslog Translator elenca in ordine alfabetico tutti gli eventi che corrispondono alla stringa di messaggi immessa.

**Comandi per la gestione di AutoSupport**

Si utilizza `system node autosupport` Comandi per modificare o visualizzare la configurazione AutoSupport, visualizzare le informazioni sui messaggi AutoSupport precedenti e inviare, reinviare o annullare un messaggio AutoSupport.

**Configurare AutoSupport**

| Se si desidera...                                 | Utilizzare questo comando...                                     |
|---------------------------------------------------|------------------------------------------------------------------|
| Controlla se vengono inviati messaggi AutoSupport | <code>system node autosupport modify con -state parametro</code> |

| Se si desidera...                                                                                                                                                                                                   | Utilizzare questo comando...                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Controlla se i messaggi AutoSupport vengono inviati al supporto tecnico                                                                                                                                             | <code>system node autosupport modify con -support parametro</code> |
| Impostare AutoSupport o modificare la configurazione di AutoSupport                                                                                                                                                 | <code>system node autosupport modify</code>                        |
| Abilitare e disabilitare i messaggi AutoSupport per i singoli eventi di attivazione e specificare report aggiuntivi del sottosistema da includere nei messaggi inviati in risposta ai singoli eventi di attivazione | <code>system node autosupport trigger modify</code>                |

#### Visualizza le informazioni sulla configurazione AutoSupport



| Se si desidera...                                                                                                  | Utilizzare questo comando...                                  |
|--------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| Visualizzare la configurazione AutoSupport                                                                         | <code>system node autosupport show con -node parametro</code> |
| Visualizza un riepilogo di tutti gli indirizzi e gli URL che ricevono messaggi AutoSupport                         | <code>system node autosupport destinations show</code>        |
| Visualizza i messaggi AutoSupport inviati all'organizzazione di supporto interna per singoli eventi di attivazione | <code>system node autosupport trigger show</code>             |
| Visualizza lo stato della configurazione AutoSupport e l'invio a varie destinazioni                                | <code>system node autosupport check show</code>               |
| Visualizza lo stato dettagliato della configurazione AutoSupport e la consegna a varie destinazioni                | <code>system node autosupport check show-details</code>       |

#### Visualizza le informazioni sui messaggi AutoSupport precedenti

| Se si desidera...                                                                                                                                                                       | Utilizzare questo comando...                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Visualizza informazioni su uno o più dei 50 messaggi AutoSupport più recenti                                                                                                            | <code>system node autosupport history show</code>                |
| Visualizza le informazioni sui messaggi AutoSupport recenti generati per caricare i file core dump o di archivio delle performance sul sito di supporto tecnico o su un URI specificato | <code>system node autosupport history show-upload-details</code> |

| Se si desidera...                                                                                                                                                             | Utilizzare questo comando...                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Consente di visualizzare le informazioni contenute nei messaggi AutoSupport, inclusi il nome e le dimensioni di ciascun file raccolto per il messaggio e gli eventuali errori | <code>system node autosupport manifest show</code> |

#### Inviare, inviare nuovamente o annullare i messaggi AutoSupport

| Se si desidera...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Utilizzare questo comando...                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ritrasmettere un messaggio AutoSupport memorizzato localmente, identificato dal numero di sequenza AutoSupport <div>  <p>Se si ritrasmette un messaggio AutoSupport e se il supporto ha già ricevuto tale messaggio, il sistema di supporto non crea un caso duplicato. Se, d'altra parte, il supporto non ha ricevuto quel messaggio, il sistema AutoSupport analizzerà il messaggio e, se necessario, creerà un caso.</p> </div> | <code>system node autosupport history retransmit</code>                                                                                                                                                                                                                                                                                                                                          |
| Generare e inviare un messaggio AutoSupport, ad esempio a scopo di test                                                                                                                                                                                                                                                                                                                                                                                                                                             | <code>system node autosupport invoke</code> <div>  <p>Utilizzare <code>-force</code> Parametro per inviare un messaggio anche se AutoSupport è disattivato. Utilizzare <code>-uri</code> parametro per inviare il messaggio alla destinazione specificata al posto della destinazione configurata.</p> </div> |
| Consente di annullare un messaggio AutoSupport                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <code>system node autosupport history cancel</code>                                                                                                                                                                                                                                                                                                                                              |

#### Informazioni correlate

["Comandi di ONTAP 9"](#)

#### Informazioni incluse nel manifesto di AutoSupport

Il manifesto AutoSupport fornisce una vista dettagliata dei file raccolti per ciascun messaggio AutoSupport. Il manifesto di AutoSupport include anche informazioni sugli errori di raccolta quando AutoSupport non è in grado di raccogliere i file di cui ha bisogno.

Il manifesto di AutoSupport include le seguenti informazioni:

- Numero di sequenza del messaggio AutoSupport
- Quali file AutoSupport sono inclusi nel messaggio AutoSupport

- Dimensione di ogni file, in byte
- Stato dell'insieme di manifest AutoSupport
- Descrizione dell'errore, se AutoSupport non riesce a raccogliere uno o più file

È possibile visualizzare il manifesto AutoSupport utilizzando `system node autosupport manifest show` comando.

Il manifesto AutoSupport è incluso in ogni messaggio AutoSupport e presentato in formato XML, il che significa che è possibile utilizzare un visualizzatore XML generico per leggerlo o visualizzarlo utilizzando il portale Active IQ (precedentemente noto come My AutoSupport).

### Soppressione del caso AutoSupport durante le finestre di manutenzione programmata

La soppressione dei casi AutoSupport consente di impedire la creazione di casi non necessari da parte dei messaggi AutoSupport attivati durante le finestre di manutenzione pianificate.

Per eliminare i casi AutoSupport, è necessario richiamare manualmente un messaggio AutoSupport con una stringa di testo appositamente formattata: `MAINT=xh`. `x` indica la durata della finestra di manutenzione in unità di ore.

### Informazioni correlate

["Come eliminare la creazione automatica del caso durante le finestre di manutenzione pianificata"](#)

### Risolvere i problemi relativi a AutoSupport quando i messaggi non vengono ricevuti

Se il sistema non invia il messaggio AutoSupport, è possibile determinare se il messaggio non viene generato da AutoSupport o non è possibile recapitare il messaggio.

### Fasi

1. Controllare lo stato di consegna dei messaggi utilizzando `system node autosupport history show` comando.
2. Leggere lo stato.

| Questo stato              | Significa                                                                                                                                                                                                                                            |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| inizializzazione in corso | Il processo di raccolta è in corso. Se questo stato è temporaneo, va bene. Tuttavia, se lo stato persiste, si è verificato un problema.                                                                                                              |
| raccolta non riuscita     | AutoSupport non è in grado di creare il contenuto AutoSupport nella directory di spool. È possibile visualizzare i dati che AutoSupport sta tentando di raccogliere immettendo il <code>system node autosupport history show -detail</code> comando. |
| raccolta in corso         | AutoSupport sta raccogliendo contenuti AutoSupport. È possibile visualizzare i dati raccolti da AutoSupport immettendo il <code>system node autosupport manifest show</code> comando.                                                                |

| Questo stato              | Significa                                                                                                                                                                                                                                                                                 |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| in coda                   | I messaggi AutoSupport vengono messi in coda per la consegna, ma non ancora recapitati.                                                                                                                                                                                                   |
| in trasmissione           | AutoSupport sta attualmente distribuendo messaggi.                                                                                                                                                                                                                                        |
| inviato correttamente     | AutoSupport ha recapitato correttamente il messaggio. È possibile scoprire dove AutoSupport ha recapitato il messaggio immettendo il <code>system node autosupport history show -delivery</code> comando.                                                                                 |
| ignorare                  | AutoSupport non ha destinazioni per il messaggio. È possibile visualizzare i dettagli di consegna immettendo il <code>system node autosupport history show -delivery</code> comando.                                                                                                      |
| riaccolato                | AutoSupport ha tentato di inviare messaggi, ma il tentativo non è riuscito. Di conseguenza, AutoSupport ha riportato i messaggi nella coda di consegna per un altro tentativo. È possibile visualizzare l'errore immettendo il <code>system node autosupport history show</code> comando. |
| trasmissione non riuscita | AutoSupport non ha recapitato il messaggio il numero di volte specificato e ha smesso di provare a recapitare il messaggio. È possibile visualizzare l'errore immettendo il <code>system node autosupport history show</code> comando.                                                    |
| ondemand: ignora          | Il messaggio AutoSupport è stato elaborato correttamente, ma il servizio AutoSupport su richiesta ha scelto di ignorarlo.                                                                                                                                                                 |

### 3. Eseguire una delle seguenti operazioni:

| Per questo stato                                | Eseguire questa operazione                                                                                                                                                                                                                        |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| inizializzazione o raccolta non riuscita        | Contattare il supporto NetApp perché AutoSupport non è in grado di generare il messaggio. Citare il seguente articolo della Knowledge base:<br><br><a href="#">"AutoSupport non riesce a consegnare: Lo stato è bloccato in inizializzazione"</a> |
| ignorare, riaccolare o trasmettere non riuscita | Verificare che le destinazioni siano configurate correttamente per SMTP, HTTP o HTTPS, poiché AutoSupport non è in grado di inviare il messaggio.                                                                                                 |

### Risolvere i problemi relativi all'erogazione dei messaggi AutoSupport su HTTP o HTTPS

Se il sistema non invia il messaggio AutoSupport previsto e si sta utilizzando HTTP o HTTPS, oppure se la funzione di aggiornamento automatico non funziona, è possibile verificare alcune impostazioni per risolvere il problema.



## Di cosa hai bisogno

La connettività di rete di base e la ricerca DNS dovrebbero essere state confermate:

- La LIF di gestione dei nodi deve essere attiva per lo stato operativo e amministrativo.
- È necessario essere in grado di eseguire il ping di un host funzionante sulla stessa subnet dalla LIF di gestione del cluster (non una LIF su uno dei nodi).
- È necessario essere in grado di eseguire il ping di un host funzionante al di fuori della subnet dalla LIF di gestione del cluster.
- È necessario essere in grado di eseguire il ping di un host funzionante al di fuori della subnet dalla LIF di gestione del cluster utilizzando il nome dell'host (non l'indirizzo IP).

## A proposito di questa attività

Questi passaggi si riferiscono ai casi in cui si è stabilito che AutoSupport è in grado di generare il messaggio, ma non è in grado di recapitare il messaggio su HTTP o HTTPS.

Se si verificano errori o non è possibile completare un passaggio di questa procedura, individuare e risolvere il problema prima di passare alla fase successiva.

## Fasi

1. Visualizzare lo stato dettagliato del sottosistema AutoSupport:

```
system node autosupport check show-details
```

Ciò include la verifica della connettività alle destinazioni AutoSupport inviando messaggi di test e fornendo un elenco di possibili errori nelle impostazioni di configurazione di AutoSupport.

2. Verificare lo stato della LIF di gestione dei nodi:

```
network interface show -home-node local -role node-mgmt -fields  
vserver,lif,status-oper,status-admin,address,role
```

Il status-oper e status-admin i campi devono restituire "up".

3. Registrare il nome SVM, il nome LIF e l'indirizzo IP LIF per un utilizzo successivo.
4. Assicurarsi che il DNS sia attivato e configurato correttamente:

```
vserver services name-service dns show
```

5. Risolvere eventuali errori restituiti dal messaggio AutoSupport:

```
system node autosupport history show -node * -fields node,seq-  
num,destination,last-update,status,error
```

Per assistenza nella risoluzione di eventuali errori restituiti, consultare ["Guida alla risoluzione di ONTAP AutoSupport \(Transport HTTPS and HTTP\)"](#).

6. Verificare che il cluster sia in grado di accedere a Internet e ai server necessari:

a. `network traceroute -lif node-management_LIF -destination DNS server`

b. `network traceroute -lif node_management_LIF -destination support.netapp.com`



L'indirizzo `support.netapp.com` di per sé non risponde al ping/traceroute, ma le informazioni per-hop sono preziose.

c. `system node autosupport show -fields proxy-url`

d. `network traceroute -node node_management_LIF -destination proxy_url`

Se uno di questi percorsi non funziona, provare lo stesso percorso da un host funzionante sulla stessa sottorete del cluster, utilizzando l'utility "traceroute" o "tracert" presente sulla maggior parte dei client di rete di terze parti. Ciò consente di determinare se il problema riguarda la configurazione di rete o la configurazione del cluster.

7. Se si utilizza HTTPS per il protocollo di trasporto AutoSupport, assicurarsi che il traffico HTTPS possa uscire dalla rete:

- a. Configurare un client Web sulla stessa subnet della LIF di gestione del cluster.

Assicurarsi che tutti i parametri di configurazione siano gli stessi valori della configurazione AutoSupport, incluso l'utilizzo dello stesso server proxy, nome utente, password e porta.

- b. Accesso `https://support.netapp.com` con il client web.

L'accesso dovrebbe essere riuscito. In caso contrario, assicurarsi che tutti i firewall siano configurati correttamente per consentire il traffico HTTPS e DNS e che il server proxy sia configurato correttamente. Per ulteriori informazioni sulla configurazione della risoluzione statica dei nomi per `support.netapp.com`, consultare l'articolo della Knowledge base "[Come aggiungere una voce HOST in ONTAP per support.netapp.com?](#)"

8. A partire da ONTAP 9.10.1, se è stata attivata la funzione di aggiornamento automatico, assicurarsi di disporre della connettività HTTPS per i seguenti URL aggiuntivi:

- <https://support-sg-emea.netapp.com>
- <https://support-sg-naeast.netapp.com>
- <https://support-sg-nawest.netapp.com>

## Risolvere i problemi relativi all'invio dei messaggi AutoSupport su SMTP

Se il sistema non riesce a inviare messaggi AutoSupport tramite SMTP, è possibile controllare diverse impostazioni per risolvere il problema.

### Di cosa hai bisogno

La connettività di rete di base e la ricerca DNS dovrebbero essere state confermate:

- La LIF di gestione dei nodi deve essere attiva per lo stato operativo e amministrativo.
- È necessario essere in grado di eseguire il ping di un host funzionante sulla stessa subnet dalla LIF di gestione del cluster (non una LIF su uno dei nodi).
- È necessario essere in grado di eseguire il ping di un host funzionante al di fuori della subnet dalla LIF di gestione del cluster.
- È necessario essere in grado di eseguire il ping di un host funzionante al di fuori della subnet dalla LIF di gestione del cluster utilizzando il nome dell'host (non l'indirizzo IP).

### A proposito di questa attività

Questa procedura si verifica nei casi in cui AutoSupport sia in grado di generare il messaggio, ma non è in

grado di recapitare il messaggio tramite SMTP.

