# Documentazione di ONTAP tools per VMware vSphere

ONTAP tools for VMware vSphere 105

NetApp
August 06, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap-tools-vmware-vsphere-105/index.html on August 06, 2026. Always check docs.netapp.com for the latest.

# Sommario


Documentazione di ONTAP tools per VMware vSphere . . . 1
Note di rilascio . . . 2
Note di rilascio per ONTAP tools . . . 2
Novità degli ONTAP tools per VMware vSphere 10.5 . . . 2
Piattaforme ONTAP e versioni del server vCenter supportate . . . 3
Confronto delle funzionalità di ONTAP tools for VMware vSphere 9 e 10 . . . 3
Concetti . . . 5
Scopri gli strumenti ONTAP . . . 5
Concetti e termini chiave negli ONTAP tools . . . 5
Controllo degli accessi in base al ruolo (RBAC) . . . 8
Scopri RBAC degli strumenti ONTAP . . . 8
RBAC con VMware vSphere . . . 10
RBAC con ONTAP . . . 16
Distribuisci ONTAP tools per VMware vSphere . . . 20
Guida rapida per ONTAP tools for VMware vSphere . . . 20
Flusso di lavoro di distribuzione ad alta disponibilità per ONTAP tools . . . 22
Requisiti e limiti di configurazione di ONTAP tools per VMware vSphere . . . 23
Requisiti di sistema . . . 23
Requisiti minimi di archiviazione e applicazione . . . 23
Requisiti delle porte . . . 24
Limiti di configurazione per distribuire ONTAP tools for VMware vSphere per vVols datastores . . . 26
Limiti di configurazione per distribuire ONTAP tools for VMware vSphere per datastore VMFS e NFS . . . 26
ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA) . . . 27
Requisiti di pre-distribuzione per ONTAP tools . . . 28
Foglio di lavoro per l'implementazione . . . 28
Configurazione del firewall di rete . . . 30
Impostazioni di storage ONTAP . . . 30
Distribuisci ONTAP tools . . . 30
Risolvi gli errori di distribuzione degli ONTAP tools . . . 36
Raccogli i file di log . . . 36
Codici di errore di distribuzione . . . 36
Configura ONTAP tools for VMware vSphere . . . 40
Aggiungi istanze del server vCenter agli strumenti ONTAP . . . 40
Registrare il provider VASA con un'istanza del server vCenter negli ONTAP tools . . . 41
Installa il plug-in NFS VAAI usando ONTAP tools . . . 42
Configurare le impostazioni dell'host ESXi negli ONTAP tools . . . 43
Configura le impostazioni di multipath e timeout del server ESXi . . . 43
Imposta i valori host di ESXi . . . 43
Configurare i ruoli e i privilegi utente ONTAP per ONTAP tools . . . 44
Requisiti di mappatura degli aggregate SVM . . . 45
Crea manualmente l'utente e il ruolo ONTAP . . . 45
Aggiorna ONTAP tools for VMware vSphere 10.1 user a 10.3 user . . . 54
Aggiorna ONTAP tools for VMware vSphere utente 10.3 a utente 10.4 . . . 55

Aggiungi un backend di storage a ONTAP tools . . . 56
Associare un backend di storage a un'istanza del vCenter Server negli ONTAP tools . . . 58
Configurare l'accesso alla rete negli ONTAP tools . . . 58
Creare un datastore in ONTAP tools . . . 59
Proteggi i datastore e le macchine virtuali . . . 64
Proteggere un cluster host negli ONTAP tools . . . 64
Proteggi usando la protezione SRA . . . 65
Configurare SRA negli ONTAP tools per proteggere i datastore . . . 65
Configurare SRA in ONTAP tools for VMware vSphere per ambienti SAN e NAS . . . 66
Configurare SRA in ONTAP tools per ambienti altamente scalabili . . . 67
Configurare SRA sull'appliance VMware Live Site Recovery utilizzando ONTAP tools . . . 68
Aggiorna le credenziali SRA negli strumenti ONTAP . . . 69
Configura i siti protetti e di ripristino negli ONTAP tools . . . 70
Configura le risorse del sito protetto e del sito di ripristino . . . 72
Verificare i sistemi di archiviazione replicati negli ONTAP tools . . . 75
Protezione fan-out negli ONTAP tools . . . 76
Gestisci ONTAP tools for VMware vSphere . . . 79
Scopri la dashboard degli strumenti ONTAP . . . 79
Come ONTAP tools gestisce gli igroup e le policy di esportazione . . . 80
Politiche di esportazione . . . 84
Come ONTAP tools gestisce gli igroup . . . 85
Riepilogo rapido del comportamento . . . 85
Contesti di gruppo . . . 85
Comportamento di denominazione . . . 87
Comportamento in base allo scenario . . . 87
Riutilizzo personalizzato degli igroup e comportamento delle API . . . 88
Vista di conversione da nativo a gestito . . . 88
Riutilizzo degli igroup nativi scoperti . . . 89
Scopri l'interfaccia utente di ONTAP tools Manager . . . 89
Gestisci le impostazioni di ONTAP tools Manager . . . 91
Modifica le impostazioni di AutoSupport degli strumenti ONTAP . . . 91
Aggiungi server NTP agli strumenti ONTAP . . . 92
Reimposta le credenziali del provider VASA e SRA negli strumenti ONTAP . . . 92
Modifica le impostazioni di backup di ONTAP tools . . . 93
Abilita i servizi di ONTAP tools . . . 93
Modificare le impostazioni dell'appliance ONTAP tools . . . 94
Aggiungere host VMware vSphere a ONTAP tools . . . 95
Gestisci i datastore . . . 95
Montare i datastore NFS e VMFS negli ONTAP tools . . . 96
Smonta i datastore NFS e VMFS negli ONTAP tools . . . 96
Montare un datastore vVols negli ONTAP tools . . . 97
Ridimensiona i datastore NFS e VMFS negli ONTAP tools . . . 97
Espandi gli datastore vVols negli ONTAP tools . . . 98
Ridurre un datastore vVols negli ONTAP tools . . . 98
Elimina i datastore in ONTAP tools . . . 99

Visualizzazioni dello storage ONTAP per i datastore negli ONTAP tools . . . 100
Visualizzazione dell'archiviazione della macchina virtuale in ONTAP tools . . . 100
Gestire le soglie di archiviazione negli ONTAP tools . . . 101
Gestire i backend di storage in ONTAP tools . . . 101
Scopri lo storage . . . 101
Modifica i backend di archiviazione . . . 101
Rimuovi i backend di storage . . . 102
Analisi dettagliata del backend di storage . . . 102
Gestisci le istanze del server vCenter negli strumenti ONTAP . . . 103
Dissocia i backend di storage con l'istanza del server vCenter . . . 103
Modifica un'istanza del server vCenter . . . 103
Rimuovi un'istanza del server vCenter . . . 104
Rinnova il certificato del server vCenter . . . 104
Gestisci i certificati degli strumenti ONTAP . . . 106
Accedi alla console di manutenzione degli strumenti ONTAP per VMware vSphere . . . 108
Scopri la console di manutenzione di ONTAP tools . . . 108
Configurare l'accesso diagnostico remoto per ONTAP tools . . . 109
Avvia SSH sugli altri nodi di ONTAP tools . . . 110
Aggiorna le credenziali del server vCenter negli ONTAP tools . . . 110
Modificare il flag di convalida del certificato negli ONTAP tools . . . 110
Report degli strumenti ONTAP . . . 112
Gestisci le macchine virtuali . . . 113
Considerazioni sulla migrazione e la clonazione di macchine virtuali per ONTAP tools . . . 113
Migrare le macchine virtuali negli archivi dati vVols in ONTAP tools . . . 114
Pulisci le configurazioni VASA negli ONTAP tools . . . 115
Collegare o scollegare un disco dati da una VM in ONTAP tools . . . 115
Scopri i sistemi di archiviazione e gli host negli ONTAP tools . . . 116
Modifica le impostazioni dell'host ESXi usando ONTAP tools . . . 116
Gestisci le password . . . 117
Cambia la password di ONTAP tools Manager . . . 117
Reimposta la password di ONTAP tools Manager . . . 117
Reimposta la password utente dell'applicazione in ONTAP tools . . . 118
Reimposta la password della console di manutenzione di ONTAP tools . . . 118
Gestisci la protezione del cluster host . . . 119
Modificare un cluster host protetto in ONTAP tools . . . 119
Rimuovere la protezione del cluster host negli ONTAP tools . . . 122
Ripristina la configurazione degli ONTAP tools . . . 123
Disinstallare ONTAP tools . . . 124
Rimuovere i volumi FlexVol dopo aver disinstallato ONTAP tools . . . 124
Aggiorna ONTAP tools per VMware vSphere . . . 126
Aggiorna da ONTAP tools for VMware vSphere 10.x a 10.5 . . . 126
Codici di errore di aggiornamento di ONTAP tools . . . 128
Migra ONTAP tools for VMware vSphere 9.xx a 10.5 . . . 134
Migra dagli ONTAP tools for VMware vSphere 9.xx alla versione 10.5 . . . 134
Migrare il VASA Provider e aggiornare l'SRA negli ONTAP tools . . . 134

Procedura per migrare il provider VASA . . . 134
Procedura per aggiornare l'adattatore di replica dello storage (SRA) . . . 139
Automatizza utilizzando l'API REST . . . 141
Scopri di più sull'API REST di ONTAP tools . . . 141
Fondamenti dei servizi web REST . . . 141
Ambiente di gestione di ONTAP tools . . . 141
Dettagli di implementazione delle API REST di ONTAP tools . . . 142
Come accedere all'API REST . . . 142
Dettagli HTTP . . . 143
Autenticazione . . . 144
Richieste sincrone e asincrone . . . 144
Effettua la tua prima chiamata API REST degli ONTAP tools . . . 144
Prima di iniziare . . . 145
Passaggio 1: Acquisisci un token di accesso . . . 145
Passaggio 2: Effettua la chiamata REST API . . . 145
Riferimento API REST di ONTAP tools . . . 146
Note legali . . . 147
Copyright . . . 147
Marchi . . . 147
Brevetti . . . 147
Informativa sulla privacy . . . 147
Open source . . . 147

# Documentazione di ONTAP tools per VMware vSphere

# Note di rilascio

## Note di rilascio per ONTAP tools

Scopri le nuove funzionalità e i miglioramenti disponibili in ONTAP tools for VMware vSphere 10.5.

Per un elenco completo delle nuove funzionalità e dei miglioramenti, consultare Novità degli ONTAP tools per VMware vSphere 10.5.

Per le informazioni più aggiornate sulla compatibilità, fare riferimento a "Tool NetApp Interoperability Matrix".

La migrazione è supportata da ONTAP tools for VMware vSphere versioni 9.12D1, 9.13D2 e 9.13P2 a ONTAP tools for VMware vSphere 10.5.

Per ulteriori informazioni, consulta il "Note di rilascio di ONTAP tools for VMware vSphere 10.5". È necessario accedere con il proprio NetApp account o crearne uno per accedere alle Note di rilascio.

## Novità degli ONTAP tools per VMware vSphere 10.5

Scopri le nuove funzionalità disponibili in ONTAP tools for VMware vSphere 10.5.

- **Qualificazione della piattaforma**

ONTAP tools for VMware vSphere 10.5 aggiunge il supporto per i sistemi ASA r2, offrendo compatibilità con le più recenti configurazioni hardware e software. Questa versione include anche l'integrazione con ONTAP 9.16.1 e 9.17.1, ampliando gli ambienti supportati.

- **Qualifiche e certificazioni VMware**

ONTAP tools for VMware vSphere 10.5 è conforme agli attuali standard di certificazione di interoperabilità VMware, supportando sia l'host ESXi che il server vCenter.

- **Supporto MetroCluster**

Questa versione introduce il supporto per le configurazioni MetroCluster, migliorando le funzionalità di alta disponibilità e ripristino di emergenza.

- **Gestione della sicurezza e dei certificati**

Questa versione introduce una gestione semplificata dei certificati autofirmati, migliorando sia l'esperienza utente che la conformità agli standard di sicurezza. Offre flussi di lavoro di convalida dei certificati ottimizzati per proteggere le comunicazioni tra ONTAP e ONTAP tools for VMware vSphere.

- **Miglioramenti alla replica**

Questa versione supporta la replica VMFS con gruppo di coerenza gerarchica, inclusi SRA e SnapMirror active sync nei sistemi ASA r2. Supporta i backup con RPO zero per migliorare la protezione e il ripristino dei dati.

- **Aggiornamento e migrazione**

Il processo di aggiornamento e migrazione dalle versioni precedenti di ONTAP tools per VMware vSphere a ONTAP tools per VMware vSphere 10.5 è progettato per essere fluido ed efficiente, riducendo al minimo i

tempi di inattività e garantendo una transizione senza intoppi.