Se si verificano errori o non è possibile completare un passaggio di questa procedura, individuare e risolvere il problema prima di passare alla fase successiva.

Tutti i comandi vengono immessi nell'interfaccia della riga di comando di ONTAP, se non diversamente specificato.

## Fasi

1. Verificare lo stato della LIF di gestione dei nodi:

```
network interface show -home-node local -role node-mgmt -fields  
vserver,lif,status-oper,status-admin,address,role
```

Il `status-oper` e `status-admin` i campi devono essere visualizzati `up`.

2. Registrare il nome SVM, il nome LIF e l'indirizzo IP LIF per un utilizzo successivo.
3. Assicurarsi che il DNS sia attivato e configurato correttamente:

```
vserver services name-service dns show
```

4. Visualizza tutti i server configurati per l'utilizzo da parte di AutoSupport:

```
system node autosupport show -fields mail-hosts
```

Registrare tutti i nomi dei server visualizzati.

5. Per ciascun server visualizzato al punto precedente, e. `support.netapp.com`, Assicurarsi che il server o l'URL possa essere raggiunto dal nodo:

```
network traceroute -node local -destination server_name
```

Se uno di questi percorsi non funziona, provare lo stesso percorso da un host funzionante sulla stessa sottorete del cluster, utilizzando l'utilità "traceroute" o "tracert" presente sulla maggior parte dei client di rete di terze parti. Ciò consente di determinare se il problema riguarda la configurazione di rete o la configurazione del cluster.

6. Accedere all'host designato come host di posta e assicurarsi che sia in grado di inviare richieste SMTP:

```
netstat -aAn|grep 25
```

25 È il numero della porta SMTP del listener.

Viene visualizzato un messaggio simile al seguente:

```
ff64878c tcp          0          0 *.25      *.*      LISTEN.
```

7. Da un altro host, aprire una sessione Telnet con la porta SMTP dell'host di posta:

```
telnet mailhost 25
```

Viene visualizzato un messaggio simile al seguente:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. Al prompt di telnet, assicurarsi che sia possibile trasmettere un messaggio dal proprio host di posta:

```
HELO domain_name
```

```
MAIL FROM: your_email_address
```

```
RCPT TO: autosupport@netapp.com
```

domain\_name è il nome di dominio della rete.

Se viene visualizzato un messaggio di errore che indica che l'inoltro è negato, l'inoltro non viene attivato sull'host di posta. Contattare l'amministratore di sistema.

9. Al prompt di telnet, inviare un messaggio di test:

```
DATA
```

```
SUBJECT: TESTING
```

```
THIS IS A TEST
```

```
.
```



Assicurarsi di inserire l'ultimo punto (.) su una linea da sola. Il punto indica all'host di posta che il messaggio è completo.

Se viene visualizzato un errore, l'host di posta non è configurato correttamente. Contattare l'amministratore di sistema.

10. Dall'interfaccia della riga di comando di ONTAP, inviare un messaggio di test AutoSupport a un indirizzo e-mail attendibile a cui si dispone dell'accesso:

```
system node autosupport invoke -node local -type test
```

11. Individuare il numero di sequenza del tentativo:

```
system node autosupport history show -node local -destination smtp
```

Individuare il numero di sequenza per il tentativo in base all'indicatore data e ora. Si tratta probabilmente del tentativo più recente.

12. Visualizza l'errore per il tentativo di messaggio di test:

```
system node autosupport history show -node local -seq-num seq_num -fields error
```

Se l'errore visualizzato è `Login denied`, Il server SMTP non accetta le richieste di invio dalla LIF di gestione del cluster. Se non si desidera passare all'utilizzo di HTTPS come protocollo di trasporto, contattare l'amministratore di rete del sito per configurare i gateway SMTP per risolvere il problema.

Se il test ha esito positivo, ma lo stesso messaggio inviato a `mailto:autosupport@netapp.com` non lo ha, assicurarsi che l'inoltro SMTP sia attivato su tutti gli host di posta SMTP oppure utilizzare HTTPS come protocollo di trasporto.

Se anche il messaggio all'account di posta elettronica amministrato in locale non riesce, verificare che i server SMTP siano configurati per inoltrare gli allegati con entrambe le caratteristiche:

- Il suffisso "7z"
- Il tipo MIME "application/x-7x-compressed".

## Risolvere i problemi del sottosistema AutoSupport

Il `system node check show` I comandi possono essere utilizzati per verificare e risolvere eventuali problemi relativi alla configurazione e all'erogazione di AutoSupport.

### Fase

1. Utilizzare i seguenti comandi per visualizzare lo stato del sottosistema AutoSupport.

| Utilizzare questo comando...                            | A tal fine...                                                                                                                                                                                                                |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>system node autosupport check show</code>         | Visualizza lo stato generale del sottosistema AutoSupport, ad esempio lo stato della destinazione HTTP o HTTPS AutoSupport, le destinazioni SMTP AutoSupport, il server AutoSupport OnDemand e la configurazione AutoSupport |
| <code>system node autosupport check show-details</code> | Visualizza lo stato dettagliato del sottosistema AutoSupport, ad esempio descrizioni dettagliate degli errori e delle azioni correttive                                                                                      |

## Monitoraggio dello stato di salute

### Monitorare lo stato di salute del sistema

I monitor dello stato di salute monitorano in modo proattivo determinate condizioni critiche nel cluster e avvisano se rilevano un guasto o un rischio. Se sono presenti avvisi attivi, lo stato di salute del sistema riporta uno stato degradato per il cluster. Gli avvisi includono le informazioni necessarie per rispondere a problemi di salute del sistema.

Se lo stato è degradato, è possibile visualizzare i dettagli del problema, incluse la probabile causa e le azioni di ripristino consigliate. Una volta risolto il problema, lo stato di salute del sistema torna automaticamente a OK.

Lo stato di salute del sistema riflette più monitor di stato separati. Uno stato degradato in un singolo monitor di salute causa uno stato degradato per lo stato generale del sistema.

Per ulteriori informazioni su come ONTAP supporta gli switch del cluster per il monitoraggio dello stato di salute del sistema nel cluster, fare riferimento alla *Hardware Universe*.

["Switch supportati in Hardware Universe"](#)

Per informazioni dettagliate sulle cause dei messaggi AutoSupport relativi al monitoraggio dello stato di salute degli switch del cluster e sulle azioni necessarie per risolvere questi avvisi, consultare l'articolo della Knowledge base.

["Messaggio AutoSupport: CSHM processo di monitoraggio dello stato di salute"](#)

## Come funziona il monitoraggio dello stato di salute

I singoli monitor dello stato di salute dispongono di una serie di policy che attivano avvisi quando si verificano determinate condizioni. La comprensione del funzionamento del monitoraggio dello stato di salute può aiutarti a rispondere ai problemi e a controllare gli avvisi futuri.

Il monitoraggio dello stato di salute è costituito dai seguenti componenti:

- Monitoraggio dello stato di salute individuale per sottosistemi specifici, ciascuno dei quali ha un proprio stato di salute

Ad esempio, il sottosistema di storage dispone di un monitor di stato della connettività del nodo.

- Un monitor generale dello stato di salute del sistema che consolida lo stato di salute dei singoli monitor

Uno stato degradato in un singolo sottosistema determina uno stato degradato per l'intero sistema. Se nessun sottosistema dispone di avvisi, lo stato generale del sistema è OK.

Ciascun monitor di stato è costituito dai seguenti elementi chiave:

- Avvisa che il monitor dello stato di salute può potenzialmente aumentare

Ogni avviso ha una definizione che include dettagli come la severità dell'avviso e la sua probabile causa.

- Policy di integrità che identificano quando viene attivato ogni avviso

Ogni policy di integrità ha un'espressione di regola, che è la condizione o la modifica esatta che attiva l'avviso.

Un monitor dello stato di salute monitora e convalida continuamente le risorse nel sottosistema per verificare la presenza di modifiche di stato o condizione. Quando una condizione o una modifica di stato corrisponde all'espressione di una regola in un criterio di integrità, il monitor dello stato genera un avviso. Un avviso causa il degrado dello stato di salute del sottosistema e dello stato di salute generale del sistema.

## Modi per rispondere agli avvisi sullo stato di salute del sistema

Quando si verifica un avviso di stato di salute del sistema, è possibile riconoscerlo, ottenere ulteriori informazioni, riparare la condizione sottostante ed evitare che si verifichi di nuovo.

Quando un monitor dello stato di salute genera un avviso, è possibile rispondere in uno dei seguenti modi:

- Ottenere informazioni sull'avviso, che includono la risorsa interessata, la severità dell'avviso, la probabile causa, il possibile effetto e le azioni correttive.
- Ottenere informazioni dettagliate sull'avviso, ad esempio l'ora in cui l'avviso è stato generato e se altri

hanno già confermato l'avviso.

- Ottenere informazioni sullo stato della risorsa o del sottosistema interessato, ad esempio uno shelf o un disco specifico.
- Riconoscere l'avviso per indicare che qualcuno sta lavorando al problema e identificarsi come "Acknowledger".
- Risolvere il problema adottando le azioni correttive fornite nell'avviso, ad esempio la risoluzione di un problema di connettività tramite il cablaggio.
- Eliminare l'avviso, se il sistema non lo ha cancellato automaticamente.
- Eliminare un avviso per evitare che influisca sullo stato di salute di un sottosistema.

La soppressione è utile quando si comprende un problema. Una volta eliminato un avviso, questo può comunque verificarsi, ma lo stato del sottosistema viene visualizzato come "ok-with-suppressed" (ok-with-suppressed), quando si verifica l'avviso sospeso.

## Personalizzazione degli avvisi sullo stato di salute del sistema

È possibile controllare quali avvisi vengono generati da un monitor dello stato di salute attivando e disattivando le policy di stato del sistema che definiscono quando vengono attivati gli avvisi. Ciò consente di personalizzare il sistema di monitoraggio dello stato di salute per il proprio ambiente specifico.

È possibile conoscere il nome di un criterio visualizzando informazioni dettagliate su un avviso generato o visualizzando le definizioni dei criteri per uno specifico Health monitor, nodo o ID avviso.

La disattivazione delle policy di integrità è diversa dalla sospensione degli avvisi. La soppressione di un avviso non influisce sullo stato di salute del sottosistema, ma può comunque verificarsi.

Se si disattiva un criterio, la condizione o lo stato definito nell'espressione della regola dei criteri non attiva più un avviso.

### Esempio di avviso che si desidera disattivare

Ad esempio, supponiamo che si verifichi un avviso non utile. Si utilizza `system health alert show -instance` Per ottenere l'ID policy per l'avviso. L'ID del criterio viene utilizzato in `system health policy definition show` per visualizzare le informazioni relative al criterio. Dopo aver esaminato l'espressione della regola e altre informazioni relative al criterio, si decide di disattivarlo. Si utilizza `system health policy definition modify` per disattivare il criterio.

## Modalità di attivazione degli avvisi di integrità per i messaggi e gli eventi AutoSupport

Gli avvisi sullo stato di salute del sistema attivano messaggi ed eventi AutoSupport nel sistema di gestione degli eventi, consentendo di monitorare lo stato di salute del sistema utilizzando messaggi AutoSupport e EMS, oltre a utilizzare direttamente il sistema di monitoraggio dello stato di salute.

Il sistema invia un messaggio AutoSupport entro cinque minuti da un avviso. Il messaggio AutoSupport include tutti gli avvisi generati dal precedente messaggio AutoSupport, ad eccezione degli avvisi che duplicano un avviso per la stessa risorsa e la causa probabile entro la settimana precedente.


Alcuni avvisi non attivano i messaggi AutoSupport. Un avviso non attiva un messaggio AutoSupport se la relativa policy di integrità disattiva l'invio di messaggi AutoSupport. Ad esempio, per impostazione predefinita, un criterio di integrità potrebbe disattivare i messaggi AutoSupport perché AutoSupport già genera un messaggio quando si verifica il problema. È possibile configurare i criteri per non attivare i messaggi AutoSupport utilizzando `system health policy definition modify` comando.

È possibile visualizzare un elenco di tutti i messaggi AutoSupport attivati dagli avvisi inviati la settimana precedente utilizzando `system health autosupport trigger history show` comando.

Gli avvisi attivano anche la generazione di eventi al sistema EMS. Ogni volta che viene creato un avviso e ogni volta che viene cancellato, viene generato un evento.

## Monitoraggio dello stato dei cluster disponibili

Esistono diversi monitor di stato che monitorano diverse parti di un cluster. I monitor di stato consentono di eseguire il ripristino dagli errori all'interno dei sistemi ONTAP rilevando gli eventi, inviando avvisi ed eliminando gli eventi non appena vengono eliminati.

| Nome del monitor di stato (identificatore) | Nome del sottosistema (identificatore) | Scopo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Switch del cluster (switch del cluster)    | Switch (stato dello switch)            | <p>Monitora gli switch di rete del cluster e gli switch di rete di gestione per la temperatura, l'utilizzo, la configurazione dell'interfaccia, la ridondanza (solo switch di rete del cluster) e il funzionamento di ventole e alimentatori. Il monitor di stato dello switch del cluster comunica con gli switch tramite SNMP. SNMPv2c è l'impostazione predefinita.</p> <div>  <p>A partire da ONTAP 9.2, questo monitor è in grado di rilevare e segnalare quando uno switch del cluster si è riavviato dall'ultimo periodo di polling.</p> </div> |
| Fabric MetroCluster                        | Switch                                 | Monitora la topologia del fabric back-end di configurazione MetroCluster e rileva configurazioni errate, come cablaggio e zoning errati e errori ISL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



| Nome del monitor di stato (identificatore)  | Nome del sottosistema (identificatore)                                                                                  | Scopo                                                                                               |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Salute di MetroCluster                      | Interconnessione, RAID e storage                                                                                        | Monitora adattatori FC-VI, adattatori FC Initiator, aggregati e dischi sinistri e porte tra cluster |
| Connettività del nodo (connessione al nodo) | Operazioni CIFS senza interruzioni (CIFS-NDO)                                                                           | Monitora le connessioni SMB per le operazioni senza interruzioni alle applicazioni Hyper-V.         |
| Storage (SAS-Connect)                       | Monitora shelf, dischi e adattatori a livello di nodo per verificare la presenza di percorsi e connessioni appropriati. | Sistema                                                                                             |
| non applicabile                             | Aggrega le informazioni provenienti da altri monitor dello stato di salute.                                             | Connettività del sistema (connessione al sistema)                                                   |

## Ricevere automaticamente gli avvisi sullo stato di salute del sistema

È possibile visualizzare manualmente gli avvisi sullo stato di salute del sistema utilizzando `system health alert show` comando. Tuttavia, è necessario iscriversi a specifici messaggi EMS (Event Management System) per ricevere automaticamente le notifiche quando un monitor dello stato di salute genera un avviso.