### Piattaforme ONTAP e versioni del server vCenter supportate

ONTAP tools for VMware vSphere 10.5 P1 supporta le configurazioni vCenter High Availability (HA) per i componenti SRA e SnapMirror active sync. vVols non è supportato in questa configurazione. Durante un failover HA, vCenter potrebbe non essere disponibile per diversi minuti. In ambienti di grandi dimensioni o in caso di errore, i tempi di failover possono superare i 15 minuti.

Per ulteriori informazioni, consultare il "Documentazione di vCenter High Availability". Per domande su vCenter HA, contattare "Supporto Broadcom".

Per i dettagli più recenti sulla compatibilità delle versioni, consulta "Tool NetApp Interoperability Matrix".

# Confronto delle funzionalità di ONTAP tools for VMware vSphere 9 e 10

Scopri se la migrazione da ONTAP tools for VMware vSphere 9 a ONTAP tools for VMware vSphere 10.2 o versioni successive è la scelta giusta per te.

Per le informazioni più aggiornate sulla compatibilità, fare riferimento a "Tool NetApp Interoperability Matrix".

| Caratteristica | ONTAP tools 9.13 | ONTAP tools 10.2 e versioni successive |
|---|---|---|
| Proposta di valore chiave | Ottimizza e semplifica le operazioni dal giorno 0 al giorno 2 con funzionalità avanzate di sicurezza, conformità e automazione | Supporto esteso per includere FC per VMFS e NVMe-oF solo per VMFS. Facilità d'uso per NetApp SnapMirror, configurazione semplice per vSphere metro storage cluster e supporto per VMware Live Site Recovery a tre siti |
| Qualifica della release ONTAP | ONTAP 9.9.1 a ONTAP 9.16.1 | ONTAP 9.12.1 a 9.15.1 per ONTAP tools 10.2. ONTAP 9.14.1, 9.15.1, 9.16.0 e 9.16.1 per ONTAP tools 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0 e 9.16.1 per ONTAP tools 10.4. ONTAP 9.16.1P3 e versioni successive sono richieste per ONTAP tools 10.4 quando usi sistemi ASA r2. ONTAP 9.15.1, 9.16.1 e 9.17.0 per ONTAP tools 10.5 |
| Supporto per le release di VMware | vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 a VMware Live Site Recovery 9.0 | vSphere 7.x-8.x vSphere 9.0 da ONTAP tools 10.5 in poi VMware Site Recovery Manager (SRM) 8.7 a VMware Live Site Recovery 9.0 **NOTA:** In ONTAP tools 10.x, SRM supporta i siti condivisi, consentendo una maggiore scalabilità e prestazioni migliorate. |
| Supporto del protocollo | Archivi dati NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI e FCP) | Archivi dati NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI/FCP/NVMe-oF) |

| Caratteristica | ONTAP tools 9.13 | ONTAP tools 10.2 e versioni successive |
|---|---|---|
| Scalabilità | Host e VM: 300 host, fino a 10K VM<br>Datastore: 600 NFS, fino a 50 VMFS | Host e VM: 600 host |
| Osservabilità | Dashboard relative a prestazioni, capacità e conformità degli host, report dinamici su VM e datastore | Dashboard aggiornate relative a prestazioni, capacità e conformità degli host, report dinamici su VM e datastore |
| Protezione dei dati | Replica SRA per VMFS e NFS. Integrazione SCV e interoperabilità per backup. | Replica SRA per iSCSI VMFS e NFS v3 datastore, protezione a tre siti che combina SMAS e VMware Live Site Recovery. Supporto SRA per FCP con VMFS. |
| Supporto VASA Provider | VASA 4.0 | VASA 3.0 |

# Concetti

## Scopri gli strumenti ONTAP

ONTAP tools per VMware vSphere è una suite di strumenti per la gestione del ciclo di vita delle macchine virtuali. Si integra con l'ecosistema VMware per semplificare il provisioning dei datastore e fornire una protezione di base per le macchine virtuali. È una raccolta di microservizi scalabili orizzontalmente ed event-driven, distribuiti come Open Virtual Appliance (OVA).

ONTAP tools per VMware vSphere supporta:

- Funzionalità principali delle macchine virtuali (VM) come la protezione e il ripristino di emergenza
- VASA Provider per la gestione dello storage basata su policy
- Gestione basata su policy dello storage
- Storage Replication Adapter (SRA)

**Elevata disponibilità per ONTAP tools for VMware**

ONTAP tools for VMware vSphere offre supporto per l'alta disponibilità (HA) per aiutarti a mantenere un funzionamento ininterrotto durante i guasti.

La soluzione HA ti aiuta a ripristinare rapidamente dai seguenti tipi di interruzioni:

- Guasto dell'host: è supportato solo il guasto di un singolo nodo.
- Guasto alla rete
- Errore della macchina virtuale (guest OS)
- Errore dell'applicazione (ONTAP tools)

Non è necessario eseguire alcuna configurazione aggiuntiva per abilitare l'HA per ONTAP tools for VMware vSphere.

ONTAP tools for VMware vSphere non supporta vCenter HA.

Per utilizzare la funzionalità HA, assicurarsi che l'hot-add della CPU e l'hot-plug della memoria siano abilitati durante la distribuzione o nelle impostazioni della macchina virtuale.

# Concetti e termini chiave negli ONTAP tools

La sezione seguente descrive i concetti e i termini chiave utilizzati nel documento.

**Autorità di certificazione (CA)**

Una CA è un'entità fidata che rilascia certificati Secure Sockets Layer (SSL).

**Gruppo di coerenza**

Un gruppo di coerenza è una raccolta di volumi gestiti come un'unica unità. I gruppi di coerenza vengono sincronizzati per coerenza dei dati tra unità di storage e volumi. In ONTAP, offrono una gestione semplice e

garanzie di protezione per un carico di lavoro applicativo che si estende su più volumi. Scopri di più su "gruppi di coerenza".

### Dual stack

Una rete dual-stack è un ambiente di rete che supporta l'utilizzo simultaneo di indirizzi IPv4 e IPv6.

### Alta disponibilità (HA)

I nodi del cluster sono configurati in coppie HA per operazioni senza interruzioni.

### Numero di unità logica (LUN)

Una LUN è un numero utilizzato per identificare un'unità logica all'interno di una Storage Area Network (SAN). Questi dispositivi indirizzabili sono in genere dischi logici a cui si accede tramite il protocollo Small Computer System Interface (SCSI) o uno dei suoi derivati incapsulati.

### Namespace e sottosistema NVMe

Un namespace NVMe è una quantità di memoria non volatile che può essere formattata in blocchi logici. I namespace sono l'equivalente delle LUN per i protocolli FC e iSCSI, e un sottosistema NVMe è analogo a un igroup. Un sottosistema NVMe può essere associato a iniziatori così che gli iniziatori associati possano accedere ai namespace all'interno del sottosistema.

### ONTAP tools Manager

ONTAP tools Manager fornisce agli amministratori di ONTAP tools for VMware vSphere un maggiore controllo sulle istanze di vCenter Server gestite e sui backend di storage integrati. Aiuta a gestire le istanze di vCenter Server, i backend di storage, i certificati, le password e i bundle di log.

### Open Virtual Appliance (OVA)

OVA è un open standard per il packaging e la distribuzione di appliance virtuali o software che devono essere eseguiti su macchine virtuali.

### Recovery Point Objective (RPO)

L'RPO (Recovery Point Objective) misura la frequenza con cui esegui il backup o replichi i dati. Specifica il momento esatto in cui devi ripristinare i dati dopo un'interruzione per riprendere le operazioni di business. Ad esempio, se un'organizzazione ha un RPO di 4 ore, può tollerare la perdita di dati fino a 4 ore in caso di disastro.

### SnapMirror active sync

SnapMirror active sync consente ai servizi di business di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover trasparente delle applicazioni utilizzando una copia secondaria. Non è necessario alcun intervento manuale o script personalizzato per attivare un failover con SnapMirror active sync. Scopri di più "SnapMirror active sync".

### Backend di storage

I backend di storage sono l'infrastruttura di storage sottostante che l'host ESXi utilizza per archiviare file, dati e altre risorse delle macchine virtuali. Consentono all'host ESXi di accedere e gestire i dati persistenti, fornendo la capacità di storage e le prestazioni necessarie per un ambiente virtualizzato.

**cluster globale (storage backend)**

I backend di storage globali, disponibili solo con le credenziali del cluster ONTAP, vengono configurati tramite l'interfaccia di ONTAP tools Manager. Possono essere aggiunti con privilegi minimi per consentire la scoperta delle risorse di cluster essenziali necessarie per la gestione di vVols. I cluster globali sono ideali per scenari di multitenancy in cui un utente SVM viene aggiunto localmente per la gestione di vVols.

**Backend di storage locale**

I backend di storage locali con credenziali di cluster o SVM vengono aggiunti tramite l'interfaccia utente di ONTAP tools e sono limitati a un vCenter. Quando usi le credenziali di cluster localmente, gli SVM associati vengono automaticamente mappati con il vCenter per gestire vVols o VMFS. Per la gestione di VMFS, incluso SRA, ONTAP tools supporta le credenziali SVM senza la necessità di un cluster globale.

### Storage Replication Adapter (SRA)

SRA è il software specifico del fornitore di storage installato all'interno dell'appliance VMware Live Site Recovery. L'adattatore consente la comunicazione tra Site Recovery Manager e uno storage controller sia a livello di Storage Virtual Machine (SVM) sia a livello di configurazione del cluster.

### Macchina virtuale di storage (SVM)

SVM è l'unità di multitenancy in ONTAP. Come una macchina virtuale in esecuzione su un hypervisor, SVM è un'entità logica che astrae le risorse fisiche. SVM contiene volumi di dati e una o più LIF attraverso cui fornisce dati ai client.

### Configurazione uniforme e non uniforme

- **Uniform host access** significa che gli host di due siti sono connessi a tutti i percorsi verso i cluster di storage su entrambi i siti. I percorsi tra siti sono estesi su distanze.
- **L'accesso host non uniforme** significa che gli host in ciascun sito sono connessi solo al cluster nello stesso sito. I percorsi tra siti e i percorsi estesi non sono connessi.

> L'accesso host uniforme è supportato per qualsiasi implementazione di sincronizzazione attiva SnapMirror; l'accesso host non uniforme è supportato solo per le implementazioni simmetriche attivo/attivo. Ulteriori informazioni su "SnapMirror panoramica della sincronizzazione attiva in ONTAP".

### Virtual Machine File System (VMFS)

VMFS è un file system cluster progettato per archiviare i file delle macchine virtuali negli ambienti VMware vSphere.

### Volumi virtuali (vVols)

vVols forniscono un'astrazione a livello di volume per lo storage utilizzato da una macchina virtuale. Include diversi vantaggi e offre un'alternativa all'utilizzo di un LUN tradizionale. Un vVol datastore è in genere associato a un singolo LUN che funge da container per vVols.

### VM Storage Policy

Le VM Storage Policies vengono create nel vCenter Server sotto Policies and Profiles. Per vVols, crea un set di regole utilizzando le regole del provider del tipo di storage NetApp vVols.

#### VMware Live Site Recovery

VMware Live Site Recovery, precedentemente noto come Site Recovery Manager (SRM), offre funzionalità di continuità operativa, ripristino di emergenza, migrazione del sito e test non invasivi per gli ambienti virtuali VMware.

#### API VMware vSphere per la consapevolezza dello storage (VASA)

VASA è un insieme di API che integrano gli array di storage con vCenter Server per la gestione e l'amministrazione. L'architettura si basa su diversi componenti, tra cui il VASA Provider, che gestisce la comunicazione tra VMware vSphere e i sistemi di storage.

#### VMware vSphere Storage API - Integrazione array (VAAI)

VAAI è un insieme di API che consente la comunicazione tra gli host VMware vSphere ESXi e i dispositivi di storage. Le API includono una serie di operazioni primitive utilizzate dagli host per delegare le operazioni di storage all'array. VAAI può fornire significativi miglioramenti delle prestazioni per le attività che richiedono un utilizzo intensivo dello storage.

#### vSphere Metro Storage Cluster

vSphere Metro Storage Cluster (vMSC) è un'architettura che abilita e supporta vSphere in una distribuzione di cluster esteso. Le soluzioni vMSC sono supportate su NetApp MetroCluster e SnapMirror active sync (precedentemente SMBC). Queste soluzioni offrono una maggiore continuità operativa in caso di errore del dominio. Il modello di resilienza si basa sulle specifiche scelte di configurazione. Scopri di più su "Cluster di storage Metro VMware vSphere".

#### datastore vVols

Il vVols datastore è una rappresentazione logica di un vVols container creato e gestito da un VASA Provider.

#### RPO zero

RPO sta per recovery point objective, ovvero la quantità di perdita di dati considerata accettabile durante un determinato periodo di tempo. Zero RPO indica che non è accettabile alcuna perdita di dati.