### A proposito di questa attività

La seguente procedura illustra come impostare le notifiche per tutti i messaggi `hm.alert.Raised` e per tutti i messaggi `hm.alert.Cleared`.

Tutti i messaggi `hm.alert.Raised` e tutti i messaggi `hm.alert.Cleared` includono una trap SNMP. I nomi dei trap SNMP sono `HealthMonitorAlertRaised` e `HealthMonitorAlertCleared`. Per informazioni sui trap SNMP, consultare la *Network Management Guide*.

### Fasi

1. Utilizzare `event destination create` Per definire la destinazione a cui si desidera inviare i messaggi EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Utilizzare `event route add-destinations` per instradare `hm.alert.raised` e il `hm.alert.cleared` a una destinazione.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

## Rispondere a uno stato di salute del sistema degradato

Quando lo stato di salute del sistema è degradato, è possibile visualizzare avvisi, leggere la causa probabile e le azioni correttive, visualizzare informazioni sul sottosistema degradato e risolvere il problema. Vengono inoltre visualizzati gli avvisi soppressi, in modo da poterli modificare e verificare se sono stati riconosciuti.

### A proposito di questa attività

È possibile scoprire che è stato generato un avviso visualizzando un messaggio AutoSupport o un evento EMS oppure utilizzando `system health` comandi.

### Fasi

1. Utilizzare `system health alert show` per visualizzare gli avvisi che compromettono lo stato di salute del sistema.
2. Leggi la probabile causa, il possibile effetto e le azioni correttive dell'avviso per determinare se puoi risolvere il problema o se hai bisogno di ulteriori informazioni.
3. Per ulteriori informazioni, utilizzare `system health alert show -instance` per visualizzare ulteriori informazioni disponibili per l'avviso.
4. Utilizzare `system health alert modify` con il `-acknowledge` parametro per indicare che si sta lavorando a un avviso specifico.
5. Intraprendere un'azione correttiva per risolvere il problema come descritto in `Corrective Actions` nel campo dell'avviso.

Le azioni correttive potrebbero includere il riavvio del sistema.

Una volta risolto il problema, l'avviso viene cancellato automaticamente. Se il sottosistema non dispone di altri avvisi, lo stato del sottosistema cambia in OK. Se lo stato di tutti i sottosistemi è corretto, lo stato generale del sistema diventa OK.

6. Utilizzare `system health status show` per confermare che lo stato di salute del sistema è OK.

Se lo stato di salute del sistema non è OK, ripetere questa procedura.

## Esempio di risposta a uno stato di salute del sistema degradato

Esaminando un esempio specifico di stato di salute del sistema degradato causato da uno shelf che non dispone di due percorsi per un nodo, è possibile visualizzare la CLI quando si risponde a un avviso.

Dopo aver avviato ONTAP, controllare lo stato del sistema e verificare che lo stato sia degradato:

```
cluster1::>system health status show
Status
-----
degraded
```

Mostra gli avvisi per scoprire dove si trova il problema e scopri che lo shelf 2 non ha due percorsi per il node1:

```
cluster1::>system health alert show
Node: node1
Resource: Shelf ID 2
Severity: Major
Indication Time: Mon Nov 10 16:48:12 2013
Probable Cause: Disk shelf 2 does not have two paths to controller
node1.
Possible Effect: Access to disk shelf 2 via controller node1 will be
lost with a single hardware component failure (e.g.
cable, HBA, or IOM failure).
Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
3. Reboot the halted controllers.
4. Contact support personnel if the alert persists.
```

Vengono visualizzati i dettagli dell'avviso per ottenere ulteriori informazioni, tra cui l'ID dell'avviso:

```

cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
    Node: node1
    Monitor: node-connect
    Alert ID: DualPathToDiskShelf_Alert
    Alerting Resource: 50:05:0c:c1:02:00:0f:02
    Subsystem: SAS-connect
    Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
    Probable Cause: Connection_establishment_error
    Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
    Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
    hardware component failure (e.g. cable, HBA, or IOM failure).
    Acknowledge: false
    Suppress: false
    Policy: DualPathToDiskShelf_Policy
    Acknowledger: -
    Suppressor: -
    Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
    Alerting Resource Name: Shelf ID 2

```

L'utente riconosce l'avviso per indicare che si sta lavorando.

```

cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true

```

Riparare il cablaggio tra lo shelf 2 e il nodo 1, quindi riavviare il sistema. Quindi, controllare nuovamente lo stato del sistema e verificare che lo stato sia OK:

```
cluster1::>system health status show
Status
-----
OK
```

## Configurare il rilevamento degli switch di rete di gestione e del cluster

Il monitor di stato dello switch del cluster tenta automaticamente di rilevare gli switch del cluster e della rete di gestione utilizzando il protocollo Cisco Discovery (CDP). È necessario configurare il monitor dello stato di salute se non riesce a rilevare automaticamente uno switch o se non si desidera utilizzare CDP per il rilevamento automatico.

### A proposito di questa attività

Il `system cluster-switch show` il comando elenca gli switch rilevati dal monitor dello stato di salute. Se non viene visualizzato uno switch che si prevede venga visualizzato nell'elenco, il monitor dello stato di salute non può rilevarlo automaticamente.

### Fasi

1. Se si desidera utilizzare CDP per il rilevamento automatico, attenersi alla seguente procedura:

- a. Assicurarsi che il protocollo Cisco Discovery Protocol (CDP) sia attivato sugli switch.

Per istruzioni, consultare la documentazione dello switch.

- b. Eseguire il seguente comando su ciascun nodo del cluster per verificare se CDP è attivato o disattivato:

```
run -node node_name -command options cdpd.enable
```

Se CDP è attivato, passare alla fase d. Se CDP è disattivato, passare alla fase c.

- c. Eseguire il seguente comando per attivare CDP:

```
run -node node_name -command options cdpd.enable on
```

Attendere cinque minuti prima di passare alla fase successiva.

- a. Utilizzare `system cluster-switch show` Per verificare se ONTAP è in grado di rilevare automaticamente gli switch.

2. Se il monitor dello stato di salute non rileva automaticamente uno switch, utilizzare `system cluster-switch create` comando per configurare il rilevamento dello switch:

```
cluster1::> system cluster-switch create -device switch1 -address
192.0.2.250 -snmp-version SNMPv2c -community cshml! -model NX5020 -type
cluster-network
```

Attendere cinque minuti prima di passare alla fase successiva.

3. Utilizzare `system cluster-switch show` Per verificare che ONTAP sia in grado di rilevare lo switch per cui sono state aggiunte informazioni.

#### Al termine

Verificare che lo Health monitor sia in grado di monitorare gli switch.

## Verificare il monitoraggio degli switch del cluster e della rete di gestione

Il monitor di stato dello switch del cluster tenta automaticamente di monitorare gli switch che rileva; tuttavia, il monitoraggio potrebbe non verificarsi automaticamente se gli switch non sono configurati correttamente. Verificare che il monitor dello stato di salute sia configurato correttamente per monitorare gli switch.

#### Fasi

1. Per identificare gli switch rilevati dal monitor di stato dello switch del cluster, immettere il seguente comando:

##### ONTAP 9.8 e versioni successive

```
system switch ethernet show
```

##### ONTAP 9.7 e versioni precedenti

```
system cluster-switch show
```

Se il `Model` visualizza il valore `OTHER`, Quindi ONTAP non può monitorare lo switch. ONTAP imposta il valore su `OTHER` se uno switch che rileva automaticamente non è supportato per il monitoraggio dello stato di salute.



Se uno switch non viene visualizzato nell'output del comando, è necessario configurare il rilevamento dello switch.

2. Eseguire l'aggiornamento al software dello switch più recente supportato e fare riferimento al file di configurazione (RCF) dal sito del supporto NetApp.

#### ["Pagina Support Downloads di NetApp"](#)

La stringa `community` nell'RCF dello switch deve corrispondere alla stringa `community` configurata per l'utilizzo da parte del monitor di stato. Per impostazione predefinita, il monitor di stato utilizza la stringa di comunità `cshml!`.



Attualmente, il monitor di stato supporta solo SNMPv2.

Se è necessario modificare le informazioni relative a uno switch monitorato dal cluster, è possibile modificare la stringa di comunità utilizzata da Health monitor utilizzando il seguente comando:

**ONTAP 9.8 e versioni successive**

```
system switch ethernet modify
```

**ONTAP 9.7 e versioni precedenti**

```
system cluster-switch modify
```

3. Verificare che la porta di gestione dello switch sia collegata alla rete di gestione.

Questa connessione è necessaria per eseguire query SNMP.

## Comandi per il monitoraggio dello stato di salute del sistema

È possibile utilizzare `system health` comandi per visualizzare informazioni sullo stato delle risorse di sistema, rispondere agli avvisi e configurare gli avvisi futuri. L'utilizzo dei comandi CLI consente di visualizzare informazioni dettagliate sulla configurazione del monitoraggio dello stato di salute. Le pagine man dei comandi contengono ulteriori informazioni.

### Visualizza lo stato dello stato di salute del sistema

| Se si desidera...                                                                                              | Utilizzare questo comando...              |
|----------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Visualizza lo stato di salute del sistema, che riflette lo stato generale dei singoli monitor di salute        | <code>system health status show</code>    |
| Visualizza lo stato di salute dei sottosistemi per i quali è disponibile il monitoraggio dello stato di salute | <code>system health subsystem show</code> |

### Visualizza lo stato della connettività del nodo

| Se si desidera...                                                                                                                                                                               | Utilizzare questo comando...                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Visualizza dettagli sulla connettività dal nodo allo shelf di storage, tra cui informazioni sulle porte, velocità della porta HBA, throughput i/o e velocità delle operazioni di i/o al secondo | <code>storage shelf show -connectivity</code><br><br>Utilizzare <code>-instance</code> parametro per visualizzare informazioni dettagliate su ogni shelf. |
| Visualizza informazioni su dischi e LUN di array, inclusi lo spazio utilizzabile, i numeri di shelf e alloggiamenti e il nome del nodo proprietario                                             | <code>storage disk show</code><br><br>Utilizzare <code>-instance</code> per visualizzare informazioni dettagliate su ciascun disco.                       |
| Visualizza informazioni dettagliate sulle porte dello shelf storage, tra cui tipo di porta, velocità e stato                                                                                    | <code>storage port show</code><br><br>Utilizzare <code>-instance</code> parametro per visualizzare informazioni dettagliate su ciascun adattatore.        |

## Gestire il rilevamento di switch di rete per cluster, storage e gestione

| Se si desidera...                                                                                                                                                                                                                                                                                                                                       | Utilizzare questo comando.<br>(ONTAP 9.8 e versioni successive) | Utilizzare questo comando.<br>(ONTAP 9.7 e versioni precedenti) |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------------------------------------------------|
| Visualizza gli switch che il cluster monitora                                                                                                                                                                                                                                                                                                           | <code>system switch ethernet show</code>                        | <code>system cluster-switch show</code>                         |
| Visualizzare gli switch attualmente monitorati dal cluster, inclusi gli switch cancellati (visualizzati nella colonna Reason (motivo) nell'output del comando) e le informazioni di configurazione necessarie per l'accesso di rete al cluster e agli switch di rete di gestione.<br><br>Questo comando è disponibile a livello di privilegio avanzato. | <code>system switch ethernet show-all</code>                    | <code>system cluster-switch show-all</code>                     |
| Configurare il rilevamento di uno switch non rilevato                                                                                                                                                                                                                                                                                                   | <code>system switch ethernet create</code>                      | <code>system cluster-switch create</code>                       |
| Modificare le informazioni relative a uno switch che il cluster monitora (ad esempio, nome del dispositivo, indirizzo IP, versione SNMP e stringa di comunità)                                                                                                                                                                                          | <code>system switch ethernet modify</code>                      | <code>system cluster-switch modify</code>                       |
| Disattiva il monitoraggio di uno switch                                                                                                                                                                                                                                                                                                                 | <code>system switch ethernet modify -disable-monitoring</code>  | <code>system cluster-switch modify -disable-monitoring</code>   |
| Disattivare il rilevamento e il monitoraggio di uno switch ed eliminare le informazioni di configurazione dello switch                                                                                                                                                                                                                                  | <code>system switch ethernet delete</code>                      | <code>system cluster-switch delete</code>                       |
| Rimuovere in modo permanente le informazioni di configurazione dello switch memorizzate nel database (in questo modo si riattiva il rilevamento automatico dello switch)                                                                                                                                                                                | <code>system switch ethernet delete -force</code>               | <code>system cluster-switch delete -force</code>                |
| Abilitare la registrazione automatica per l'invio con messaggi AutoSupport.                                                                                                                                                                                                                                                                             | <code>system switch ethernet log</code>                         | <code>system cluster-switch log</code>                          |





## Rispondere agli avvisi generati


| Se si desidera...                                                                                                                                                | Utilizzare questo comando...                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Visualizza le informazioni sugli avvisi generati, ad esempio la risorsa e il nodo in cui è stato attivato l'avviso, la gravità e la probabile causa dell'avviso  | <code>system health alert show</code>                       |
| Visualizza le informazioni relative a ciascun avviso generato                                                                                                    | <code>system health alert show -instance</code>             |
| Indica che qualcuno sta lavorando a un avviso                                                                                                                    | <code>system health alert modify</code>                     |
| Riconoscere un avviso                                                                                                                                            | <code>system health alert modify -acknowledge</code>        |
| Eliminare un avviso successivo in modo che non influisca sullo stato di salute di un sottosistema                                                                | <code>system health alert modify -suppress</code>           |
| Eliminare un avviso non cancellato automaticamente                                                                                                               | <code>system health alert delete</code>                     |
| Visualizza le informazioni sui messaggi AutoSupport attivati nell'ultima settimana, ad esempio per determinare se un avviso ha attivato un messaggio AutoSupport | <code>system health autosupport trigger history show</code> |

## Configurare gli avvisi futuri

| Se si desidera...                                                                                             | Utilizzare questo comando...                        |
|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| Attivare o disattivare il criterio che controlla se uno stato di risorsa specifico genera un avviso specifico | <code>system health policy definition modify</code> |

## Visualizza informazioni sulla configurazione del monitoraggio dello stato di salute

| Se si desidera...                                                                                | Utilizzare questo comando...                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Visualizzare informazioni sui monitor di stato, ad esempio nodi, nomi, sottosistemi e stato      | <code>system health config show</code><br><br> Utilizzare <code>-instance</code> parametro per visualizzare informazioni dettagliate su ciascun monitor di salute.                |
| Visualizza informazioni sugli avvisi potenzialmente generati da un monitor dello stato di salute | <code>system health alert definition show</code><br><br> Utilizzare <code>-instance</code> parametro per visualizzare informazioni dettagliate su ciascuna definizione di avviso. |

| Se si desidera...                                                                                                             | Utilizzare questo comando...                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Visualizza informazioni sui criteri di monitoraggio dello stato di salute, che determinano quando vengono generati gli avvisi | <pre>system health policy definition show</pre> <div>  <p>Utilizzare <code>-instance</code> parametro per visualizzare informazioni dettagliate su ogni policy. Utilizzare altri parametri per filtrare l'elenco degli avvisi, ad esempio in base allo stato della policy (attivato o meno), al monitor dello stato di salute, agli avvisi e così via.</p> </div> |

## Visualizzare le informazioni ambientali

I sensori consentono di monitorare i componenti ambientali del sistema. Le informazioni che è possibile visualizzare sui sensori ambientali includono tipo, nome, stato, valore e avvisi di soglia.