# Controllo degli accessi in base al ruolo (RBAC)

## Scopri RBAC degli strumenti ONTAP

Il controllo degli accessi basato sui ruoli (RBAC) è un framework di sicurezza per il controllo dell'accesso alle risorse all'interno di un'organizzazione. RBAC semplifica l'amministrazione definendo ruoli con specifici livelli di autorità per eseguire azioni, invece di assegnare autorizzazioni ai singoli utenti. I ruoli definiti vengono assegnati agli utenti, il che aiuta a ridurre il rischio di errore e semplifica la gestione del controllo degli accessi in tutta la tua organizzazione.

Il modello standard RBAC si compone di diverse tecnologie o fasi di implementazione di complessità crescente. Di conseguenza, le implementazioni RBAC effettive, in base alle esigenze dei fornitori di software e dei loro clienti, possono variare da relativamente semplici a molto complesse.

## Componenti RBAC

A un livello generale, esistono diversi componenti che sono generalmente inclusi in ogni implementazione RBAC. Questi componenti sono collegati tra loro in vari modi nell'ambito della definizione dei processi di autorizzazione.

### Privileges

Un *privilegio* è un'azione o una capacità che può essere consentita o negata. Può trattarsi di qualcosa di semplice, come la possibilità di leggere un file, o di un'operazione più astratta specifica di un determinato sistema software. Privileges possono anche essere definiti per limitare l'accesso agli endpoint delle REST API e ai comandi della CLI. Ogni implementazione di RBAC include privilegi predefiniti e può anche consentire agli amministratori di creare privilegi personalizzati.

### Ruoli

Un ruolo è un container che include uno o più privilegi. I ruoli sono generalmente definiti in base a compiti o funzioni lavorative specifiche. Quando un ruolo viene assegnato a un utente, l'utente riceve tutti i privilegi contenuti nel ruolo. E come per i privilegi, le implementazioni includono ruoli predefiniti e generalmente permettono di creare ruoli personalizzati.

### Oggetti

Un *oggetto* rappresenta una risorsa reale o astratta identificata all'interno dell'ambiente RBAC. Le azioni definite tramite i privilegi vengono eseguite sugli oggetti associati o con essi. A seconda dell'implementazione, i privilegi possono essere concessi a un tipo di oggetto o a una specifica istanza di oggetto.

### Utenti e gruppi

Agli utenti viene assegnato o associato un ruolo applicato dopo l'autenticazione. Alcune implementazioni RBAC consentono di assegnare un solo ruolo a un utente, mentre altre consentono più ruoli per utente, magari con un solo ruolo attivo alla volta. L'assegnazione di ruoli ai gruppi può semplificare ulteriormente l'amministrazione della sicurezza.

### Autorizzazioni

Un permesso è una definizione che associa un utente o un gruppo insieme a un ruolo a un oggetto. I permessi possono essere utili in un modello a oggetti gerarchico, dove possono essere facoltativamente ereditati dagli elementi figli della gerarchia.

## Due ambienti RBAC

Ci sono due ambienti RBAC distinti che devi considerare quando lavori con ONTAP tools for VMware vSphere 10. ONTAP tools for VMware vSphere 10 richiede privilegi specifici sia in vCenter che in ONTAP per eseguire le sue operazioni. Anche se ONTAP tools automatizza le attività di gestione dello storage, non crea account utente né in vCenter né in ONTAP. Gli account di servizio devono essere creati da un amministratore vSphere quando necessario. Questa documentazione fornisce indicazioni agli amministratori per assegnare i ruoli e le autorizzazioni necessari per una gestione efficace di ONTAP tools.

### VMware vCenter Server

L'implementazione RBAC in VMware vCenter Server viene utilizzata per limitare l'accesso agli oggetti esposti tramite l'interfaccia utente del client vSphere. Come parte dell'installazione di ONTAP tools for VMware vSphere 10, l'ambiente RBAC viene esteso per includere oggetti aggiuntivi che rappresentano le funzionalità di ONTAP tools. L'accesso a questi oggetti è fornito tramite il plug-in remoto. Vedi "vCenter Server ambiente RBAC" per ulteriori informazioni.

### cluster ONTAP

ONTAP tools for VMware vSphere 10 si connette a un cluster ONTAP tramite l'ONTAP REST API per eseguire

operazioni relative allo storage. L'accesso alle risorse di storage è controllato tramite un ruolo ONTAP associato all'utente ONTAP fornito durante l'autenticazione. Vedi "Ambiente RBAC di ONTAP" per maggiori informazioni.

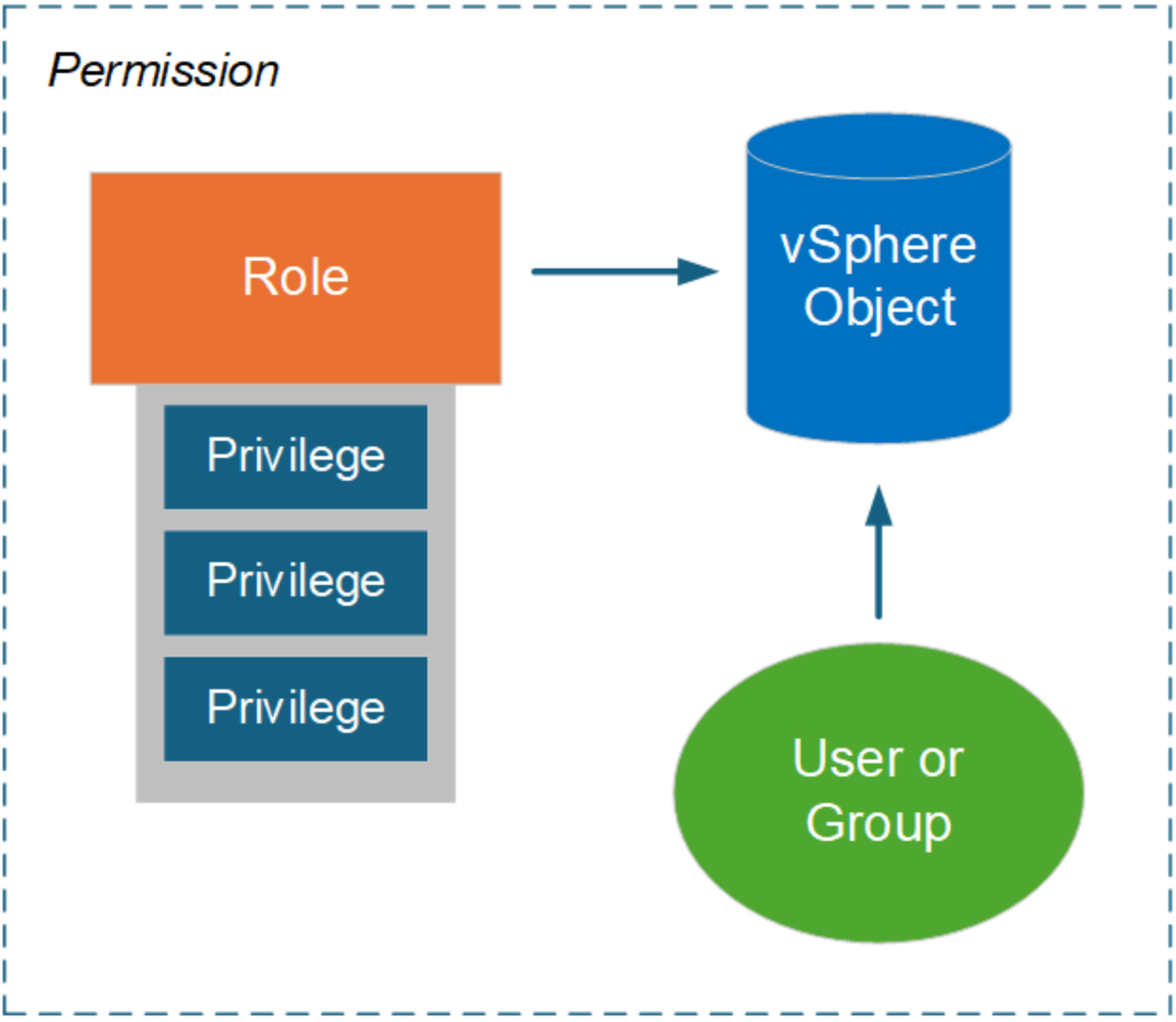
## RBAC con VMware vSphere

### Come funziona RBAC di vCenter Server con ONTAP tools

VMware vCenter Server offre una funzionalità RBAC che ti permette di controllare l'accesso agli oggetti vSphere. È una parte importante dei servizi di sicurezza centralizzati di autenticazione e autorizzazione di vCenter.

#### Illustrazione di un permesso del server vCenter

Un permesso è il fondamento per l'applicazione del controllo degli accessi nell'ambiente vCenter Server. Viene applicato a un oggetto vSphere con un utente o un gruppo incluso nella definizione del permesso. Una rappresentazione high-level di un permesso vCenter è fornita nella figura qui sotto.



#### Componenti di un'autorizzazione del server vCenter

Un'autorizzazione del server vCenter è un insieme di diversi componenti che vengono collegati tra loro al momento della creazione dell'autorizzazione stessa.

### oggetti vSphere

Le autorizzazioni sono associate a oggetti vSphere, come il vCenter Server, host ESXi, macchine virtuali, datastore, data center e cartelle. In base alle autorizzazioni assegnate all'oggetto, il vCenter Server determina quali azioni o attività possono essere eseguite sull'oggetto da ciascun utente o gruppo. Per le attività specifiche di ONTAP tools for VMware vSphere, tutte le autorizzazioni vengono assegnate e convalidate a livello di root o di cartella root del vCenter Server. Vedi "Usa RBAC con il server vCenter" per ulteriori informazioni.

### Privileges e ruoli

Ci sono due tipi di privilegi vSphere utilizzati con ONTAP tools for VMware vSphere 10. Per semplificare il lavoro con RBAC in questo ambiente, ONTAP tools fornisce ruoli che contengono i privilegi nativi e personalizzati richiesti. I privilegi includono:

- Privilegi nativi del server vCenter

  Questi sono i privilegi forniti da vCenter Server.

- Privilegi specifici degli strumenti ONTAP

  Questi sono privilegi personalizzati unici di ONTAP tools for VMware vSphere.

### Utenti e gruppi

Puoi definire utenti e gruppi usando Active Directory o l'istanza locale del server vCenter. In combinazione con un ruolo, puoi creare un'autorizzazione su un oggetto nella gerarchia degli oggetti vSphere. L'autorizzazione concede l'accesso in base ai privilegi del ruolo associato. Nota che i ruoli non vengono assegnati direttamente agli utenti in modo isolato. Invece, utenti e gruppi ottengono l'accesso a un oggetto tramite i privilegi di ruolo come parte dell'autorizzazione del server vCenter.

### vCenter Server: considerazioni RBAC per ONTAP tools

Ci sono diversi aspetti degli ONTAP tools for VMware vSphere 10 nell'implementazione RBAC con vCenter Server che dovresti considerare prima di usarli in un ambiente di produzione.

#### vCenter ruoli e l'account amministratore

Devi definire e utilizzare i ruoli server personalizzati di vCenter solo se vuoi limitare l'accesso agli oggetti vSphere e alle attività amministrative associate. Se non è necessario limitare l'accesso, puoi usare un account amministratore. Ogni account amministratore è definito con il ruolo di Administrator al livello superiore della gerarchia degli oggetti. Questo garantisce l'accesso completo agli oggetti vSphere, inclusi quelli aggiunti da ONTAP tools for VMware vSphere 10.

#### Gerarchia degli oggetti vSphere

L'inventario degli oggetti vSphere è organizzato in una gerarchia. Ad esempio, puoi scendere nella gerarchia come segue:

`vCenter Server` --> `Datacenter` --> `Cluster` --> `ESXi host` --> `Virtual Machine`

Tutte le autorizzazioni vengono validate nella gerarchia degli oggetti di vSphere, ad eccezione delle operazioni del plug-in VAAI, che vengono validate rispetto all'host ESXi di destinazione.

#### Ruoli inclusi con ONTAP tools for VMware vSphere 10

Per semplificare il lavoro con il controllo degli accessi basato sui ruoli (RBAC) del server vCenter, ONTAP tools for VMware vSphere fornisce ruoli predefiniti adattati a varie attività amministrative.

> Se necessario, è possibile creare nuovi ruoli personalizzati. Per farlo, clonare uno dei ruoli esistenti di ONTAP tools e modificarlo secondo le proprie esigenze. Dopo aver apportato le modifiche alla configurazione, gli utenti client vSphere interessati dovranno disconnettersi e accedere nuovamente per attivare le modifiche.

Per visualizzare i ruoli di ONTAP tools for VMware vSphere, selezionare **Menu** nella parte superiore del vSphere Client e fare clic su **Amministrazione** e poi su **Ruoli** a sinistra. I seguenti privilegi devono essere inclusi nel ruolo assegnato all'utente vCenter responsabile della distribuzione o dell'onboarding del vCenter Server. Assicurarsi che questi privilegi siano configurati come prerequisito per il processo di distribuzione o onboarding.