### Fase

1. Per visualizzare informazioni sui sensori ambientali, utilizzare `system node environment sensors show` comando.

## Analisi del file system

### Panoramica di file System Analytics

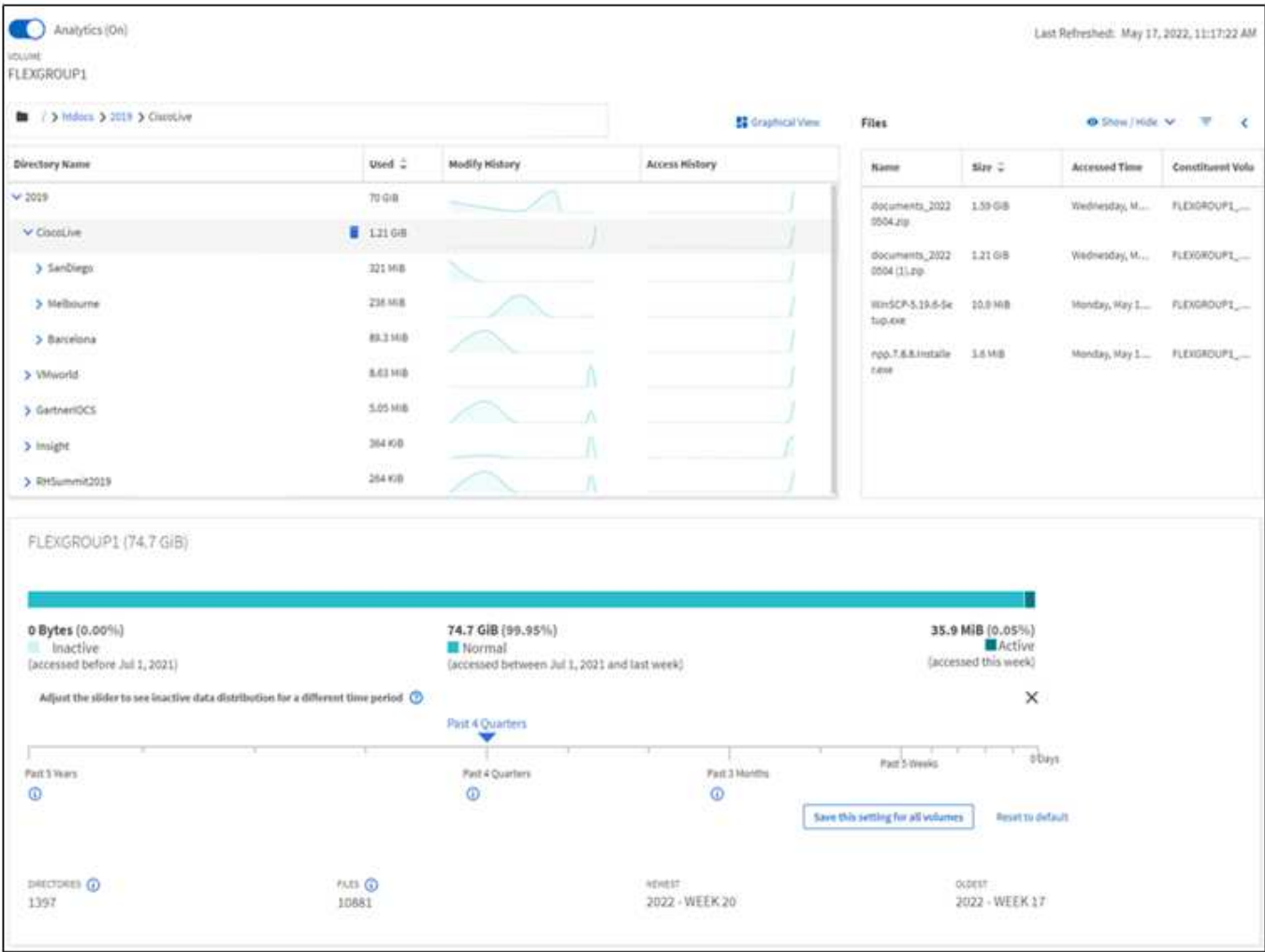
L'analisi del file system (FSA) è stata introdotta per la prima volta in ONTAP 9.8 per fornire visibilità in tempo reale sull'utilizzo dei file e sulle tendenze della capacità dello storage all'interno dei volumi ONTAP FlexGroup o FlexVol. Questa funzionalità nativa elimina la necessità di strumenti esterni e fornisce informazioni chiave sull'utilizzo dello storage e sull'opportunità di ottimizzare lo storage in base alle esigenze aziendali.

Con FSA, è possibile ottenere visibilità a tutti i livelli della gerarchia di file system di un volume in NAS. Ad esempio, è possibile ottenere informazioni sull'utilizzo e sulla capacità a livello di Storage VM (SVM), volume, directory e file. Puoi utilizzare FSA per rispondere a domande come:

- Cosa sta riempiendo lo storage e ci sono file di grandi dimensioni che è possibile spostare in un'altra posizione di storage?
- Quali sono i volumi, le directory e i file più attivi? Le performance dello storage sono ottimizzate per le esigenze dei miei utenti?
- Quanti dati sono stati aggiunti nell'ultimo mese?
- Chi sono i miei utenti di storage più attivi o meno attivi?
- Quanti dati inattivi o inattivi si trovano nello storage primario? Posso spostare questi dati in un cold Tier a costi inferiori?
- Le modifiche pianificate alla qualità del servizio avranno un impatto negativo sull'accesso ai file critici e ad accesso frequente?

L'analisi del file system è integrata in Gestione sistema ONTAP. Le visualizzazioni di System Manager offrono:

- Visibilità in tempo reale per una gestione e un funzionamento dei dati efficaci
- Raccolta e aggregazione dei dati in tempo reale
- Dimensioni e conteggi delle sottodirectory e dei file, insieme ai profili di performance associati
- Istogrammi di età dei file per la cronologia delle modifiche e degli accessi



Tipi di volume supportati

L'analisi del file system è progettata per fornire visibilità sui volumi con dati NAS attivi, ad eccezione delle cache FlexCache e dei volumi di destinazione SnapMirror.

Disponibilità delle funzionalità di analisi del file system

Ogni release di ONTAP amplia l'ambito dell'analisi del file system.

|                                   | ONTAP 9.14.1 | ONTAP 9.13.1 | ONTAP 9.12.1 | ONTAP 9.11.1 | ONTAP 9.10.1 | ONTAP 9.9.1 | ONTAP 9.8 |
|-----------------------------------|--------------|--------------|--------------|--------------|--------------|-------------|-----------|
| Visualizzazione in System Manager | ✓            | ✓            | ✓            | ✓            | ✓            | ✓           | ✓         |

|                                                                             | ONTAP<br>9.14.1 | ONTAP<br>9.13.1 | ONTAP<br>9.12.1 | ONTAP<br>9.11.1 | ONTAP<br>9.10.1 | ONTAP<br>9.9.1 | ONTAP<br>9.8 |
|-----------------------------------------------------------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|----------------|--------------|
| Analisi della capacità                                                      | ✓               | ✓               | ✓               | ✓               | ✓               | ✓              | ✓            |
| Informazioni sui dati inattivi                                              | ✓               | ✓               | ✓               | ✓               | ✓               | ✓              | ✓            |
| Supporto per volumi in transizione da Data ONTAP 7-Mode                     | ✓               | ✓               | ✓               | ✓               | ✓               | ✓              |              |
| Possibilità di personalizzare il periodo inattivo in System Manager         | ✓               | ✓               | ✓               | ✓               | ✓               | ✓              |              |
| Monitoraggio delle attività a livello di volume                             | ✓               | ✓               | ✓               | ✓               | ✓               |                |              |
| Scarica i dati di Activity Tracking in CSV                                  | ✓               | ✓               | ✓               | ✓               | ✓               |                |              |
| Monitoraggio delle attività a livello di SVM                                | ✓               | ✓               | ✓               | ✓               |                 |                |              |
| Tempistiche                                                                 | ✓               | ✓               | ✓               | ✓               |                 |                |              |
| Analisi dell'utilizzo                                                       | ✓               | ✓               | ✓               |                 |                 |                |              |
| Opzione per attivare l'analisi del file system per impostazione predefinita | ✓               | ✓               |                 |                 |                 |                |              |
| Monitor di avanzamento scansione inizializzazione                           | ✓               |                 |                 |                 |                 |                |              |

**Scopri di più su file System Analytics**

# ONTAP File System Analytics



Daniel Tennant  
Director of Software Engineering  
December 13, 2020



© 2020 NetApp, Inc. All rights reserved. — NETAPP CONFIDENTIAL —



## Ulteriori letture

- ["TR 4687: Linee guida sulle Best practice per l'analisi del file system ONTAP"](#)
- ["Knowledge base: Latenza elevata o fluttuante dopo l'attivazione dell'analisi del file system NetApp ONTAP"](#)

## Abilita analisi del file system

Per raccogliere e visualizzare i dati di utilizzo, ad esempio l'analisi della capacità, è necessario attivare l'analisi del file system su un volume.

### A proposito di questa attività

- A partire da ONTAP 9.8, è possibile attivare l'analisi del file system su un volume nuovo o esistente. Se si aggiorna un sistema a ONTAP 9.8 o versioni successive, assicurarsi che tutti i processi di aggiornamento siano stati completati prima di attivare l'analisi del file system.
- A seconda delle dimensioni e dei contenuti del volume, l'abilitazione delle analisi potrebbe richiedere tempo mentre ONTAP elabora i dati esistenti nel volume. System Manager visualizza l'avanzamento e presenta i dati di analisi una volta completati. Per informazioni più precise sull'avanzamento dell'inizializzazione, utilizzare il comando `ONTAP CLI volume analytics show`.

A partire da ONTAP 9.14.1, ONTAP fornisce il monitoraggio dell'avanzamento della scansione di inizializzazione, oltre alle notifiche sugli eventi di rallentamento che influiscono sull'avanzamento della scansione.

Per ulteriori considerazioni relative alla scansione di inizializzazione, vedere [Considerazioni sulla scansione](#).

## Fasi

È possibile attivare l'analisi del file system con Gestione di sistema di ONTAP o l'interfaccia CLI.

## System Manager

| In ONTAP 9.8 e 9.9.1                                                                                                                                                                                                                                   | A partire da ONTAP 9.10.1                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Selezionare <b>Storage &gt; Volumes</b> (archiviazione > volumi). 2. Selezionare il volume desiderato, quindi selezionare <b>Explorer</b> . 3. Selezionare <b>Enable Analytics</b> (attiva analisi) o <b>Disable Analytics</b> (Disattiva analisi). | 1. Selezionare <b>Storage &gt; Volumes</b> (archiviazione > volumi). 2. Selezionare il volume desiderato. Dal menu dei singoli volumi, selezionare <b>file System &gt; Explorer</b> . 3. Selezionare <b>Enable Analytics</b> (attiva analisi) o <b>Disable Analytics</b> (Disattiva analisi). |

## CLI

### Abilitare l'analisi del file system con la CLI

1. Eseguire il seguente comando:

```
volume analytics on -vserver svm_name -volume volume_name [-foreground {true|false}]`Per impostazione predefinita, il comando viene eseguito in primo piano; ONTAP visualizza l'avanzamento e presenta i dati di analisi al termine. Per informazioni più precise, è possibile eseguire il comando in background utilizzando `-foreground false e quindi utilizzare volume analytics show Per visualizzare l'avanzamento dell'inizializzazione nella CLI.
```

2. Dopo aver attivato correttamente l'analisi del file system, utilizzare Gestione sistema o l'API REST di ONTAP per visualizzare i dati analitici.


## Modificare le impostazioni predefinite di file System Analytics

A partire da ONTAP 9.13.1, è possibile modificare le impostazioni SVM o cluster per attivare l'analisi del file system per impostazione predefinita sui nuovi volumi.

## System Manager

Se si utilizza System Manager, è possibile modificare le impostazioni della macchina virtuale dello storage o del cluster per abilitare l'analisi della capacità e il monitoraggio delle attività alla creazione del volume per impostazione predefinita. L'abilitazione predefinita si applica solo ai volumi creati dopo la modifica delle impostazioni, non ai volumi esistenti.

### Modificare le impostazioni di analisi del file system su un cluster

1. In System Manager, accedere a **Impostazioni cluster**.
2. In **Impostazioni cluster**, esaminare la scheda Impostazioni file system. Per modificare le impostazioni, selezionare  icona.
3. Nel campo **monitoraggio attività**, immettere i nomi delle SVM per cui attivare il monitoraggio attività per impostazione predefinita. Se si lascia il campo vuoto, il monitoraggio attività viene disattivato su tutte le SVM.

Deselezionare la casella **Enable on new storage vms** (attiva sulle nuove macchine virtuali storage) per disattivare il monitoraggio delle attività per impostazione predefinita sulle nuove macchine virtuali storage.

4. Nel campo **Analytics**, immettere i nomi delle VM di storage per le quali si desidera abilitare l'analisi della capacità per impostazione predefinita. Lasciando il campo vuoto, l'analisi della capacità viene disattivata su tutte le SVM.

Deselezionare la casella **Enable on new storage VM** (attiva sulle nuove macchine virtuali storage) per disattivare l'analisi della capacità per impostazione predefinita sulle nuove macchine virtuali storage.

5. Selezionare **Salva**.

### Modificare le impostazioni di analisi del file system su una SVM

1. Selezionare la SVM che si desidera modificare, quindi **Impostazioni Storage VM**.
2. Nella scheda **analisi del file system**, utilizzare i pulsanti per attivare o disattivare il monitoraggio delle attività e l'analisi della capacità per tutti i nuovi volumi sulla VM di storage.

## CLI

È possibile configurare la VM di storage per abilitare l'analisi del file system per impostazione predefinita sui nuovi volumi utilizzando l'interfaccia CLI di ONTAP.

### Abilitare l'analisi del file system per impostazione predefinita su una SVM

1. Modificare la SVM per attivare l'analisi della capacità e il monitoraggio delle attività per impostazione predefinita su tutti i volumi appena creati:  

```
vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto-enable-analytics true
```

## Visualizzare l'attività del file system

Dopo aver attivato file System Analytics (FSA), è possibile visualizzare il contenuto della directory principale di un volume selezionato, ordinato in base allo spazio utilizzato in ogni sottostruttura.

Selezionare qualsiasi oggetto del file system per esplorare il file system e visualizzare informazioni dettagliate su ciascun oggetto in una directory. Le informazioni sulle directory possono anche essere visualizzate graficamente. Nel tempo, vengono visualizzati i dati storici per ogni sottostruttura. Lo spazio utilizzato non viene ordinato se sono presenti più di 3000 directory.

## Esplora risorse

La schermata file System Analytics **Explorer** è composta da tre aree:

- Visualizzazione ad albero di directory e sottodirectory; elenco espandibile con nome, dimensione, cronologia delle modifiche e cronologia degli accessi.
- File; mostra nome, dimensione e tempo di accesso per l'oggetto selezionato nell'elenco di directory.
- Confronto dei dati attivi e inattivi per l'oggetto selezionato nell'elenco delle directory.

A partire da ONTAP 9.9.1, è possibile personalizzare l'intervallo da segnalare. Il valore predefinito è di un anno. In base a queste personalizzazioni, è possibile intraprendere azioni correttive, come lo spostamento di volumi e la modifica della policy di tiering.

L'ora di accesso viene visualizzata per impostazione predefinita. Tuttavia, se l'impostazione predefinita del volume è stata modificata dall'interfaccia CLI (impostando il `-atime-update` opzione a `false` con `volume modify` comando), quindi viene visualizzata solo l'ora dell'ultima modifica. Ad esempio:

- La vista ad albero non visualizza la **cronologia di accesso**.
- La vista file viene modificata.
- La vista dati attiva/inattiva si basa sull'ora modificata (`mtime`).

Utilizzando queste schermate, è possibile esaminare quanto segue:

- Le posizioni del file system occupano la maggior parte dello spazio
- Informazioni dettagliate su un albero di directory, incluso il numero di file e sottodirectory all'interno di directory e sottodirectory
- Posizioni del file system che contengono dati vecchi (ad esempio, scratch, temp o log tree)

Tenere a mente i seguenti punti quando si interpreta l'output FSA:

- FSA mostra dove e quando i tuoi dati sono in uso, non la quantità di dati che vengono elaborati. Ad esempio, un elevato consumo di spazio da parte dei file recentemente utilizzati o modificati non indica necessariamente elevati carichi di elaborazione del sistema.
- Il modo in cui la scheda **Volume Explorer** calcola il consumo di spazio per FSA potrebbe differire da altri strumenti. In particolare, potrebbero esserci differenze significative rispetto al consumo riportato in **Volume Overview** se il volume dispone delle funzionalità di efficienza dello storage abilitate. Questo perché la scheda **Volume Explorer** non include i risparmi in termini di efficienza.
- A causa delle limitazioni di spazio nella visualizzazione della directory, non è possibile visualizzare una profondità della directory superiore a 8 livelli nella *visualizzazione elenco*. Per visualizzare le directory più profonde di 8 livelli, passare a *Graphical View*, individuare la directory desiderata, quindi tornare a *List View*. In questo modo si otterrà ulteriore spazio sullo schermo.

## Fasi

1. Visualizzare il contenuto della directory principale di un volume selezionato:



| In ONTAP 9.8 e 9.9.1                                                                                                                       | A partire da ONTAP 9.10.1                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fare clic su <b>Storage &gt; Volumes</b> (archiviazione > volumi), selezionare il volume desiderato, quindi fare clic su <b>Explorer</b> . | Selezionare <b>Storage &gt; Volumes</b> (archiviazione > volumi), quindi selezionare il volume desiderato. Dal menu dei singoli volumi, selezionare <b>file System &gt; Explorer</b> . |

## Attiva monitoraggio attività

A partire da ONTAP 9.10.1, l'analisi del file system include una funzione di monitoraggio delle attività che consente di identificare gli oggetti hot e scaricare i dati come file CSV. A partire da ONTAP 9.11.1, il monitoraggio delle attività viene esteso all'ambito SVM. Inoltre, a partire da ONTAP 9.11.1, System Manager dispone di una timeline per il monitoraggio delle attività, che consente di esaminare fino a cinque minuti di dati di monitoraggio delle attività.

Il monitoraggio delle attività consente il monitoraggio in quattro categorie:

- Directory
- File
- Client
- Utenti

Per ciascuna categoria monitorata, Activity Tracking visualizza IOPS di lettura, IOPS di scrittura, risultati di lettura e risultati di scrittura. Le query su Activity Tracking si aggiornano ogni 10 - 15 secondi relativi agli hot spot rilevati nel sistema nell'intervallo di cinque secondi precedente.

Le informazioni di monitoraggio dell'attività sono approssimative e la precisione dei dati dipende dalla distribuzione del traffico i/o in entrata.

Quando si visualizza Activity Tracking in System Manager a livello di volume, viene aggiornato attivamente solo il menu del volume espanso. Se la vista di qualsiasi volume viene compressa, non si aggiornerà fino a quando la visualizzazione del volume non viene espansa. È possibile interrompere gli aggiornamenti con il pulsante **Pause Refresh** (Pausa aggiornamento\*). I dati delle attività possono essere scaricati in formato CSV che visualizza tutti i dati point-in-time acquisiti per il volume selezionato.

Con la funzione timeline disponibile a partire da ONTAP 9.11.1, è possibile registrare l'attività dell'hotspot su un volume o una SVM, aggiornando continuamente circa ogni cinque secondi e mantenendo i cinque minuti precedenti di dati. I dati della timeline vengono conservati solo per i campi che sono aree visibili della pagina. Se si comprime una categoria di rilevamento o si scorre in modo che la timeline non sia visualizzata, la timeline interrompe la raccolta dei dati. Per impostazione predefinita, le tempistiche sono disattivate e vengono disattivate automaticamente quando ci si allontana dalla scheda Activity (attività).

## Attiva monitoraggio attività per un singolo volume

È possibile attivare il monitoraggio delle attività con Gestore di sistema di ONTAP o l'interfaccia CLI.

### A proposito di questa attività

Se si utilizza RBAC con l'API REST di ONTAP o Gestione sistema, sarà necessario creare ruoli personalizzati per gestire l'accesso al monitoraggio delle attività. Vedere [Controllo degli accessi in base al ruolo](#) per questo processo.

## System Manager

### Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi). Selezionare il volume desiderato. Dal menu dei singoli volumi, selezionare file System (file system), quindi selezionare la scheda Activity (attività).
2. Assicurarsi che l'opzione **Activity Tracking** sia attivata per visualizzare i singoli report su directory, file, client e utenti principali.
3. Per analizzare i dati in modo più approfondito senza aggiornamenti, selezionare **Pause Refresh** (Pausa aggiornamento\*). È possibile scaricare i dati per ottenere anche un record CSV del report.

### CLI

#### Fasi

1. Attiva monitoraggio attività:

```
volume activity-tracking on -vserver svm_name -volume volume_name
```

2. Controllare se lo stato di monitoraggio attività di un volume è attivato o disattivato con il comando:

```
volume activity-tracking show -vserver svm_name -volume volume_name -state
```

3. Una volta attivata, utilizzare Gestione di sistema ONTAP o l'API REST ONTAP per visualizzare i dati di monitoraggio delle attività.

## Attiva monitoraggio attività per più volumi

Puoi attivare il monitoraggio delle attività per più volumi con System Manager o la CLI.

### A proposito di questa attività

Se si utilizza RBAC con l'API REST di ONTAP o Gestione sistema, sarà necessario creare ruoli personalizzati per gestire l'accesso al monitoraggio delle attività. Vedere [Controllo degli accessi in base al ruolo](#) per questo processo.

## System Manager

### Abilitare per volumi specifici

1. Selezionare **Storage > Volumes** (Storage > volumi). Selezionare il volume desiderato. Dal menu dei singoli volumi, selezionare file System (file system), quindi selezionare la scheda Activity (attività).
2. Selezionare i volumi su cui si desidera attivare il monitoraggio attività. Nella parte superiore dell'elenco dei volumi, selezionare il pulsante **altre opzioni**. Selezionare **Enable Activity Tracking** (attiva monitoraggio attività).
3. Per visualizzare Activity Tracking a livello di SVM, selezionare la SVM specifica che si desidera visualizzare da **Storage > Volumes**. Accedere alla scheda file System (file system), quindi Activity (attività) per visualizzare i dati dei volumi per i quali è stata attivata l'opzione Activity Tracking (tracciamento attività).

### Abilitare per tutti i volumi

1. Selezionare **Storage > Volumes** (Storage > volumi). Selezionare una SVM dal menu.
2. Accedere alla scheda **file System** e scegliere la scheda **More** per attivare il monitoraggio delle attività su tutti i volumi nella SVM.

## CLI

A partire da ONTAP 9.13.1, è possibile attivare il monitoraggio delle attività per più volumi utilizzando l'interfaccia utente di ONTAP.

### Fasi

1. Attiva monitoraggio attività:

```
volume activity-tracking on -vserver svm_name -volume [*|!volume_names]
```

Utilizzare \* Per attivare il monitoraggio delle attività per tutti i volumi sulla VM di storage specificata.

Utilizzare ! Seguito dai nomi dei volumi per abilitare il monitoraggio delle attività per tutti i volumi su SVM, ad eccezione dei volumi denominati.

2. Confermare che l'operazione è riuscita:

```
volume show -fields activity-tracking-state
```

3. Una volta attivata, utilizzare Gestione di sistema ONTAP o l'API REST ONTAP per visualizzare i dati di monitoraggio delle attività.

## Abilita l'analisi dell'utilizzo

A partire da ONTAP 9.12.1, è possibile abilitare l'analisi dell'utilizzo per vedere quali directory all'interno di un volume utilizzano più spazio. È possibile visualizzare il numero totale di directory in un volume o il numero totale di file in un volume. Il reporting è limitato alle 25 directory che utilizzano la maggior parte dello spazio.

Gli analytics delle directory di grandi dimensioni vengono aggiornati ogni 15 minuti. È possibile monitorare l'aggiornamento più recente selezionando l'indicatore data e ora ultimo aggiornamento nella parte superiore della pagina. È inoltre possibile fare clic sul pulsante Download per scaricare i dati in una cartella di lavoro Excel. L'operazione di download viene eseguita in background e presenta le informazioni più recenti per il

volume selezionato. Se la scansione si ripresenta senza alcun risultato, assicurarsi che il volume sia online. Eventi come SnapRestore causeranno la ricostruzione dell'elenco di directory di grandi dimensioni da parte di analisi del file system.

#### Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi). Selezionare il volume desiderato.
2. Dal menu dei singoli volumi, selezionare **file System**. Quindi selezionare la scheda **Usage** (utilizzo).
3. Attivare l'opzione **Analytics** per abilitare l'analisi dell'utilizzo.
4. System Manager visualizza un grafico a barre che identifica le directory con le dimensioni maggiori in ordine decrescente.



ONTAP potrebbe visualizzare dati parziali o non visualizzare alcun dato durante la raccolta dell'elenco delle directory principali. L'avanzamento della scansione può essere nella scheda **Usage** (utilizzo) visualizzata durante la scansione.

Per ottenere ulteriori informazioni su una directory specifica, è possibile [visualizzare l'attività su un file system](#).

### Intraprendere azioni correttive basate sugli analytics

A partire da ONTAP 9.9.1, puoi intraprendere azioni correttive in base ai dati correnti e ai risultati desiderati direttamente dalle visualizzazioni di analisi del file system.

#### Eliminare directory e file

Nella visualizzazione Esplora risorse, è possibile selezionare le directory o i singoli file da eliminare. Le directory vengono eliminate con la funzionalità di eliminazione rapida delle directory a bassa latenza. (L'eliminazione rapida delle directory è disponibile anche a partire da ONTAP 9.9.1 senza l'opzione di analisi attivata).

#### Fasi

1. Fare clic su **Storage > Volumes**, quindi su **Explorer**.

Quando si passa il mouse su un file o una cartella, viene visualizzata l'opzione da eliminare. È possibile eliminare un solo oggetto alla volta.



Quando le directory e i file vengono cancellati, i nuovi valori di capacità dello storage non vengono visualizzati immediatamente.

### Assegna il costo dei supporti nei Tier di storage per confrontare i costi delle posizioni di storage dei dati inattive

Il costo dei supporti è un valore assegnato in base alla valutazione dei costi di storage, rappresentato come valuta per GB. Una volta impostato, System Manager utilizza il costo dei supporti assegnato per proiettare i risparmi stimati quando si spostano i volumi.

Il costo dei supporti impostato non è persistente; può essere impostato solo per una singola sessione del browser.

#### Fasi

1. Fare clic su **Storage > Tier**, quindi fare clic su **Set Media Cost** (Imposta costo supporti) nei riquadri del

Tier locale (aggregato) desiderato.

Assicurarsi di selezionare i livelli attivi e inattivi per attivare il confronto.

2. Inserire un tipo di valuta e un importo.


Quando si inserisce o si modifica il costo del supporto, la modifica viene apportata a tutti i tipi di supporto.

### **Spostamento dei volumi per ridurre i costi di storage**

In base ai display analitici e al confronto dei costi multimediali, puoi spostare i volumi in uno storage meno costoso nei Tier locali.

È possibile confrontare e spostare un solo volume alla volta.

#### **Fasi**

1. Dopo aver attivato la visualizzazione dei costi dei supporti, fare clic su **Storage > Tier**, quindi su **Volumes**.
2. Per confrontare le opzioni di destinazione di un volume, fare clic su  Per il volume, fare clic su **Move** (Sposta).
3. Nella schermata **Select Destination Local Tier** (Seleziona livello locale di destinazione), selezionare i Tier di destinazione per visualizzare la differenza di costo stimata.
4. Dopo aver confrontato le opzioni, selezionare il livello desiderato e fare clic su **Move** (Sposta).