- Allarmi
  - Conferma l'allarme
- Libreria dei contenuti
  - Aggiungi elemento della libreria
  - Verifica in un template
  - Dai un'occhiata a un modello
  - Scarica i file
  - Importa storage
  - Storage di lettura
  - Sincronizza elemento della libreria
  - Sincronizza la libreria sottoscritta
  - Visualizza le impostazioni di configurazione
- Datastore
  - Assegna spazio
  - Esplora datastore
  - Operazioni sui file di basso livello
  - Rimuovi file
  - Aggiornare i file della macchina virtuale
  - Aggiornare i metadati della macchina virtuale
- ESX Agent Manager
  - Visualizza
- Cartella

    - Crea cartella
- Host
    - Configurazione
        - Impostazioni avanzate
        - Modifica impostazioni
        - Configurazione di rete
        - Risorse di sistema
        - Configurazione dell'avvio automatico della macchina virtuale
    - Operazioni locali
        - Crea macchina virtuale
        - Eliminare la macchina virtuale
        - Riconfigurare la macchina virtuale
- Rete
    - Assegna rete
    - Configurare
- OvfManager
    - OvfConsumer Accesso
- Profilo host
    - Visualizza
- Risorsa
    - Assegna la macchina virtuale al pool di risorse
- Attività pianificata
    - Crea attività
    - Modifica attività
    - Esegui attività
- Attività
    - Crea attività
    - Aggiorna attività
- vApp
    - Aggiungi macchina virtuale
    - Assegna pool di risorse
    - Assegna vApp
    - Crea
    - Importare
    - Sposta
    - Spegni
    - Accendi

    - Scarica da URL
    - Visualizza l’ambiente OVF
- Macchina virtuale
    - Modifica configurazione
        - Aggiungi disco esistente
        - Aggiungi nuovo disco
        - Aggiungi o rimuovi dispositivo
        - Configurazione avanzata
        - Modifica il conteggio della CPU
        - Modifica memoria
        - Modifica impostazioni
        - Cambia risorsa
        - Estendi il disco virtuale
        - Modificare le impostazioni del dispositivo
        - Rimuovere il disco
        - Reimposta le informazioni guest
        - Aggiorna la compatibilità della macchina virtuale
    - Modifica inventario
        - Crea da esistente
        - Crea nuovo
        - Sposta
        - Registrati
        - Rimuovi
        - Annulla registrazione
    - Interazione
        - Operazione di backup su macchina virtuale
        - Configura i supporti CD
        - Configura i supporti floppy
        - Collega i dispositivi
        - Interazione con la console
        - Gestione del sistema operativo guest tramite API VIX
        - Spegni
        - Accendi
        - Ripristina
        - Sospendi
    - Provisioning
        - Consenti l’accesso al disco

        - Clona modello
        - Personalizza guest
        - Distribuisci modello
        - Modifica specifica di personalizzazione
        - Leggi le specifiche di personalizzazione
    - Gestione Snapshot
        - Crea snapshot
        - Rimuovi snapshot
        - Rinomina snapshot
        - Ripristina allo snapshot

Ci sono tre ruoli predefiniti, come descritto di seguito.

**Amministratore di NetApp ONTAP tools for VMware vSphere**

Fornisce tutti i privilegi nativi del server vCenter e i privilegi specifici degli ONTAP tools necessari per eseguire le attività principali di amministratore degli ONTAP tools for VMware vSphere.

**NetApp ONTAP tools for VMware vSphere in sola lettura**

Fornisce accesso in sola lettura agli strumenti ONTAP. Questi utenti non possono eseguire alcuna azione degli strumenti ONTAP per VMware vSphere soggetta a controllo degli accessi.

**Provisioning di NetApp ONTAP tools for VMware vSphere**

Fornisce alcuni dei privilegi nativi del vCenter Server e dei privilegi specifici degli ONTAP tools necessari per il provisioning dello storage. Puoi eseguire le seguenti attività:

- Crea nuovi archivi dati
- Gestisci i datastore

#### vSphere oggetti e backend di storage ONTAP

I due ambienti RBAC lavorano insieme. Quando esegui un'attività nell'interfaccia client di vSphere, vengono prima verificati i ruoli degli ONTAP tools definiti per il vCenter Server. Se l'operazione è consentita da vSphere, vengono poi esaminati i privilegi del ruolo ONTAP. Questo secondo passaggio viene eseguito in base al ruolo ONTAP assegnato all'utente quando è stato creato e configurato il backend di storage.

#### Lavorare con RBAC del server vCenter

Ci sono alcuni aspetti da considerare quando lavori con i privilegi e le autorizzazioni del server vCenter.

### Privilegi richiesti

Per accedere all'interfaccia utente di ONTAP tools for VMware vSphere 10, devi avere il privilegio *View* specifico di ONTAP tools. Se accedi a vSphere senza questo privilegio e fai clic sull'icona NetApp, ONTAP tools for VMware vSphere mostra un messaggio di errore e ti impedisce di accedere all'interfaccia utente.

Il livello di assegnazione nella gerarchia degli oggetti vSphere determina a quali parti dell'interfaccia utente puoi accedere. Assegnando il privilegio di visualizzazione all'oggetto radice, puoi accedere a ONTAP tools for VMware vSphere facendo clic sull'icona NetApp.

Puoi invece assegnare il privilegio di visualizzazione a un altro livello di oggetto vSphere inferiore. Tuttavia,

questo limiterà i menu di ONTAP tools for VMware vSphere a cui puoi accedere e che puoi usare.

#### Assegnare le autorizzazioni

Devi usare le autorizzazioni del server vCenter se vuoi limitare l'accesso agli oggetti e alle attività di vSphere. Il punto in cui assegni le autorizzazioni nella gerarchia degli oggetti di vSphere determina quali attività di ONTAP tools for VMware vSphere 10 gli utenti possono eseguire.

A meno che tu non abbia bisogno di definire un accesso più restrittivo, di solito è una buona pratica assegnare le autorizzazioni a livello di oggetto radice o di cartella radice.

Le autorizzazioni disponibili con ONTAP tools for VMware vSphere 10 si applicano a oggetti personalizzati non-vSphere, come i sistemi storage. Se possibile, dovresti assegnare queste autorizzazioni all'oggetto radice di ONTAP tools for VMware vSphere perché non esiste un oggetto vSphere a cui puoi assegnarle. Ad esempio, qualsiasi autorizzazione che includa il privilegio "Aggiungi/Modifica/Rimuovi sistemi storage" di ONTAP tools for VMware vSphere dovrebbe essere assegnata a livello dell'oggetto radice.

Quando definisci un'autorizzazione a un livello superiore nella gerarchia degli oggetti, puoi configurarla in modo che venga trasmessa ed ereditata dagli oggetti figlio. Se serve, puoi assegnare autorizzazioni aggiuntive agli oggetti figlio che sovrascrivono quelle ereditate dal genitore.

Puoi modificare un'autorizzazione in qualsiasi momento. Se cambi uno qualsiasi dei privilegi all'interno di un'autorizzazione, gli utenti associati all'autorizzazione devono disconnettersi da vSphere e accedere di nuovo per rendere effettiva la modifica.

## RBAC con ONTAP

### Come funziona ONTAP RBAC con ONTAP tools

ONTAP offre un ambiente RBAC robusto ed estensibile. Puoi utilizzare la funzionalità RBAC per controllare l'accesso allo storage e alle operazioni di sistema esposte tramite REST API e CLI. È utile conoscere l'ambiente prima di usarlo con una distribuzione di ONTAP tools for VMware vSphere 10.

#### Panoramica delle opzioni amministrative

Sono disponibili diverse opzioni per l'utilizzo di ONTAP RBAC, a seconda dell'ambiente e degli obiettivi. Di seguito trovi una panoramica delle principali decisioni amministrative. Vedi anche "Automazione ONTAP: Panoramica della sicurezza RBAC" per ulteriori informazioni.

ONTAP RBAC è progettato specificamente per un ambiente di storage ed è più semplice rispetto all'implementazione RBAC fornita con vCenter Server. Con ONTAP, assegni un ruolo direttamente all'utente. Non è necessario configurare autorizzazioni esplicite, come quelle utilizzate con vCenter Server, con ONTAP RBAC.

#### Tipi di ruoli e privilegi

È necessario un ruolo ONTAP quando si definisce un utente ONTAP. Esistono due tipi di ruoli ONTAP:

- REST

  I ruoli REST sono stati introdotti con ONTAP 9.6 e vengono generalmente applicati agli utenti che accedono a ONTAP tramite l'API REST. I privilegi inclusi in questi ruoli sono definiti in termini di accesso

agli endpoint dell'API REST di ONTAP e alle azioni associate.

- Tradizionale

  Si tratta dei ruoli legacy esistenti prima di ONTAP 9.6. Essi continuano a rappresentare un aspetto fondamentale di RBAC. I privilegi sono definiti in termini di accesso ai comandi CLI di ONTAP.

Sebbene i ruoli REST siano stati introdotti più di recente, i ruoli tradizionali offrono alcuni vantaggi. Ad esempio, è possibile includere parametri di query aggiuntivi per consentire ai Privileges di definire con maggiore precisione gli oggetti a cui si applicano.

**Ambito**

I ruoli ONTAP possono essere definiti con uno dei due diversi ambiti. Possono essere applicati a uno specifico SVM di dati (livello SVM) o all'intero cluster ONTAP (livello cluster).

**Definizioni dei ruoli**

ONTAP offre una serie di ruoli predefiniti sia a livello di cluster che di SVM. Puoi anche definire ruoli personalizzati.

#### Lavorare con i ruoli REST di ONTAP

Ci sono diverse considerazioni da tenere presenti quando utilizzi i ruoli REST ONTAP inclusi negli ONTAP tools for VMware vSphere 10.

**Mappatura dei ruoli**

Sia che tu utilizzi un ruolo tradizionale o REST, tutte le decisioni di accesso di ONTAP si basano sul comando CLI sottostante. Ma poiché i privilegi in un ruolo REST sono definiti in termini di endpoint REST API, ONTAP deve creare un ruolo tradizionale *mappato* per ciascuno dei ruoli REST. Quindi, ogni ruolo REST viene associato a un ruolo tradizionale sottostante. Questo permette a ONTAP di prendere decisioni di controllo degli accessi in modo coerente, indipendentemente dal tipo di ruolo. Non puoi modificare i ruoli mappati in parallelo.

**Definizione di un ruolo REST utilizzando i privilegi CLI**

Poiché ONTAP utilizza sempre i comandi CLI per determinare l'accesso a livello base, è possibile esprimere un ruolo REST utilizzando i privilegi dei comandi CLI anziché gli endpoint REST. Un vantaggio di questo approccio è la maggiore granularità disponibile con i ruoli tradizionali.

**Interfaccia amministrativa durante la definizione dei ruoli ONTAP**

Puoi creare utenti e ruoli con la ONTAP CLI e la REST API. Tuttavia, è più comodo usare l'interfaccia di System Manager insieme al file JSON disponibile tramite ONTAP tools Manager. Vedi "Usa ONTAP RBAC con ONTAP tools for VMware vSphere 10" per maggiori informazioni.

### Considerazioni RBAC di ONTAP per ONTAP tools

Ci sono diversi aspetti degli ONTAP tools for VMware vSphere 10 relativi all'implementazione RBAC con ONTAP che dovresti considerare prima di utilizzarli in un ambiente di produzione.

#### Panoramica del processo di configurazione

ONTAP tools for VMware vSphere include il supporto per la creazione di un utente ONTAP con un ruolo personalizzato. Le definizioni sono contenute in un file JSON che puoi caricare sul cluster ONTAP. Puoi creare l'utente e personalizzare il ruolo in base al tuo ambiente e alle tue esigenze di sicurezza.

Di seguito sono descritte a un livello high-level le principali fasi di configurazione. Consulta "Configura i ruoli utente e i privilegi di ONTAP" per maggiori dettagli.

**1. Prepara**

Devi avere le credenziali amministrative sia per ONTAP tools Manager che per l'ONTAP cluster.

**2. Scarica il file di definizione JSON**

Dopo aver effettuato l'accesso all'interfaccia utente di ONTAP tools Manager, puoi scaricare il file JSON contenente le definizioni RBAC.

**3. Crea un utente ONTAP con un ruolo**

Dopo aver effettuato l'accesso a System Manager, puoi creare l'utente e il ruolo:

1. Seleziona **Cluster** a sinistra e poi **Settings**.
2. Scorri verso il basso fino a **Utenti e ruoli** e fai clic su −→.
3. Seleziona **Aggiungi** sotto **Utenti** e seleziona **Prodotti di virtualizzazione**.
4. Seleziona il file JSON sulla tua workstation locale e caricalo.

**4. Configura il ruolo**

Nell'ambito della definizione del ruolo, devi prendere diverse decisioni amministrative. Vedi Configura il ruolo usando System Manager per maggiori dettagli.

#### Configura il ruolo usando System Manager

Dopo aver iniziato a creare un nuovo utente e ruolo con System Manager e aver caricato il file JSON, puoi personalizzare il ruolo in base al tuo ambiente e alle tue esigenze.

### Configurazione principale di utenti e ruoli

Le definizioni RBAC sono raggruppate in diverse funzionalità di prodotto, incluse combinazioni di VSC, VASA Provider e SRA. Dovresti selezionare l'ambiente o gli ambienti in cui ti serve il supporto RBAC. Ad esempio, se vuoi che i ruoli supportino la funzionalità di plug-in remoto, seleziona VSC. Devi anche scegliere il nome utente e la password associata.

### Privileges

I privilegi di ruolo sono organizzati in quattro gruppi in base al livello di accesso necessario per lo storage ONTAP. I privilegi su cui si basano i ruoli includono:

- Scoperta

  Questo ruolo ti permette di aggiungere sistemi di archiviazione.

- Crea storage

  Questo ruolo ti consente di creare spazio di archiviazione. Include anche tutti i privilegi associati al ruolo di discovery.

- Modifica lo storage

  Questo ruolo ti consente di modificare lo spazio di archiviazione. Include anche tutti i privilegi associati ai ruoli di individuazione e creazione dello spazio di archiviazione.

- Distruggi storage

  Questo ruolo ti permette di eliminare lo storage. Include anche tutti i privilegi associati ai ruoli di individuazione, creazione e modifica dello storage.

### Genera l’utente con un ruolo

Dopo aver selezionato le opzioni di configurazione per il tuo ambiente, fai clic su **Aggiungi** e ONTAP crea l’utente e il ruolo. Il nome del ruolo generato è una concatenazione dei seguenti valori:

- Valore del prefisso costante definito nel file JSON (ad esempio "OTV_10")
- Funzionalità del prodotto selezionata
- Elenco dei set di privilegi.

#### Esempio

```
OTV_10_VSC_Discovery_Create
```

Il nuovo utente verrà aggiunto all’elenco nella pagina 'Utenti e ruoli'. Si noti che sono supportati entrambi i metodi di accesso utente, HTTP e ONTAPI.

# Distribuisci ONTAP tools per VMware vSphere

## Guida rapida per ONTAP tools for VMware vSphere

Configura ONTAP tools for VMware vSphere con questa sezione di avvio rapido.

Completa innanzitutto queste attività principali per rendere operativi gli ONTAP tools per la gestione e il provisioning fin dal giorno 0. Successivamente, completa le attività facoltative in base al tuo ambiente e ai requisiti di protezione.

Inizialmente, distribuirai ONTAP tools for VMware vSphere come una configurazione a nodo singolo di piccole dimensioni che fornisce servizi di base per supportare i datastore NFS e VMFS. Per espandere la configurazione per ulteriori container per servizio, per una maggiore resilienza o per utilizzare i datastore vVols e l'alta disponibilità (HA), completa prima questo flusso di lavoro e poi procedi con i passaggi di espansione. Per ulteriori informazioni, consulta la "workflow di deployment HA".

**Pianifica la tua implementazione**

Conferma che il tuo ambiente sia pronto per una distribuzione supportata. Verifica che le versioni di vSphere, ONTAP e dell'host ESXi siano compatibili con la versione degli ONTAP tools. Alloca CPU, memoria e spazio su disco sufficienti. In base alle tue regole di sicurezza, potresti dover configurare firewall o altri strumenti di sicurezza per consentire il traffico di rete.

Assicurati che il vCenter Server sia installato e accessibile.

- "Strumento Interoperability Matrix Tool"
- "Requisiti e limiti di configurazione di ONTAP tools per VMware vSphere"
- "Prima di iniziare"

**Distribuisci ONTAP tools per VMware vSphere**

Distribuisci l'appliance ONTAP tools per stabilire i servizi di base per i datastore NFS e VMFS.

Inizialmente, implementerai ONTAP tools for VMware vSphere come configurazione a nodo singolo di piccole dimensioni. Se prevedi di espandere la configurazione per utilizzare datastore vVols e l'alta disponibilità (HA), lo farai dopo aver completato questo workflow. Per espandere a una configurazione HA, assicurati che CPU hot-add e memory hot-plug siano abilitati.

Durante la distribuzione, esamina attentamente i campi di **Customize template**, in particolare host name, utilizzo dell'indirizzo IP di ONTAP tools e requisiti DNS.

- "Distribuisci ONTAP tools per VMware vSphere"

**Registrati e installa il plug-in client vCenter**

Aggiungi un'istanza del server vCenter per registrare il plug-in client vCenter e applicare i privilegi e i ruoli necessari. Quando aggiungi un'istanza del server vCenter, ONTAP tools registra il plug-in remoto, applica privilegi personalizzati per il plug-in e le API, crea ruoli personalizzati e aggiunge un collegamento al plug-in nell'interfaccia utente vSphere.

- "Aggiungi istanze del server vCenter agli strumenti ONTAP"

4 **Configura i backend di storage**

Connetti le risorse di storage ONTAP per consentire agli strumenti ONTAP di eseguire il provisioning e la gestione dei datastore. Aggiungi un backend di storage a un cluster ONTAP. Negli ambienti multitenant in cui un vCenter Server è associato a un tenant SVM, usa ONTAP tools Manager per aggiungere il cluster. Poi associa il backend di storage al vCenter Server per creare una mappatura globale per quella istanza di vCenter.

Aggiungi i backend di storage locali con credenziali del cluster o SVM utilizzando l'interfaccia utente di ONTAP tools. Questi backend di storage sono limitati a un singolo vCenter. Quando usi le credenziali del cluster in locale, gli SVM associati vengono automaticamente mappati al vCenter per gestire vVols o VMFS. Per la gestione di VMFS, incluso SRA, ONTAP tools supporta le credenziali SVM senza la necessità di un cluster globale.

- "Aggiungi un backend di storage"
- "Associa il backend di storage a un'istanza del server vCenter"

## Attività successive facoltative

1 **Configura i ruoli e i privilegi utente ONTAP**

Configura ruoli ONTAP personalizzati per l'accesso con privilegi minimi invece dell'account admin predefinito.

- "Configura i ruoli utente e i privilegi di ONTAP"

2 **Aggiorna i certificati per più istanze di vCenter Server**

Aggiorna i certificati per utilizzare una comunicazione affidabile basata su certificati tra più istanze di vCenter Server.

- "Gestisci i certificati"

3 **Configura la protezione SRA**

Abilita la funzionalità SRA per configurare la protezione di disaster recovery per i datastore NFS e VMFS.

- "Abilita i servizi di ONTAP tools per VMware vSphere"
- "Configura SRA sull'appliance VMware Live Site Recovery"

4 **Abilita la protezione di sincronizzazione attiva SnapMirror**

Configura la protezione del cluster host con SnapMirror active sync per proteggere i datastore VMFS. Nei sistemi ONTAP, esegui il peering del cluster e dell'SVM necessari, quindi configura la protezione del cluster host negli ONTAP tools for VMware vSphere. Questa opzione si applica solo ai datastore VMFS.

- "Proteggi usando la protezione del cluster host"

5 **Configura il backup e il ripristino per la tua distribuzione di ONTAP tools**

Configura backup e ripristino per proteggere la configurazione di ONTAP tools e recuperare rapidamente dai guasti.

Il backup è abilitato per impostazione predefinita in ONTAP tools for VMware vSphere 10.5 e viene eseguito ogni 10 minuti. Pianifica i backup della tua configurazione di ONTAP tools for VMware vSphere che puoi utilizzare per ripristinare la configurazione in caso di errore.

- "Modifica le impostazioni di backup"
- "Ripristina la configurazione degli ONTAP tools"

# Flusso di lavoro di distribuzione ad alta disponibilità per ONTAP tools

Per aumentare la resilienza e supportare un maggior numero di container per servizio, espandi la tua distribuzione iniziale degli ONTAP tools a una configurazione ad alta disponibilità (HA). L'abilitazione del servizio VASA Provider è necessaria per i datastore vVols in una configurazione HA.

1 **Amplia la distribuzione**

Puoi scalare la configurazione degli ONTAP tools for VMware vSphere per aumentare il numero di nodi nella distribuzione e modificare la configurazione in un setup HA.

- "Modifica la configurazione di ONTAP tools for VMware vSphere"

2 **Abilita i servizi**

Per configurare i datastore vVols, è necessario abilitare il servizio VASA Provider. Registra il provider VASA con vCenter e assicurati che le tue policy di archiviazione soddisfino i requisiti di HA, incluse le configurazioni di rete e di archiviazione corrette.

Abilita i servizi SRA per utilizzare ONTAP tools Storage Replication Adapter (SRA) per VMware Site Recovery Manager (SRM) o VMware Live Site Recovery (VLSR).

- "Abilita i servizi VASA Provider e SRA"

3 **Aggiorna i certificati**

Se usi datastore vVol con più istanze di vCenter Server, aggiorna il certificato autofirmato con un certificato firmato da un'autorità di certificazione (CA).

- "Gestisci i certificati"

# Requisiti e limiti di configurazione di ONTAP tools per VMware vSphere

Prima di distribuire gli ONTAP tools for VMware vSphere, dovresti conoscere i requisiti di spazio per il pacchetto di distribuzione e alcuni requisiti di base del sistema host.

È possibile utilizzare ONTAP tools for VMware vSphere con VMware vCenter Server Virtual Appliance (vCSA). È necessario distribuire ONTAP tools for VMware vSphere in un ambiente vSphere supportato che includa host ESXi.

## Requisiti di sistema

- **Requisiti di spazio del pacchetto di installazione per nodo**
  - 15 GB per installazioni thin provisioned
  - 348 GB per installazioni con provisioning completo
- **Requisiti di dimensionamento del sistema host** La tabella seguente mostra la memoria consigliata per ogni dimensione di implementazione. Per le implementazioni ad alta disponibilità (HA), ti serve una quantità di memoria pari al triplo della dimensione dell'appliance indicata.

| Tipo di deployment | CPU per nodo | Memoria (GB) per nodo | Spazio su disco (GB) con provisioning statico per nodo |
|---|---|---|---|
| Piccolo | 9 | 18 | 350 |
| Medio | 13 | 26 | 350 |
| Nota importante: la distribuzione su larga scala è solo per la configurazione HA. | 17 | 34 | 350 |

Quando il backup è abilitato, ogni cluster ONTAP tools necessita di ulteriori 50 GB di spazio sul datastore in cui sono distribuite le VM. Pertanto, la configurazione non HA richiede 400 GB e la configurazione HA richiede 1100 GB di spazio in totale.

## Requisiti minimi di archiviazione e applicazione

| Archiviazione, host e applicazioni | Requisiti di versione |
|---|---|
| ONTAP | 9.15.1, 9.16.1, e 9.17.0 |
| Host ESXi supportati da ONTAP tools | Dalla versione 7.0.3 in poi |
| Strumenti ONTAP supportati vCenter Server | Dalla versione 7.0U3 in poi |
| VASA Provider | 3,0 |
| Applicazione OVA | 10,5 |
| Host ESXi per distribuire la macchina virtuale ONTAP tools | 7.0U3 e 8.0U3 |

| Archiviazione, host e applicazioni | Requisiti di versione |
| --- | --- |
| vCenter Server per distribuire la macchina virtuale di ONTAP tools | 7.0 e 8.0 |

A partire da ONTAP tools for VMware vSphere 10.4, l'hardware della macchina virtuale viene cambiato dalla versione 10 alla 17.

Lo strumento Interoperability Matrix Tool (IMT) contiene le informazioni più recenti sulle versioni supportate di ONTAP, vCenter Server, host ESXi e applicazioni plug-in.

"Strumento Interoperability Matrix Tool"

## Requisiti delle porte

La tabella seguente illustra le porte di rete che NetApp utilizza e i loro scopi. Esistono tre diversi tipi di porte:

- Porte esterne: Queste porte sono accessibili dall'esterno del cluster o del nodo Kubernetes. Consentono ai servizi di comunicare con reti o utenti esterni, permettendo l'integrazione con sistemi esterni all'ambiente del cluster.
- Porte inter-nodo: queste porte consentono la comunicazione tra i nodi all'interno del cluster Kubernetes. Sono necessarie per attività del cluster come la condivisione dei dati e la collaborazione. Per le implementazioni a nodo singolo, le porte inter-nodo vengono utilizzate solo all'interno del nodo e non necessitano di accesso esterno. Le porte inter-nodo possono accettare traffico dall'esterno del cluster. Blocca l'accesso a Internet alle porte inter-nodo tramite regole firewall.
- Porte interne: queste porte comunicano all'interno del cluster Kubernetes utilizzando indirizzi ClusterIP. Non sono esposte esternamente e non è necessario aggiungerle alle regole del firewall.

Assicurati che tutti i nodi di ONTAP tools risiedano sulla stessa sottorete per mantenere una comunicazione ininterrotta tra loro.