### **Controllo degli accessi in base al ruolo con file System Analytics**

A partire da ONTAP 9.12.1, ONTAP include un ruolo predefinito RBAC (role-based access control) chiamato `admin-no-fsa`. Il `admin-no-fsa` il ruolo concede privilegi di livello amministratore, ma impedisce all'utente di eseguire operazioni correlate a `files Endpoint` (ad es. Analisi del file system) nell'interfaccia CLI di ONTAP, nell'API REST e in Gestore di sistema.

Per ulteriori informazioni su `admin-no-fsa` ruolo, fare riferimento a [Ruoli predefiniti per gli amministratori del cluster](#).

Se si utilizza una versione di ONTAP rilasciata prima di ONTAP 9.12.1, sarà necessario creare un ruolo dedicato per controllare l'accesso all'analisi del file system. Nelle versioni di ONTAP precedenti a ONTAP 9.12.1, è necessario configurare le autorizzazioni RBAC tramite l'interfaccia CLI di ONTAP o l'API REST di ONTAP.

## System Manager

A partire da ONTAP 9.12.1, è possibile configurare le autorizzazioni RBAC per l'analisi del file system utilizzando Gestione sistema.

### Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni). In **Security**, selezionare **Users and Roles** e scegliere ➔.
2. In **ruoli**, selezionare **+ Add**.
3. Fornire un nome per il ruolo. Nella sezione attributi ruolo, configurare l'accesso o le restrizioni per il ruolo utente fornendo l'appropriato "Endpoint API". Consultare la tabella seguente per i percorsi primari e secondari per configurare l'accesso o le restrizioni di file System Analytics.

| Restrizione                                    | Percorso primario    | Percorso secondario                                                                                                                                                                         |
|------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitoraggio delle attività sui volumi         | /api/storage/volumes | <ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul> |
| Monitoraggio delle attività su SVM             | /api/svm/svms        | <ul style="list-style-type: none"><li>• /:uuid/top-metrics/directories</li><li>• /:uuid/top-metrics/files</li><li>• /:uuid/top-metrics/clients</li><li>• /:uuid/top-metrics/users</li></ul> |
| Tutte le operazioni di analisi del file system | /api/storage/volumes | /:uuid/files                                                                                                                                                                                |

È possibile utilizzare /\*/ Invece di un UUID per impostare la policy per tutti i volumi o le SVM all'endpoint.

Scegliere i privilegi di accesso per ciascun endpoint.

4. Selezionare **Salva**.
5. Per assegnare il ruolo a uno o più utenti, vedere [Controllare l'accesso dell'amministratore](#).

### CLI

Se si utilizza una versione di ONTAP rilasciata prima di ONTAP 9.12.1, utilizzare l'interfaccia utente di ONTAP per creare un ruolo personalizzato.

## Fasi

1. Creare un ruolo predefinito per avere accesso a tutte le funzionalità.

Questa operazione deve essere eseguita prima di creare un ruolo restrittivo per garantire che il ruolo sia limitato solo al monitoraggio attività:

```
security login role create -cmddirname DEFAULT -access all -role storageAdmin
```

2. Creare il ruolo restrittivo:

```
security login role create -cmddirname "volume file show-disk-usage" -access none -role storageAdmin
```

3. Autorizzare i ruoli ad accedere ai servizi Web di SVM:

- `rest` Per chiamate API REST
- `security` per la protezione tramite password
- `sysmgr` Per l'accesso a System Manager

```
vserver services web access create -vserver svm-name -name _ -name rest -role storageAdmin
```

```
vserver services web access create -vserver svm-name -name security -role storageAdmin
```

```
vserver services web access create -vserver svm-name -name sysmgr -role storageAdmin
```

4. Creare un utente.

È necessario eseguire un comando di creazione distinto per ciascuna applicazione che si desidera applicare all'utente. La chiamata a `create` più volte sullo stesso utente applica semplicemente tutte le applicazioni a quell'utente e non crea un nuovo utente ogni volta. Il `http` Il parametro per il tipo di applicazione si applica all'API REST di ONTAP e al Gestore di sistema.

```
security login create -user-or-group-name storageUser -authentication -method password -application http -role storageAdmin
```

5. Con le nuove credenziali utente, è ora possibile accedere a Gestore di sistema o utilizzare l'API REST di ONTAP per accedere ai dati di analisi dei file system.

## Ulteriori informazioni

- [Ruoli predefiniti per gli amministratori del cluster](#)
- [Controlla l'accesso dell'amministratore con System Manager](#)
- ["Scopri di più sui ruoli RBAC e sull'API REST ONTAP"](#)

## Considerazioni per l'analisi del file system

Devi essere consapevole di determinati limiti di utilizzo e potenziali impatti sulle

performance associati all'implementazione di file System Analytics.

## Relazioni protette con SVM

Se sono state attivate le analisi del file system su volumi con SVM contenente una relazione di protezione, i dati di analisi non vengono replicati nella SVM di destinazione. Se la SVM di origine deve essere risincronizzata in un'operazione di recovery, è necessario riabilitare manualmente le analisi sui volumi desiderati dopo il recovery.

## Considerazioni sulle performance

In alcuni casi, l'abilitazione di file System Analytics potrebbe avere un impatto negativo sulle performance durante la raccolta iniziale dei metadati. Ciò si verifica in genere nei sistemi che sono al massimo utilizzo. Per evitare di abilitare l'analisi su tali sistemi, è possibile utilizzare gli strumenti di monitoraggio delle performance di Gestore di sistema di ONTAP.

Se si verifica un notevole aumento della latenza, consultare l'articolo della Knowledge base ["Latenza elevata o fluttuante dopo l'attivazione dell'analisi del file system NetApp ONTAP"](#).

## Considerazioni sulla scansione

Quando abiliti le analisi della capacità, ONTAP esegue una scansione di inizializzazione per l'analisi della capacità. La scansione accede ai metadati per tutti i file nei volumi per i quali è abilitata l'analisi della capacità. Durante la scansione non viene letto alcun dato di file. A partire da ONTAP 9.14.1, è possibile tenere traccia dell'avanzamento della scansione con l'API REST, nella scheda **Esplora risorse** di Gestione sistema o con `volume analytics show` Comando CLI. Se è presente un evento di rallentamento, ONTAP fornisce una notifica.

Al termine della scansione, file System Analytics viene continuamente aggiornato in tempo reale in base alle modifiche del file system senza dover eseguire nuovamente la scansione.

Il tempo richiesto per la scansione è proporzionale al numero di directory e file sul volume. Poiché la scansione raccoglie i metadati, le dimensioni del file non influiscono sul tempo di scansione.

Per ulteriori informazioni sulla scansione di inizializzazione, vedere ["TR-4867: Linee guida sulle Best practice per l'analisi del file system"](#).

## Best practice

Si consiglia di avviare la scansione su volumi che non condividono aggregati. È possibile visualizzare gli aggregati che attualmente ospitano i volumi utilizzando il comando:

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

Durante l'esecuzione della scansione, i volumi continuano a servire il traffico client. Si consiglia di avviare la scansione durante i periodi in cui si prevede una riduzione del traffico client.

Se il traffico del client aumenta, consuma le risorse di sistema e la scansione richiede più tempo.

A partire da ONTAP 9.12.1, è possibile sospendere la raccolta dei dati in Gestore di sistema e con l'interfaccia utente di ONTAP.

- Se si utilizza l'interfaccia utente di ONTAP:
  - È possibile sospendere la raccolta dati con il comando: `volume analytics initialization`



```
pause -vserver svm_name -volume volume_name
```

- Una volta rallentato il traffico del client, è possibile riprendere la raccolta dei dati con il comando:  
`volume analytics initialization resume -vserver svm_name -volume volume_name`
- Se si utilizza System Manager, nella vista **Explorer** del menu del volume, utilizzare i pulsanti **Pause Data Collection** e **Resume Data Collection** per gestire la scansione.

## Configurazione EMS

### Panoramica della configurazione EMS

È possibile configurare ONTAP 9 in modo che invii notifiche di eventi EMS (sistema di gestione degli eventi) importanti direttamente a un indirizzo e-mail, a un server syslog, a un traphost SNMP (Simple Management Network Protocol) o a un'applicazione webhook, in modo da ricevere una notifica immediata dei problemi di sistema che richiedono un'attenzione immediata.

Poiché le notifiche di eventi importanti non sono attivate per impostazione predefinita, è necessario configurare EMS in modo che invii le notifiche a un indirizzo e-mail, a un server syslog, a un host trapSNMP o a un'applicazione webhook.

Esaminare le versioni specifiche della release di ["Riferimento EMS ONTAP 9"](#).

Se la mappatura degli eventi EMS utilizza set di comandi ONTAP deprecati (come destinazione dell'evento, percorso dell'evento), si consiglia di aggiornare la mappatura. ["Scopri come aggiornare la mappatura EMS da comandi ONTAP non aggiornati"](#).

### Configurare le notifiche e i filtri degli eventi EMS con System Manager

È possibile utilizzare System Manager per configurare il modo in cui il sistema di gestione degli eventi (EMS) invia le notifiche degli eventi, in modo da poter essere avvisati dei problemi di sistema che richiedono una rapida attenzione.

| Versione di ONTAP                  | Con System Manager, è possibile...                                                                                                                                   |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ONTAP 9.12.1 e versioni successive | Specificare il protocollo TLS (Transport Layer Security) quando si inviano eventi ai server syslog remoti.                                                           |
| ONTAP 9.10.1 e versioni successive | Configurare indirizzi e-mail, server syslog, applicazioni webhook e host SNMP.                                                                                       |
| ONTAP da 9.7 a 9.10.0              | Configurare solo i traphost SNMP. È possibile configurare un'altra destinazione EMS con la CLI ONTAP. Vedere <a href="#">"Panoramica della configurazione EMS"</a> . |

È possibile eseguire le seguenti procedure:

- [\[add-ems-destination\]](#)
- [\[create-ems-filter\]](#)

- [\[edit-ems-destination\]](#)
- [\[edit-ems-filter\]](#)
- [\[delete-ems-destination\]](#)
- [\[delete-ems-filter\]](#)

#### Informazioni correlate



- ["Riferimento EMS ONTAP"](#)
- ["Utilizzo della CLI per configurare i traphost SNMP in modo che ricevano le notifiche degli eventi"](#)

### Aggiungere una destinazione di notifica degli eventi EMS

È possibile utilizzare System Manager per specificare dove si desidera inviare i messaggi EMS.

A partire da ONTAP 9.12.1, gli eventi EMS possono essere inviati a una porta designata su un server syslog remoto tramite il protocollo TLS (Transport Layer Security). Per ulteriori informazioni, vedere `event notification destination create` pagina man.

#### Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su , Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **Destinazioni eventi**.
4. Fare clic su  **Add**.
5. Specificare un nome, un tipo di destinazione EMS e i filtri.



Se necessario, è possibile aggiungere un nuovo filtro. Fare clic su **Aggiungi un nuovo filtro eventi**.

6. A seconda del tipo di destinazione EMS selezionato, specificare quanto segue:



| Per configurare...                     | Specificare o selezionare...                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP traphost                          | <ul style="list-style-type: none"> <li>• Nome TrapHost</li> </ul>                                                                                                                                                                                                                                                                                                                                                                          |
| E-mail<br>(A partire da 9.10.1)        | <ul style="list-style-type: none"> <li>• Indirizzo e-mail di destinazione</li> <li>• Server di posta</li> <li>• Da indirizzo e-mail</li> </ul>                                                                                                                                                                                                                                                                                             |
| Server syslog<br>(A partire da 9.10.1) | <ul style="list-style-type: none"> <li>• Nome host o indirizzo IP del server</li> <li>• Porta syslog (a partire da 9.12.1)</li> <li>• Trasporto syslog (a partire da 9.12.1)</li> </ul> <p>Selezionando <b>TCP Encrypted</b> si attiva il protocollo TLS (Transport Layer Security). Se non viene immesso alcun valore per <b>porta Syslog</b>, viene utilizzato un valore predefinito in base alla selezione <b>trasporto Syslog</b>.</p> |


|                                      |                                                                                                                                                                     |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Webhook<br><br>(A partire da 9.10.1) | <ul style="list-style-type: none"> <li>• URL Webhook</li> <li>• Autenticazione client (selezionare questa opzione per specificare un certificato client)</li> </ul> |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Creare un nuovo filtro per la notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per definire nuovi filtri personalizzati che specificano le regole per la gestione delle notifiche EMS.

### Fasi



1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su , Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **filtri eventi**.
4. Fare clic su  **Add**.
5. Specificare un nome e scegliere se si desidera copiare le regole da un filtro eventi esistente o aggiungere nuove regole.
6. A seconda della scelta, attenersi alla seguente procedura:

| Se si sceglie....                                     | Quindi, eseguire questi passaggi...                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Copia delle regole dal filtro eventi esistente</b> | <ol style="list-style-type: none"> <li>1. Selezionare un filtro eventi esistente.</li> <li>2. Modificare le regole esistenti.</li> <li>3. Aggiungere altre regole, se necessario, facendo clic su  <b>Add</b>.</li> </ol> |
| <b>Aggiungi nuove regole</b>                          | Specificare il tipo, il modello di nome, le severità e il tipo di trap SNMP per ogni nuova regola.                                                                                                                                                                                                           |

## Modificare una destinazione di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per modificare le informazioni di destinazione della notifica degli eventi.

### Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su , Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **Destinazioni eventi**.
4. Accanto al nome della destinazione dell'evento, fare clic su , Quindi fare clic su **Edit** (Modifica).
5. Modificare le informazioni sulla destinazione dell'evento, quindi fare clic su **Salva**.



## Modificare un filtro di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per modificare i filtri personalizzati e modificare la modalità di gestione delle notifiche degli eventi.



Non è possibile modificare i filtri definiti dal sistema.

#### Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su , Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **filtri eventi**.
4. Accanto al nome del filtro eventi, fare clic su , Quindi fare clic su **Edit** (Modifica).
5. Modificare le informazioni del filtro eventi, quindi fare clic su **Save** (Salva).



#### Eliminare una destinazione di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per eliminare una destinazione di notifica degli eventi EMS.



Non è possibile eliminare le destinazioni SNMP.

#### Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su , Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **Destinazioni eventi**.
4. Accanto al nome della destinazione dell'evento, fare clic su , Quindi fare clic su **Delete** (Elimina).



#### Eliminare un filtro di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per eliminare i filtri personalizzati.



Non è possibile eliminare i filtri definiti dal sistema.

#### Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su , Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **filtri eventi**.
4. Accanto al nome del filtro eventi, fare clic su , Quindi fare clic su **Delete** (Elimina).

## Configurare le notifiche degli eventi EMS con la CLI

#### Workflow di configurazione EMS

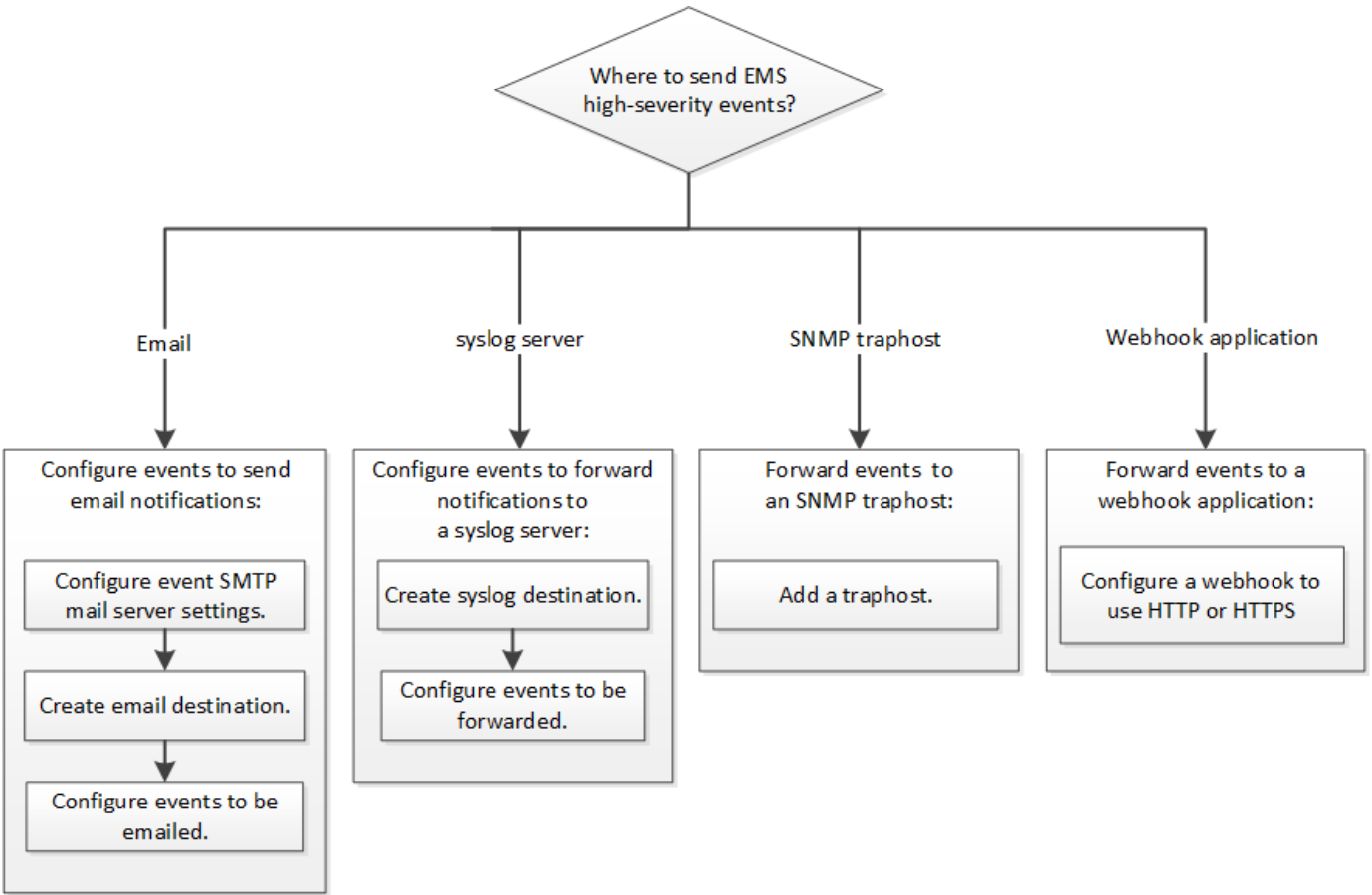
È necessario configurare le notifiche di eventi EMS importanti da inviare come email, inoltrate a un server syslog, inoltrate a un host traphost SNMP o inoltrate a un'applicazione webhook. In questo modo, è possibile evitare interruzioni del sistema adottando azioni correttive in modo tempestivo.

**A proposito di questa attività**

Se l'ambiente in uso contiene già un server syslog per l'aggregazione degli eventi registrati da altri sistemi, come server e applicazioni, è più semplice utilizzare tale server syslog anche per le notifiche di eventi importanti provenienti dai sistemi storage.

Se l'ambiente non contiene già un server syslog, è più semplice utilizzare l'e-mail per le notifiche di eventi importanti.

Se si inoltrano già notifiche di eventi a un host trapSNMP, potrebbe essere necessario monitorare tale host per rilevare eventi importanti.



**Scelte**

- Impostare EMS per l'invio delle notifiche degli eventi.

| Se vuoi...                                                                  | Fare riferimento a...                                                                           |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| EMS per inviare notifiche di eventi importanti a un indirizzo e-mail        | <a href="#">Configurare eventi EMS importanti per l'invio di notifiche e-mail</a>               |
| EMS per inoltrare notifiche di eventi importanti a un server syslog         | <a href="#">Configurare eventi EMS importanti per inoltrare le notifiche a un server syslog</a> |
| Se si desidera che EMS inoltri le notifiche degli eventi a un host trapSNMP | <a href="#">Configurare i traphost SNMP per ricevere le notifiche degli eventi</a>              |

Se si desidera che EMS inoltri le notifiche degli eventi a un'applicazione webhook

[Configurare eventi EMS importanti per inoltrare le notifiche a un'applicazione webhook](#)

## Configurare eventi EMS importanti per l'invio di notifiche e-mail

Per ricevere notifiche via email degli eventi più importanti, è necessario configurare il servizio EMS in modo che invii messaggi di posta elettronica per gli eventi che segnalano attività importanti.

### Di cosa hai bisogno

Il DNS deve essere configurato sul cluster per risolvere gli indirizzi e-mail.

### A proposito di questa attività

È possibile eseguire questa attività ogni volta che il cluster è in esecuzione immettendo i comandi nella riga di comando ONTAP.

### Fasi

1. Configurare le impostazioni del server di posta SMTP dell'evento:

```
event config modify -mail-server mailhost.your_domain -mail-from  
cluster_admin@your_domain
```

2. Creare una destinazione email per le notifiche degli eventi:

```
event notification destination create -name storage-admins -email  
your_email@your_domain
```

3. Configurare gli eventi importanti per l'invio di notifiche e-mail:

```
event notification create -filter-name important-events -destinations storage-  
admins
```

## Configurazione di eventi EMS importanti per inoltrare le notifiche a un server syslog

Per registrare le notifiche degli eventi più gravi su un server syslog, è necessario configurare EMS in modo che inoltri le notifiche per gli eventi che segnalano attività importanti.

### Di cosa hai bisogno

Il DNS deve essere configurato sul cluster per risolvere il nome del server syslog.

### A proposito di questa attività

Se l'ambiente non contiene già un server syslog per le notifiche degli eventi, è necessario crearne uno. Se l'ambiente in uso contiene già un server syslog per la registrazione degli eventi da altri sistemi, è possibile utilizzare tale server per le notifiche di eventi importanti.

È possibile eseguire questa attività ogni volta che il cluster è in esecuzione immettendo i comandi nell'interfaccia utente di ONTAP.

A partire da ONTAP 9.12.1, gli eventi EMS possono essere inviati a una porta designata su un server syslog

remoto tramite il protocollo TLS (Transport Layer Security). Sono disponibili due nuovi parametri:

### **tcp-encrypted**

Quando `tcp-encrypted` è specificato per `syslog-transport`, ONTAP verifica l'identità dell'host di destinazione convalidandone il certificato. Il valore predefinito è `udp-unencrypted`.

### **syslog-port**

Il valore predefinito `syslog-port` il parametro dipende dall'impostazione di `syslog-transport` parametro. Se `syslog-transport` è impostato su `tcp-encrypted`, `syslog-port` ha il valore predefinito 6514.

Per ulteriori informazioni, vedere `event notification destination create` pagina man.

### **Fasi**

1. Creare una destinazione del server syslog per eventi importanti:

```
event notification destination create -name syslog-ems -syslog syslog-server-address -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}
```

A partire da ONTAP 9.12.1, è possibile specificare i seguenti valori per `syslog-transport`:

- ° `udp-unencrypted` - User Datagram Protocol senza sicurezza
- ° `tcp-unencrypted` - Transmission Control Protocol senza sicurezza
- ° `tcp-encrypted` - Transmission Control Protocol con Transport Layer Security (TLS)

Il protocollo predefinito è `udp-unencrypted`.

2. Configurare gli eventi importanti per inoltrare le notifiche al server syslog:

```
event notification create -filter-name important-events -destinations syslog-ems
```

## **Configurare i traphost SNMP per ricevere le notifiche degli eventi**

Per ricevere le notifiche degli eventi su un host trapSNMP, è necessario configurare un host traphost.

### **Di cosa hai bisogno**

- I trap SNMP e SNMP devono essere attivati sul cluster.



I trap SNMP e SNMP sono attivati per impostazione predefinita.

- Il DNS deve essere configurato sul cluster per risolvere i nomi degli host trapezoidali.

### **A proposito di questa attività**

Se non si dispone già di un host trapSNMP configurato per ricevere notifiche di eventi (trap SNMP), è necessario aggiungerne uno.

È possibile eseguire questa attività ogni volta che il cluster è in esecuzione immettendo i comandi nella riga di comando ONTAP.

## Fase

1. Se l'ambiente non dispone già di un host trapSNMP configurato per ricevere le notifiche degli eventi, aggiungerne uno:

```
system snmp traphost add -peer-address snmp_traphost_name
```

Tutte le notifiche degli eventi supportate da SNMP per impostazione predefinita vengono inoltrate all'host principale SNMP.

## Configurare eventi EMS importanti per inoltrare le notifiche a un'applicazione webhook

È possibile configurare ONTAP per inoltrare notifiche di eventi importanti a un'applicazione webhook. I passaggi necessari per la configurazione dipendono dal livello di sicurezza scelto.

### Prepararsi a configurare l'inoltro degli eventi EMS

Prima di configurare ONTAP per inoltrare le notifiche degli eventi a un'applicazione webhook, è necessario prendere in considerazione diversi concetti e requisiti.

### Applicazione Webhook

È necessaria un'applicazione webhook in grado di ricevere le notifiche degli eventi ONTAP. Un webhook è una routine di callback definita dall'utente che estende le funzionalità dell'applicazione o del server remoto in cui viene eseguito. I webhook vengono chiamati o attivati dal client (in questo caso ONTAP) inviando una richiesta HTTP all'URL di destinazione. In particolare, ONTAP invia una richiesta HTTP POST al server che ospita l'applicazione webhook insieme ai dettagli della notifica degli eventi formattati in XML.

### Opzioni di sicurezza

Sono disponibili diverse opzioni di sicurezza a seconda di come viene utilizzato il protocollo TLS (Transport Layer Security). L'opzione scelta determina la configurazione ONTAP richiesta.



TLS è un protocollo crittografico ampiamente utilizzato su Internet. Fornisce privacy, integrità dei dati e autenticazione utilizzando uno o più certificati a chiave pubblica. I certificati vengono emessi da autorità di certificazione attendibili.

### HTTP

È possibile utilizzare HTTP per trasportare le notifiche degli eventi. Con questa configurazione, la connessione non è sicura. Le identità del client ONTAP e dell'applicazione webhook non vengono verificate. Inoltre, il traffico di rete non viene crittografato o protetto. Vedere ["Configurare una destinazione webhook per l'utilizzo di HTTP"](#) per informazioni dettagliate sulla configurazione.

### HTTPS

Per una maggiore sicurezza, è possibile installare un certificato sul server che ospita la routine webhook. Il protocollo HTTPS viene utilizzato da ONTAP per verificare l'identità del server applicazioni webhook e da entrambe le parti per garantire la privacy e l'integrità del traffico di rete. Vedere ["Configurare una destinazione webhook per l'utilizzo di HTTPS"](#) per informazioni dettagliate sulla configurazione.

### HTTPS con autenticazione reciproca

È possibile migliorare ulteriormente la protezione HTTPS installando un certificato client sul sistema ONTAP che invia le richieste del manuale. Oltre a verificare l'identità del server dell'applicazione webhook e



a proteggere il traffico di rete, ONTAP verifica l'identità del client ONTAP. Questa autenticazione peer bidirezionale è nota come *Mutual TLS*. Vedere ["Configurare una destinazione webhook per l'utilizzo di HTTPS con autenticazione reciproca"](#) per informazioni dettagliate sulla configurazione.

## Informazioni correlate

- ["Il protocollo TLS \(Transport Layer Security\) versione 1.3"](#)

## Configurare una destinazione webhook per l'utilizzo di HTTP

È possibile configurare ONTAP in modo che inoltri le notifiche degli eventi a un'applicazione webhook utilizzando HTTP. Si tratta dell'opzione meno sicura, ma la più semplice da configurare.

### Fasi

1. Creare una nuova destinazione `restapi-ems` per ricevere gli eventi:

```
event notification destination create -name restapi-ems -rest-api-url  
http://<webhook-application>
```

Nel comando precedente, è necessario utilizzare lo schema **HTTP** per la destinazione.

2. Creare una notifica che colleghi `important-events` filtrare con `restapi-ems` destinazione:

```
event notification create -filter-name important-events -destinations restapi-  
ems
```

## Configurare una destinazione webhook per l'utilizzo di HTTPS

È possibile configurare ONTAP in modo che inoltri le notifiche degli eventi a un'applicazione webhook utilizzando HTTPS. ONTAP utilizza il certificato del server per confermare l'identità dell'applicazione webhook e proteggere il traffico di rete.

### Prima di iniziare

- Generare una chiave privata e un certificato per il server applicazioni webhook
- Disporre del certificato root per l'installazione in ONTAP

### Fasi

1. Installare la chiave privata del server e i certificati appropriati sul server che ospita l'applicazione webhook. Le specifiche fasi di configurazione dipendono dal server.
2. Installare il certificato root del server in ONTAP:

```
security certificate install -type server-ca
```

Il comando chiederà il certificato.

3. Creare il `restapi-ems` destinazione per ricevere gli eventi:

```
event notification destination create -name restapi-ems -rest-api-url  
https://<webhook-application>
```

Nel comando precedente, è necessario utilizzare lo schema **HTTPS** per la destinazione.