Fai clic per espandere o comprimere la tabella dei requisiti della porta.

| Nome servizio/componente | Porta | Protocollo | Tipo di porta | Descrizione |
|---|---|---|---|---|
| ntv-gateway-svc (LB) | 443, 8443 | TCP | Esterno | Porta di transito per le comunicazioni in entrata relative al servizio VASA Provider. Il certificato autofirmato del VASA Provider e il certificato CA personalizzato sono ospitati su questa porta. |
| SSH | 22 | TCP | Esterno | Secure Shell per l'accesso al server remoto e l'esecuzione di comandi. |
| server rke2 | 9345 | TCP | Inter-nodo | API di supervisione RKE2 (Limita alle reti attendibili). |
| kube-apiserver | 6443 | TCP | Inter-nodo | Porta del server API di Kubernetes (limita alle reti attendibili). |
| rpcbind/portmapper | 111 | TCP/UDP | Inter-nodo | Utilizzato per la comunicazione RPC tra i servizi. |
| coredns (DNS) | 53 | TCP/UDP | Inter-nodo | Servizio DNS (Domain Name System) per la risoluzione dei nomi all'interno del cluster. |
| NTP | 123 | UDP | Inter-nodo | Network Time Protocol (NTP) per la sincronizzazione dell'ora. |
| etcd | 2379, 2380, 2381 | TCP | Inter-nodo | Archivio chiave-valore per i dati del cluster. |
| kube-vip | 2112 | TCP | Inter-nodo | Porta del server API di Kubernetes. |
| kubelet | 10248, 10250 | TCP | Inter-nodo | Componente Kubernetes |

| Nome servizio/componente | Porta | Protocollo | Tipo di porta | Descrizione |
|---|---|---|---|---|
| kube-controller | 10257 | TCP | Inter-nodo | Componente Kubernetes |
| cloud-controller | 10258 | TCP | Inter-nodo | Componente Kubernetes |
| kube-scheduler | 10259 | TCP | Inter-nodo | Componente Kubernetes |
| kube-proxy | 10249, 10256 | TCP | Inter-nodo | Componente Kubernetes |
| calico-node | 9091, 9099 | TCP | Inter-nodo | Componente di rete Calico. |
| containerd | 10010 | TCP | Inter-nodo | Servizio demone del container. |
| VXLAN (Flannel) | 8472 | UDP | Inter-nodo | Rete overlay per la comunicazione tra i pod. |

Per le implementazioni HA, assicurati che la porta UDP 8472 sia aperta tra tutti i nodi. Questa porta consente la comunicazione tra i pod dei nodi; se la blocchi, interromperai la comunicazione di rete tra i nodi.

## Limiti di configurazione per distribuire ONTAP tools for VMware vSphere per vVols datastores

È possibile utilizzare la seguente tabella come guida per la configurazione di ONTAP tools for VMware vSphere.

| Deployment | Tipo | Numero di vVols | Numero di host |
|---|---|---|---|
| Non-HA | Piccolo (S) | fino a 12K | 32 |
| Non-HA | Medio (M) | fino a 24K | 64 |
| Alta disponibilità | Piccolo (S) | fino a 24K | 64 |
| Alta disponibilità | Medio (M) | fino a 50k | 128 |
| Alta disponibilità | Grande (L) | fino a 100k | 256 |

I conteggi degli host nella tabella rappresentano il totale combinato tra tutti i vCenters connessi.

## Limiti di configurazione per distribuire ONTAP tools for VMware vSphere per datastore VMFS e NFS

I limiti di configurazione elencati in questa sezione sono convalidati e supportati da NetApp. I limiti effettivi possono variare a seconda dell'ambiente e del carico di lavoro. Il superamento di questi limiti può influire sulle prestazioni o sul supporto e non è consigliato. Considerare quanto segue quando si esamina la tabella:

- Il Disaster Recovery (DR) delle macchine virtuali è configurato utilizzando criteri sincroni, asincroni o di sincronizzazione rigorosa. Il DR non è supportato per il protocollo NVMe.
- La protezione del cluster host ESXi utilizza SnapMirror Active Sync, che non supporta distribuzioni multi-vCenter.
- ONTAP tools limita solo il numero di host ESXi e datastore in base alle dimensioni dell'implementazione. Non ci sono restrizioni sul numero di vCenter Server che possono essere connessi a ONTAP tools.
- ONTAP tools esegue il discovery parallelo di tutti gli oggetti di storage. I limiti di configurazione per gli oggetti di storage ONTAP si applicano indipendentemente dal numero di oggetti attivamente in uso.
- ONTAP tools non impone un limite al numero di vCenter Servers che possono essere integrati. I limiti di configurazione sono determinati dal numero di host e datastore supportati, come dettagliato nella tabella seguente.

| Distribuzione | Numero di datastore VMFS e NFS | Numero di datastore VMFS con DR abilitato | Numero di host |
|---|---|---|---|
| Non-HA Piccolo | 200 | 80 | 32 |
| Non-HA medio | 250 | 100 | 32 |
| HA Small | 350 | 200 | 64 |
| HA Medium | 600 | 200 | 128 |
| HA Large | 1024 | 250 | 256 |

## ONTAP tools for VMware vSphere - Storage Replication Adapter (SRA)

La tabella seguente mostra i numeri supportati per ogni istanza di VMware Live Site Recovery utilizzando ONTAP tools for VMware vSphere.

| Dimensioni del deployment vCenter | Piccolo | Medio |
|---|---|---|
| Numero totale di macchine virtuali configurate per la protezione tramite replica basata su array | 2000 | 5000 |
| Numero totale di gruppi di protezione basati su array per la replica | 250 | 250 |
| Numero totale di gruppi di protezione per piano di recovery | 50 | 50 |
| Numero di datastore replicati | 255 | 255 |
| Numero di VM | 4000 | 7000 |

La tabella seguente mostra il numero di istanze di VMware Live Site Recovery e la corrispondente dimensione di implementazione di ONTAP tools for VMware vSphere.

| Numero di istanze di VMware Live Site Recovery | Dimensioni di deployment degli ONTAP tools |
|---|---|
| Fino a 4 | Piccolo |
| da 4 a 8 | Medio |

| | |
|---|---|
| Più di 8 | Grande |

Per ulteriori informazioni, consulta "Limiti operativi di VMware Live Site Recovery".

# Requisiti di pre-distribuzione per ONTAP tools

Assicurati che i seguenti requisiti siano soddisfatti prima di procedere con l'implementazione:

| Requisiti | Il tuo stato |
|---|---|
| vSphere versione, versione di ONTAP e versione dell'host ESXi sono compatibili con la versione degli strumenti ONTAP. | □ Sì □ No |
| vCenter Server environment è stato impostato e configurato | □ Sì □ No |
| La cache del browser è stata eliminata | □ Sì □ No |
| Hai le credenziali del server vCenter principale | □ Sì □ No |
| Hai le credenziali di accesso per l'istanza del server vCenter, a cui gli ONTAP tools for VMware vSphere si connetteranno dopo la distribuzione per la registrazione | □ Sì □ No |
| Il nome di dominio su cui viene emesso il certificato è mappato all'indirizzo IP virtuale in una distribuzione multi-vCenter in cui i certificati CA personalizzati sono obbligatori. | □ Sì □ No |
| Hai eseguito il controllo nslookup sul domain name per verificare se il dominio viene risolto all'indirizzo IP previsto. | □ Sì □ No |
| Il certificato viene creato con il domain name e l'indirizzo IP degli ONTAP tools. | □ Sì □ No |
| L'applicazione ONTAP tools e i servizi interni sono raggiungibili dal vCenter Server. | □ Sì □ No |
| Quando usi SVM multi-tenant, hai un LIF di gestione SVM su ciascuna SVM. | □ Sì □ No |

## Foglio di lavoro per l'implementazione

### Per la distribuzione a nodo singolo

Utilizza il seguente foglio di lavoro per raccogliere le informazioni necessarie per la distribuzione iniziale di ONTAP tools for VMware vSphere:

| Requisito | Il tuo valore |
|---|---|
| Indirizzo IP per l'applicazione ONTAP tools. Questo è l'indirizzo IP per accedere all'interfaccia web del gestore ONTAP tools (load balancer) a `https://<ip>:8443/virtualization/ui/` | |
| Indirizzo IP virtuale di ONTAP tools per la comunicazione interna. Questo indirizzo IP viene utilizzato per la comunicazione interna in una configurazione con più istanze di ONTAP tools. Questo indirizzo IP non deve essere uguale all'indirizzo IP per l'applicazione ONTAP tools. (Il Kubernetes Control Plane) | |
| Nome host DNS per il nodo di gestione degli ONTAP tools | |
| DNS server primario | |
| DNS server secondario | |
| dominio di ricerca DNS | |
| Indirizzo IPv4 per il nodo di gestione degli ONTAP tools. Si tratta di un indirizzo IPv4 univoco per l'interfaccia di gestione del nodo sulla rete di gestione. Questo viene utilizzato per connettersi all'appliance degli strumenti ONTAP per l'accesso diagnostico remoto tramite SSH. | |
| Maschera di sottorete per l'indirizzo IPv4 | |
| Gateway predefinito per l'indirizzo IPv4 | |
| Indirizzo IPv6 (facoltativo) | |
| Lunghezza prefisso IPv6 (opzionale) | |
| Gateway per l'indirizzo IPv6 (opzionale) | |

Crea record DNS per tutti gli indirizzi IP sopra indicati. Prima di assegnare i nomi host, mappali agli indirizzi IP liberi nel DNS. Tutti gli indirizzi IP devono trovarsi sulla stessa VLAN selezionata per la distribuzione.

**Per la distribuzione ad alta disponibilità (HA)**

Oltre ai requisiti per la distribuzione a nodo singolo, ti serviranno le seguenti informazioni per la distribuzione ad alta disponibilità (HA):

| Requisito | Il tuo valore |
|---|---|
| DNS server primario | |
| DNS server secondario | |
| dominio di ricerca DNS | |
| Nome host DNS per il secondo nodo | |

| | |
|---|---|
| Indirizzo IP del secondo nodo | |
| Nome host DNS per il terzo nodo | |
| Indirizzo IP per il terzo nodo | |

### Configurazione del firewall di rete

Assicurati che le porte del firewall necessarie siano aperte per tutti gli indirizzi IP rilevanti. ONTAP tools richiede l'accesso al LIF tramite la porta 443. Per un elenco completo delle porte richieste, consulta la sezione relativa ai requisiti delle porte su "Requisiti e limiti di configurazione di ONTAP tools per VMware vSphere".

### Impostazioni di storage ONTAP

Per garantire una perfetta integrazione dello storage ONTAP con ONTAP tools for VMware vSphere, considera le seguenti impostazioni:

- Se usi Fibre Channel (FC) per la connettività di archiviazione, configura lo zoning sugli switch FC per connettere gli host ESXi con le LIF FC dell'SVM. "Scopri la zonizzazione FC e FCoE con i sistemi ONTAP"
- Per utilizzare la replica SnapMirror gestita dagli strumenti ONTAP, l'amministratore dello storage ONTAP deve creare "Relazioni tra cluster peer ONTAP" e "Relazioni peer SVM intercluster ONTAP" in ONTAP prima di utilizzare SnapMirror.

# Distribuisci ONTAP tools

L'appliance ONTAP tools for VMware vSphere viene distribuita come un singolo nodo di piccole dimensioni con servizi di base per supportare i datastore NFS e VMFS. Il processo di distribuzione di ONTAP tools potrebbe richiedere fino a 45 minuti.

**Prima di iniziare**

Se stai implementando un singolo nodo di piccole dimensioni, un archivio di contenuti è facoltativo. Per le implementazioni multi-nodo o HA, un archivio di contenuti è obbligatorio. In VMware, un archivio di contenuti memorizza modelli di macchine virtuali, vApp template e altri file. Implementare con un archivio di contenuti offre un'esperienza senza interruzioni perché non dipende dalla connettività di rete.

Considera quanto segue prima di creare un archivio di contenuti:

- Crea l'archivio di contenuti su un archivio dati condiviso in modo che tutti gli host del cluster possano accedervi.
- Configura l'archivio di contenuti prima di distribuire ONTAP tools for VMware vSphere OVA.
- Assicurati che l'archivio di contenuti sia stato creato prima di configurare l'appliance per l'HA.

Non eliminare il modello OVA dall'archivio di contenuti dopo la distribuzione.

Per consentire la distribuzione ad alta disponibilità in futuro, evitare di distribuire la macchina virtuale ONTAP tools direttamente su un host ESXi. Distribuirla invece all'interno di un cluster ESXi host o pool di risorse.

Segui questi passaggi per creare un archivio di contenuti:

1. Scarica il file che contiene i binari (*.ova*) e i certificati firmati per ONTAP tools for VMware vSphere dal "Sito di supporto NetApp".
2. Accedi al vSphere client
3. Seleziona il menu client vSphere e seleziona **archivio di contenuti**.
4. Seleziona **Crea** sulla destra della pagina.
5. Assegna un nome alla libreria e crea l'archivio di contenuti.
6. Accedi all'archivio di contenuti che hai creato.
7. Seleziona **Azioni** sulla destra della pagina, seleziona **Importa elemento** e importa il file OVA.

Per ulteriori informazioni, consultare "Creazione e utilizzo dell'archivio di contenuti" blog.