4. Creare la notifica che collega `important-events` filtra con il nuovo `restapi-ems` destinazione:

```
event notification create -filter-name important-events -destinations restapi-ems
```

### Configurare una destinazione webhook per l'utilizzo di HTTPS con autenticazione reciproca

È possibile configurare ONTAP per inoltrare le notifiche degli eventi a un'applicazione webhook utilizzando HTTPS con autenticazione reciproca. Con questa configurazione sono disponibili due certificati. ONTAP utilizza il certificato del server per confermare l'identità dell'applicazione webhook e proteggere il traffico di rete. Inoltre, l'applicazione che ospita il webhook utilizza il certificato client per confermare l'identità del client ONTAP.

#### Prima di iniziare

Prima di configurare ONTAP, è necessario effettuare le seguenti operazioni:

- Generare una chiave privata e un certificato per il server applicazioni webhook
- Disporre del certificato root per l'installazione in ONTAP
- Generare una chiave privata e un certificato per il client ONTAP

#### Fasi

1. Eseguire le prime due fasi dell'attività "[Configurare una destinazione webhook per l'utilizzo di HTTPS](#)" Per installare il certificato del server in modo che ONTAP possa verificare l'identità del server.
2. Installare i certificati root e intermedi appropriati nell'applicazione webhook per convalidare il certificato client.
3. Installare il certificato client in ONTAP:

```
security certificate install -type client
```

Il comando richiede la chiave privata e il certificato.

4. Creare il `restapi-ems` destinazione per ricevere gli eventi:

```
event notification destination create -name restapi-ems -rest-api-url  
https://<webhook-application> -certificate-authority <issuer of the client  
certificate> -certificate-serial <serial of the client certificate>
```

Nel comando precedente, è necessario utilizzare lo schema **HTTPS** per la destinazione.

5. Creare la notifica che collega `important-events` filtra con il nuovo `restapi-ems` destinazione:

```
event notification create -filter-name important-events -destinations restapi-ems
```

### Aggiornare la mappatura degli eventi EMS obsoleta

#### Modelli di mappatura degli eventi EMS

Prima di ONTAP 9.0, gli eventi EMS potevano essere mappati solo alle destinazioni degli eventi in base alla corrispondenza del modello di nome dell'evento. Il comando ONTAP viene impostato (`event destination, event route`) Che utilizzano questo modello

continuano a essere disponibili nelle ultime versioni di ONTAP, ma sono state deprecate a partire da ONTAP 9.0.

A partire da ONTAP 9.0, la Best practice per il mapping della destinazione degli eventi EMS di ONTAP consiste nell'utilizzare il modello di filtro eventi più scalabile in cui la corrispondenza dei modelli viene eseguita su più campi, utilizzando l' `event filter`, `event notification`, e `event notification destination set` di comandi.

Se la mappatura EMS è configurata utilizzando i comandi non aggiornati, aggiornare la mappatura per utilizzare `event filter`, `event notification`, e `event notification destination set` di comandi.

Esistono due tipi di destinazioni degli eventi:

**1. Destinazioni generate dal sistema:** Esistono cinque destinazioni di eventi generate dal sistema (create per impostazione predefinita)

- ° `allevents`
- ° `asup`
- ° `criticals`
- ° `pager`
- ° `traphost`

Alcune destinazioni generate dal sistema sono destinate a scopi speciali. Ad esempio, la destinazione `asup` instrada gli eventi `callhome.*` al modulo AutoSupport in ONTAP per generare messaggi AutoSupport.

**2. Destinazioni create dall'utente:** Vengono create manualmente utilizzando `event destination create` comando.

```
cluster-1::event*> destination show
```

| Name   | Mail Dest. | SNMP Dest. | Syslog Dest. |
|--------|------------|------------|--------------|
| Params |            |            |              |

|           |       |       |       |
|-----------|-------|-------|-------|
| -----     | ----- | ----- | ----- |
| -----     |       |       |       |
| allevents | -     | -     | -     |
| false     |       |       |       |
| asup      | -     | -     | -     |
| false     |       |       |       |
| criticals | -     | -     | -     |
| false     |       |       |       |
| pager     | -     | -     | -     |
| false     |       |       |       |
| traphost  | -     | -     | -     |
| false     |       |       |       |

5 entries were displayed.

+

```
cluster-1::event*> destination create -name test -mail test@xyz.com
```

This command is deprecated. Use the "event filter", "event notification destination" and "event notification" commands, instead.

+

```
cluster-1::event*> destination show
```

+

Hide

| Name   | Mail Dest. | SNMP Dest. | Syslog Dest. |
|--------|------------|------------|--------------|
| Params |            |            |              |

|           |              |       |       |
|-----------|--------------|-------|-------|
| -----     | -----        | ----- | ----- |
| -----     |              |       |       |
| allevents | -            | -     | -     |
| false     |              |       |       |
| asup      | -            | -     | -     |
| false     |              |       |       |
| criticals | -            | -     | -     |
| false     |              |       |       |
| pager     | -            | -     | -     |
| false     |              |       |       |
| test      | test@xyz.com | -     | -     |
| false     |              |       |       |
| traphost  | -            | -     | -     |
| false     |              |       |       |

6 entries were displayed.

Nel modello obsoleto, gli eventi EMS vengono mappati singolarmente a una destinazione utilizzando event route add-destinations comando.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.
```

```
cluster-1::event*> route show -message-name raid.aggr.*
```

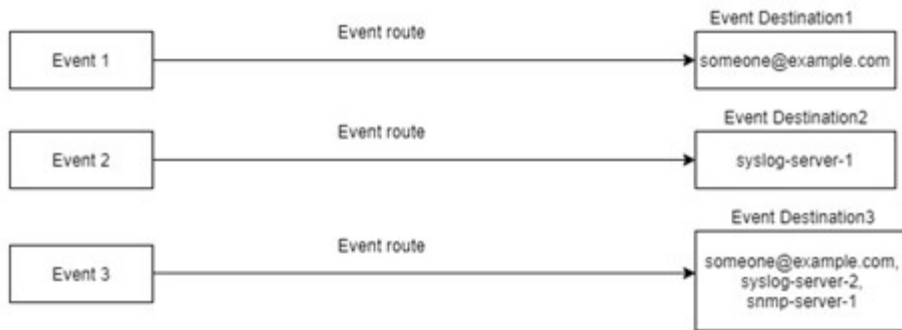
| Time                       | Severity      | Destinations | Freq | Threshd |
|----------------------------|---------------|--------------|------|---------|
| raid.aggr.autoGrow.abort   | NOTICE        | test         | 0    | 0       |
| raid.aggr.autoGrow.success | NOTICE        | test         | 0    | 0       |
| raid.aggr.lock.conflict    | INFORMATIONAL | test         | 0    | 0       |
| raid.aggr.log.CP.count     | DEBUG         | test         | 0    | 0       |

4 entries were displayed.

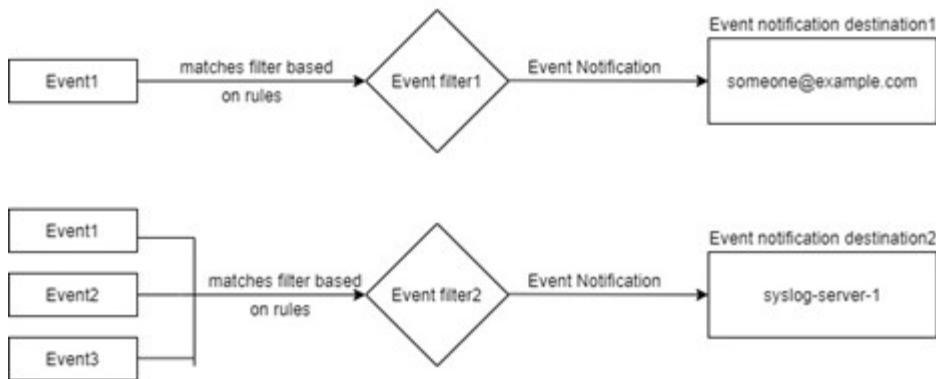
Il nuovo meccanismo di notifica degli eventi EMS, più scalabile, si basa sui filtri degli eventi e sulle destinazioni di notifica degli eventi. Fare riferimento al seguente articolo della Knowledge base per informazioni dettagliate sul nuovo meccanismo di notifica degli eventi:

- ["Panoramica del sistema di gestione degli eventi per ONTAP 9"](#)

Legacy routing based model



Event notification based model



## Aggiornare la mappatura degli eventi EMS dai comandi ONTAP non aggiornati

Se la mappatura degli eventi EMS è attualmente configurata utilizzando i set di comandi ONTAP deprecati (`event destination`, `event route`), seguire questa procedura per aggiornare la mappatura per utilizzare `event filter`, `event notification`, e `event notification destination` set di comandi.

### Fasi

1. Elencare tutte le destinazioni degli eventi nel sistema utilizzando `event destination show` comando.

```
cluster-1::event*> destination show
```

Hide

| Name | Mail Dest. | SNMP Dest. | Syslog Dest. |
|------|------------|------------|--------------|
|------|------------|------------|--------------|

Params

|           |              |   |   |
|-----------|--------------|---|---|
| allevents | -            | - | - |
| false     |              |   |   |
| asup      | -            | - | - |
| false     |              |   |   |
| criticals | -            | - | - |
| false     |              |   |   |
| pager     | -            | - | - |
| false     |              |   |   |
| test      | test@xyz.com | - | - |
| false     |              |   |   |
| traphost  | -            | - | - |
| false     |              |   |   |

6 entries were displayed.

2. Per ciascuna destinazione, elencare gli eventi associati utilizzando `event route show -destinations <destination name>` comando.

```
cluster-1::event*> route show -destinations test
```

| Time                       | Severity      | Destinations | Freq | Threshd |
|----------------------------|---------------|--------------|------|---------|
| raid.aggr.autoGrow.abort   | NOTICE        | test         | 0    | 0       |
| raid.aggr.autoGrow.success | NOTICE        | test         | 0    | 0       |
| raid.aggr.lock.conflict    | INFORMATIONAL | test         | 0    | 0       |
| raid.aggr.log.CP.count     | DEBUG         | test         | 0    | 0       |

4 entries were displayed.

3. Creare un corrispondente `event filter` che include tutti questi sottoinsiemi di eventi. Ad esempio, se si desidera includere solo il `raid.aggr.*` eventi, utilizzare un carattere jolly per message-name quando si crea il filtro. È inoltre possibile creare filtri per singoli eventi.



È possibile creare fino a 50 filtri per eventi.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule      Rule      Message Name      SNMP Trap Type
Severity
      Position Type
-----
test_events
      1      include  raid.aggr.*      *      *
      2      exclude  *      *      *
2 entries were displayed.
```

4. Creare un event notification destination per ciascuno di event destination Endpoint (ad esempio, SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name      Type      Destination
-----
dest1      email      test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost  snmp      - (from "system snmp traphost")
2 entries were displayed.
```

5. Creare una notifica degli eventi mappando il filtro degli eventi alla destinazione di notifica degli eventi.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID  Filter Name      Destinations
---
1   default-trap-events  snmp-traphost
2   asup_events          dest1
2 entries were displayed.
```

6. Ripetere i punti 1-5 per ciascuno event destination questo ha un event route mappatura.





Gli eventi instradati alle destinazioni SNMP devono essere mappati a. snmp-traphost destinazione della notifica degli eventi. La destinazione SNMP traphost utilizza l'host SNMP traphost configurato dal sistema.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
      scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>      Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

      Destination Name: snmp-traphost
      Type of Destination: snmp
      Destination: 10.234.166.135 (from "system snmp
traphost")
      Server CA Certificates Present?: -
      Client Certificate Issuing CA: -
      Client Certificate Serial Number: -
      Client Certificate Valid?: -
```

# Riferimento al comando ONTAP

Per ogni release principale di ONTAP, i comandi CLI comunemente disponibili (pagine di manuale di ONTAP o pagine man) sono raggruppati in un *riferimento di comando*. Questi riferimenti ai comandi spiegano come utilizzare i comandi CLI in ogni release di ONTAP. Le pagine man sono disponibili anche nella riga di comando di ONTAP con il `man` comando.

## Riferimenti ai comandi per le versioni supportate di ONTAP

- ["ONTAP 9.14.1"](#)
- ["ONTAP 9.13.1"](#)
- ["ONTAP 9.12.1"](#)
- ["ONTAP 9.11.1"](#)
- ["ONTAP 9.10.1"](#)
- ["ONTAP 9.9.1"](#)
- ["ONTAP 9.8"](#)
- ["ONTAP 9.7"](#)
- ["ONTAP 9.6"](#)
- ["ONTAP 9.5"](#)
- ["ONTAP 9.3"](#)

## Riferimenti ai comandi per le versioni a supporto limitato di ONTAP (solo PDF)

- ["ONTAP 9.4"](#)
- ["ONTAP 9.2"](#)
- ["ONTAP 9.1"](#)
- ["ONTAP 9.0"](#)

## Tool di confronto CLI

È possibile ottenere informazioni sulle modifiche apportate ai comandi dell'interfaccia della riga di comando (CLI) tra le release di ONTAP utilizzando ["Tool di confronto CLI"](#) Sul sito di supporto NetApp.

### Ulteriori letture

- [Utilizzare l'interfaccia della riga di comando di ONTAP](#)
- [Metodi per navigare nelle directory dei comandi CLI](#)

# Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

## Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## Direttiva sulla privacy

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

### ONTAP

["Avviso per ONTAP 9.14.1"](#)

["Avviso per ONTAP 9.14.0"](#)

["Avviso per ONTAP 9.13.1"](#)

["Avviso per ONTAP 9.12.1"](#)

["Avviso per ONTAP 9.12.0"](#)

["Avviso per ONTAP 9.11.1"](#)

["Avviso per ONTAP 9.10.1"](#)

["Avviso per ONTAP 9.10.0"](#)

["Avviso per ONTAP 9.9.1"](#)

["Avviso per ONTAP 9.8"](#)

["Avviso per ONTAP 9.7"](#)

["Avviso per ONTAP 9.6"](#)

["Avviso per ONTAP 9.5"](#)

["Avviso per ONTAP 9.4"](#)

["Avviso per ONTAP 9.3"](#)

["Avviso per ONTAP 9.2"](#)

["Avviso per ONTAP 9.1"](#)

## **MEDIATORE ONTAP PER IP MCC**

"9.9.1 Avviso per ONTAP MEDIATOR per MCC IP"

"9.8 Avviso per ONTAP MEDIATOR per MCC IP"

"9.7 Avviso per ONTAP MEDIATOR per MCC IP"

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.