Prima di procedere con la distribuzione, impostare il Distributed Resource Scheduler (DRS) del cluster su Conservative. Ciò garantisce che le VM non vengano migrate durante l'installazione.

Gli ONTAP tools for VMware vSphere vengono inizialmente distribuiti come configurazione non HA. Per passare a una distribuzione HA, è necessario abilitare la funzionalità di CPU hot-add e memory hot-plug. È possibile eseguire questo passaggio durante il processo di distribuzione oppure modificare le impostazioni della macchina virtuale dopo la distribuzione.

**Passaggi**

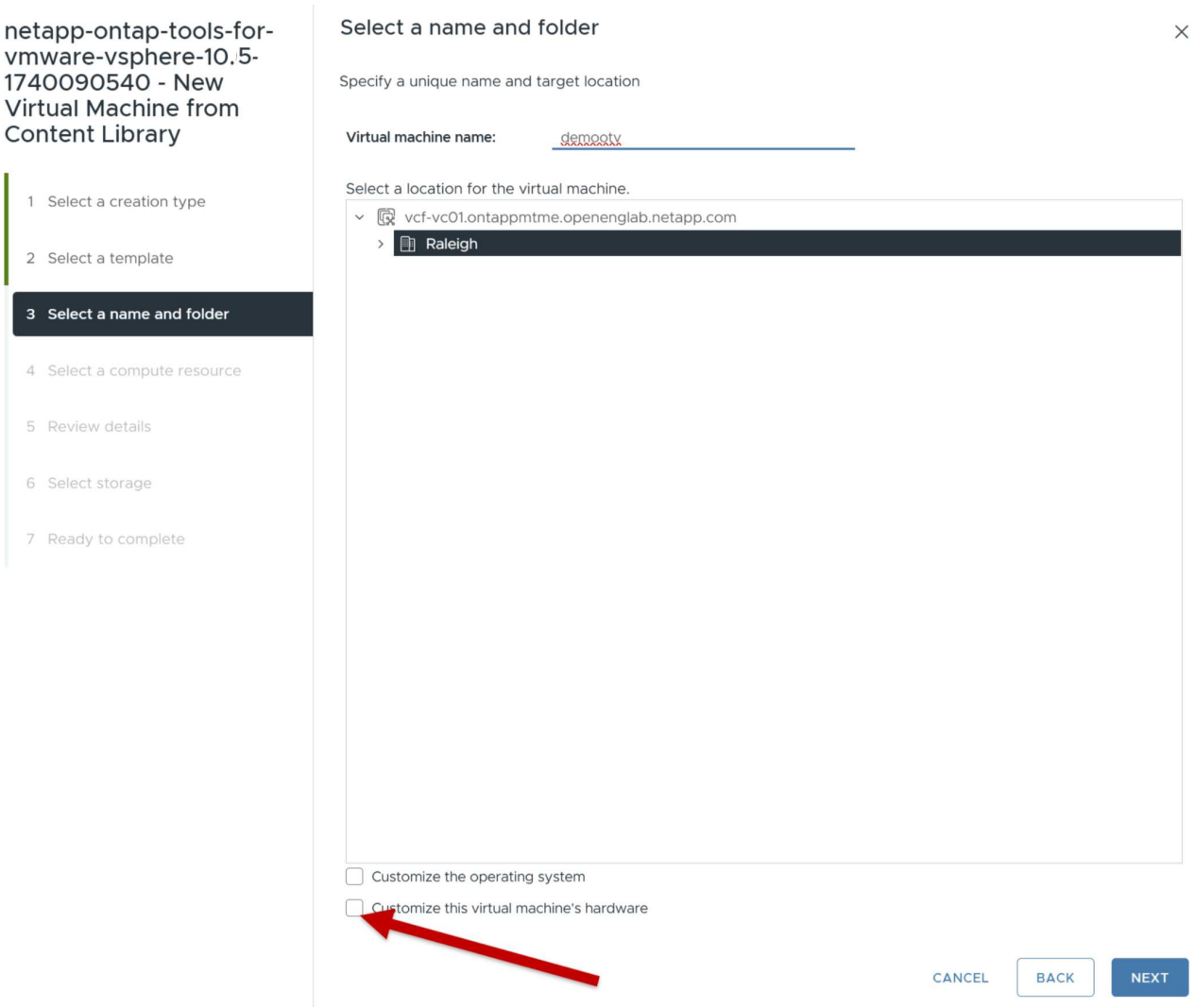
1. Scarica il file che contiene i file binari (*.ova*) e i certificati firmati per gli ONTAP tools for VMware vSphere dal "Sito di supporto NetApp". Se hai importato l'OVA nell'archivio di contenuti, puoi saltare questo passaggio e procedere con il prossimo.
2. Accedi al vSphere server.
3. Vai al pool di risorse, cluster o host dove vuoi distribuire l'OVA.

Non memorizzare mai la macchina virtuale ONTAP tools for VMware vSphere su datastore vVols che essa gestisce.

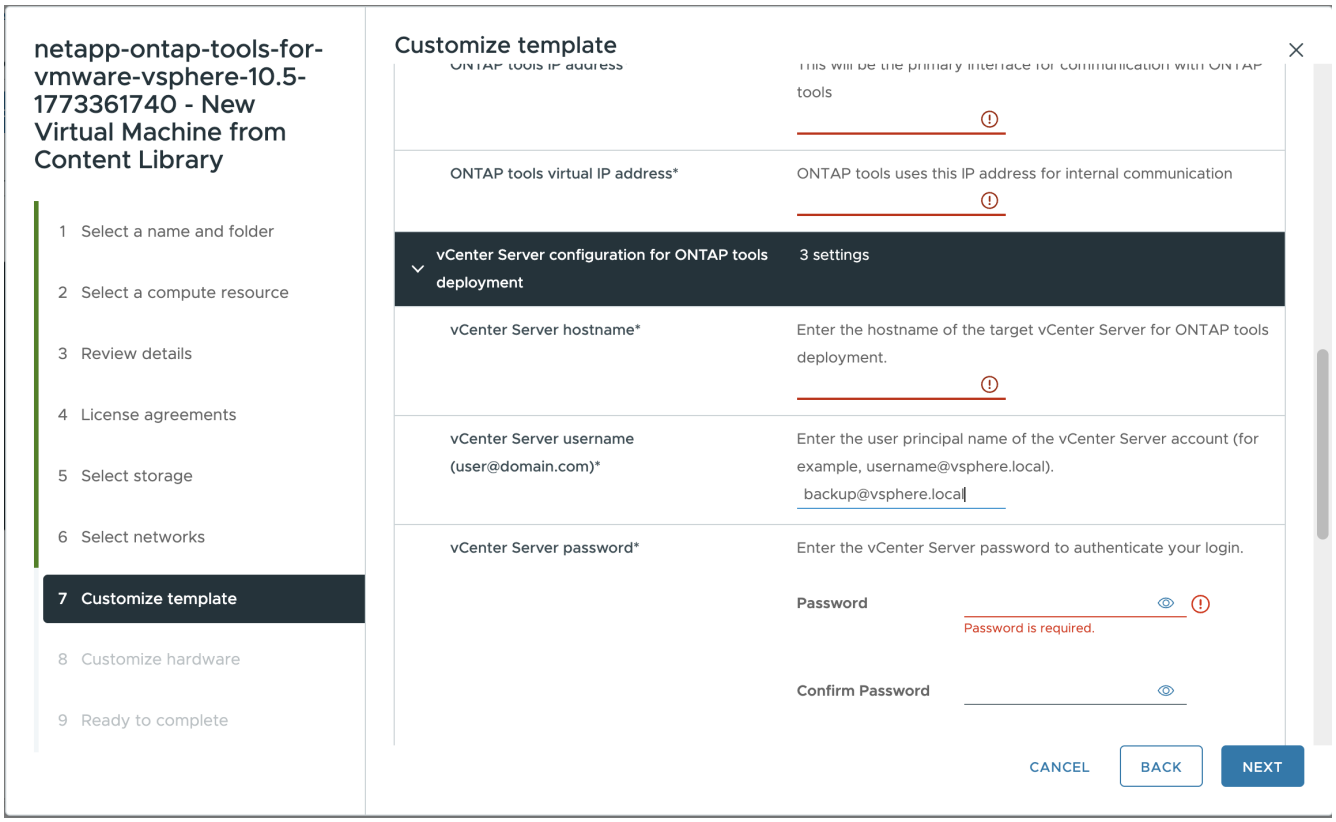
4. Puoi distribuire il file OVA dall'archivio di contenuti o dal sistema locale.

| Dal sistema locale | Dall'archivio di contenuti |
|---|---|
| a. Fai clic con il pulsante destro del mouse e seleziona **Deploy OVF template…**. b. Scegli il file OVA dall'URL o individua la sua posizione, quindi seleziona **Next**. | a. Vai al tuo archivio di contenuti e seleziona l'elemento della libreria che desideri distribuire. b. Seleziona **Azioni** > **Nuova VM da questo modello** |

5. Nel campo **Seleziona un nome e una cartella**, inserisci il nome della macchina virtuale e scegli la sua posizione.
   - Se si utilizza la versione vCenter Server 8.0.3, selezionare l'opzione **Personalizza l'hardware di questa macchina virtuale**, che attiverà un passaggio aggiuntivo denominato **Personalizza l'hardware** prima di procedere alla finestra **Pronto per completare**.
   - Se si utilizza la versione vCenter Server 7.0.3, seguire i passaggi descritti nella sezione **Cosa fare dopo?** al termine della distribuzione.




6. Seleziona una risorsa computer e fai clic su **Avanti**. Facoltativamente, seleziona la casella per **Accendere automaticamente la VM distribuita**.
7. Esamina i dettagli del modello e seleziona **Avanti**.
8. Leggi e accetta il contratto di licenza e seleziona **Avanti**.
9. Seleziona lo storage per la configurazione e il formato del disco, quindi fai clic su **Avanti**.
10. Seleziona la rete di destinazione per ciascuna rete di origine e seleziona **Avanti**.
11. Nella finestra **Personalizza modello**, compila i campi obbligatori.




I valori presenti nella pagina **Personalizza modello** sono necessari per una distribuzione riuscita.

Presta particolare attenzione a questi campi:

- **Nome host**: Inserisci l'host name della VM ONTAP tools. Usa un formato di host name valido.
- **Indirizzo IP degli ONTAP tools**: Questa è l'interfaccia di gestione principale utilizzata per accedere agli ONTAP tools.
- **Indirizzo IPv4**: Questo è l'indirizzo IP del nodo utilizzato per la shell diagnostica e l'accesso SSH per la risoluzione dei problemi e la manutenzione.

Se usi nomi DNS per l'host o vCenter, assicurati che quei nomi vengano risolti correttamente nel DNS.

Il nome host vCenter è il nome dell'istanza del server vCenter in cui è distribuita l'appliance ONTAP tools.

Se si distribuiscono gli strumenti ONTAP in una topologia a due vCenter Server, in cui l'appliance è ospitata in un'istanza vCenter e ne gestisce un'altra, è possibile assegnare un ruolo con restrizioni per l'istanza vCenter che ospita gli strumenti ONTAP. È possibile creare un utente e un ruolo vCenter dedicati con solo le autorizzazioni necessarie per la distribuzione del modello OVF. Per dettagli, consultare i ruoli elencati in "Ruoli inclusi con ONTAP tools for VMware vSphere 10".

Per l'istanza vCenter che verrà gestita da ONTAP tools, assicurati che l'account utente vCenter abbia i privilegi di amministratore.

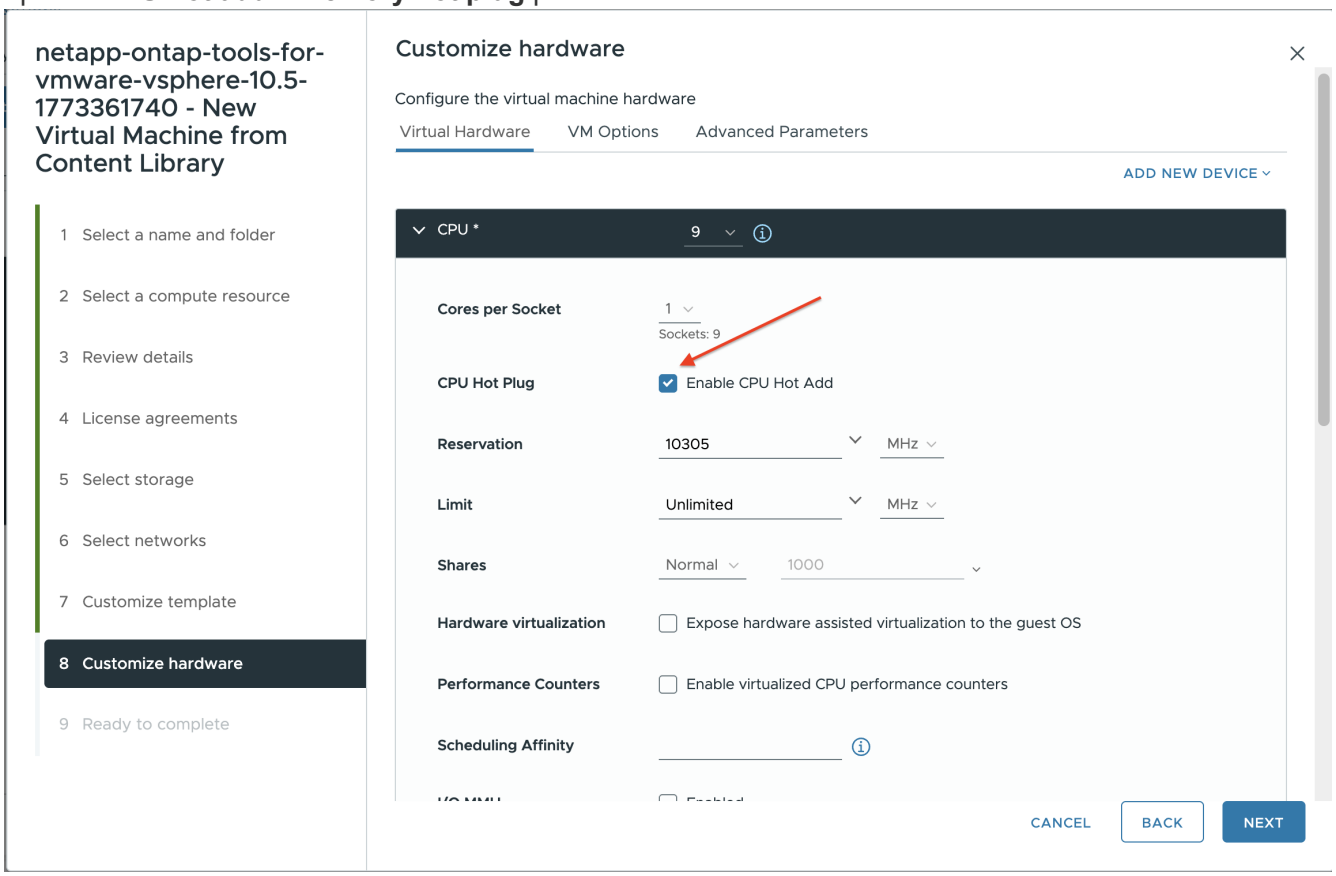
- I nomi host devono includere lettere (A-Z, a-z), cifre (0-9) e trattini (-). Per configurare il dual stack,

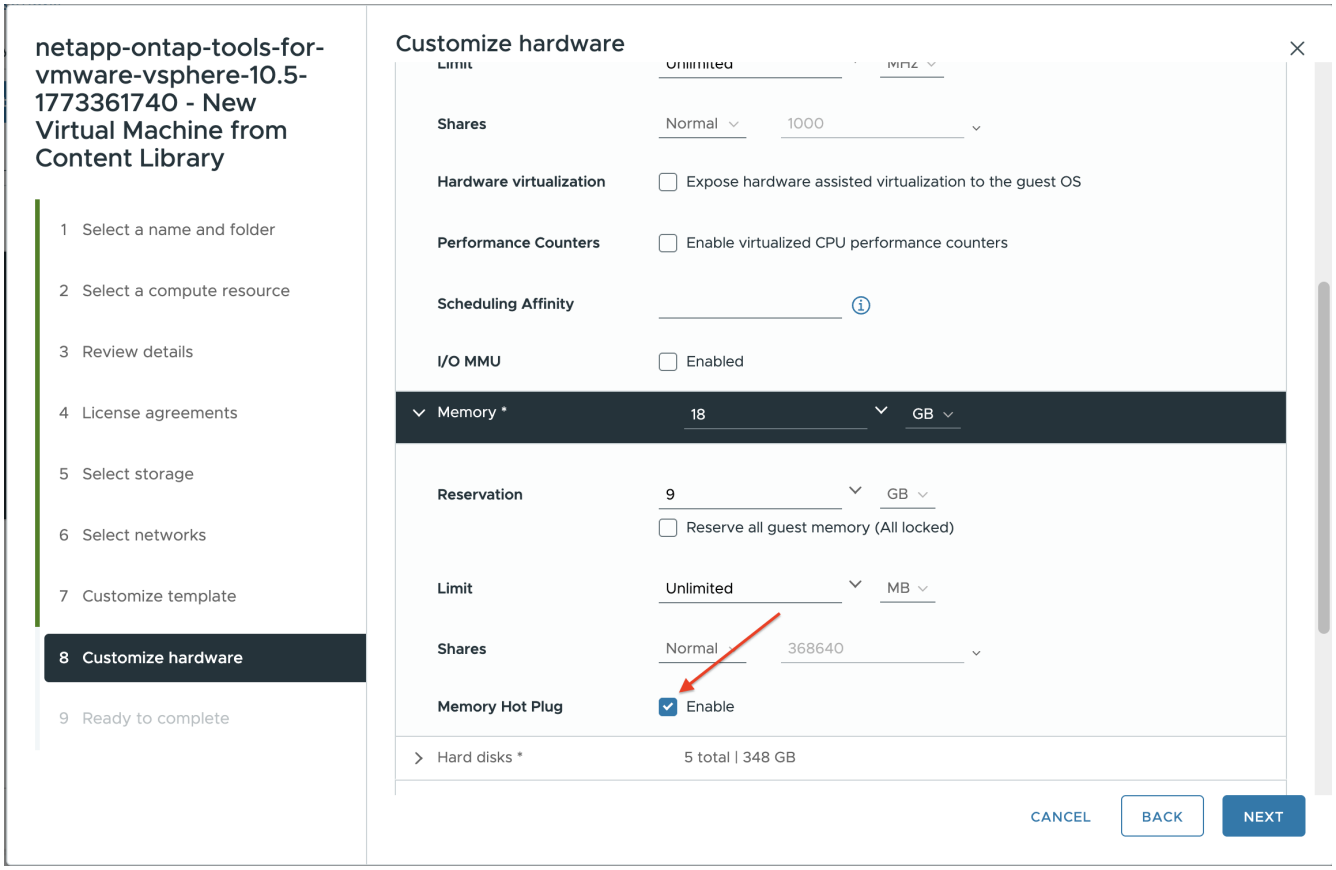
specifica l'host name mappato all'indirizzo IPv6.

> IPv6 puro non è supportato. La modalità mista è supportata con VLAN che contengono sia indirizzi IPv6 che IPv4.

- L'indirizzo IP di ONTAP tools è l'interfaccia principale per comunicare con ONTAP tools.
- IPv4 è la componente dell'indirizzo IP nella configurazione del nodo, che puoi utilizzare per abilitare la shell diagnostica e l'accesso SSH al nodo per il debug e la manutenzione.

12. Quando si utilizza la versione vCenter Server 8.0.3, nella finestra **Personalizza hardware**, abilitare le opzioni **CPU hot add** e **Memory hot plug** per consentire la funzionalità HA.






13. Rivedi i dettagli nella finestra **Pronto per completare**, seleziona **Fine**.

    Man mano che viene creata l'attività di distribuzione, l'avanzamento viene visualizzato nella barra delle attività di vSphere.

14. Accendi la VM al termine dell'attività se non hai selezionato l'opzione per accenderla automaticamente.

Puoi monitorare l'avanzamento dell'installazione all'interno della console web della macchina virtuale.

Se nel modulo OVF sono presenti delle discrepanze, viene visualizzata una finestra di dialogo che ti chiede di correggere. Usa il tasto Tab per navigare, apporta le modifiche necessarie e seleziona **OK**. Hai tre tentativi per risolvere eventuali problemi. Se i problemi continuano dopo tre tentativi, il processo di installazione si interrompe e ti consigliamo di riprovare l'installazione su una nuova macchina virtuale.

**E adesso?**

Se hai distribuito ONTAP tools for VMware vSphere con vCenter Server 7.0.3, segui questi passaggi dopo la distribuzione.

1. Accedi al vCenter client
2. Spegni il nodo ONTAP tools.
3. Vai alla macchina virtuale ONTAP tools for VMware vSphere sotto **Inventari** e seleziona l'opzione **Modifica impostazioni**.
4. Nelle opzioni **CPU**, seleziona la casella **Abilita aggiunta a caldo della CPU**
5. Nella sezione **Memoria**, seleziona la casella **Abilita** accanto a **Memory hot plug**.

# Risolvi gli errori di distribuzione degli ONTAP tools

Se riscontri problemi di distribuzione, controlla i log e i codici di errore per diagnosticare e risolvere i problemi. A partire da ONTAP tools for VMware vSphere 10.5, i pacchetti di log raccolti dai pod includono i log di MongoDB, RabbitMQ e Vault, insieme allo stato e alle descrizioni di tutti i pod. Questi vengono forniti in aggiunta ai log di servizio ONTAP tools for VMware vSphere esistenti, migliorando la supportabilità e la risoluzione dei problemi.

## Raccogli i file di log

È possibile raccogliere i file di registro per ONTAP tools for VMware vSphere dalle opzioni disponibili nell'interfaccia utente di ONTAP tools Manager. Il supporto tecnico potrebbe chiedere di raccogliere i file di registro per aiutare a risolvere un problema.

> La generazione dei log da ONTAP tools Manager include tutti i log per tutte le istanze del server vCenter. La generazione dei log dall'interfaccia utente client vCenter è limitata al server vCenter selezionato.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona **Log Bundles** dalla barra laterale.

   Questa operazione può richiedere diversi minuti.
4. Seleziona **Genera** per generare i file di log.
5. Inserisci l'etichetta per il pacchetto di log e seleziona **Genera**.

   Scarica il file tar.gz e invialo al supporto tecnico.

Segui i passaggi seguenti per generare il pacchetto di log utilizzando l'interfaccia utente del client vCenter:

**Passaggi**

1. Accedi al vSphere client.
2. Dalla home page del client vSphere, vai su **Supporto** > **Log bundle** > **Genera**.
3. Fornisci l'etichetta del pacchetto di log e genera il pacchetto di log. Puoi vedere l'opzione di download quando i file sono stati generati. Il download potrebbe richiedere un po' di tempo.

> Il pacchetto di log generato sostituisce il pacchetto di log generato negli ultimi 3 giorni o 72 ore.

## Codici di errore di distribuzione

Potresti incontrare codici di errore durante la distribuzione, il riavvio e le operazioni di ripristino degli ONTAP tools for VMware vSphere. I codici di errore sono composti da cinque cifre: le prime due rappresentano lo script che ha riscontrato il problema e le ultime tre rappresentano il flusso di lavoro specifico all'interno di quello script.

Tutti i log degli errori vengono registrati nel file ansible-perl-errors.log nella directory /var/log per facilitare l'individuazione e la risoluzione dei problemi. Questo file di log contiene il codice di errore e l'attività Ansible non riuscita.

I codici di errore riportati in questa pagina sono solo a scopo di riferimento. Contatta il team di supporto se l'errore persiste o se non viene indicata alcuna soluzione.

La tabella seguente elenca i codici di errore e i corrispondenti nomi dei file.

| Codice di errore | Nome script |
|---|---|
| 00 | firstboot-network-config.pl, modalità deploy |
| 01 | firstboot-network-config.pl, modalità upgrade |
| 02 | firstboot-inputs-validation.pl |
| 03 | firstboot-deploy-otv-ng.pl, deploy, HA |
| 04 | firstboot-deploy-otv-ng.pl, deploy, non-HA |
| 05 | firstboot-deploy-otv-ng.pl, reboot |
| 06 | firstboot-deploy-otv-ng.pl, aggiornamento, HA |
| 07 | firstboot-deploy-otv-ng.pl, aggiornamento, non-HA |
| 08 | firstboot-otv-recovery.pl |
| 09 | post-deploy-upgrade.pl |

Le ultime tre cifre del codice di errore indicano lo specifico errore del flusso di lavoro all'interno dello script:

| Codice errore di deployment | Flusso di lavoro | Risoluzione |
|---|---|---|
| 049 | Per la rete e la convalida, lo script perl li assegnerà a breve | - |
| 050 | Generazione della chiave SSH non riuscita | Riavvia la macchina virtuale (VM) primaria. |
| 053 | Installazione di RKE2 non riuscita | Esegui i seguenti comandi e riavvia la VM principale oppure ridistribuisci: sudo rke2-killall.sh (su tutte le VM) sudo rke2-uninstall.sh (su tutte le VM). |
| 054 | Impostazione di kubeconfig non riuscita | Ridistribuisci |
| 055 | Impossibile distribuire il registry | Se il pod del registry è presente, attendi che il pod sia pronto e quindi riavvia la VM primaria oppure esegui una nuova distribuzione. |

| | | |
|---|---|---|
| 059 | KubeVip implementazione non riuscita | Assicurarsi che l'indirizzo IP virtuale per il piano di controllo di Kubernetes e l'indirizzo IP degli ONTAP tools forniti durante la distribuzione appartengano alla stessa VLAN e siano indirizzi IP liberi. Riavviare se tutti i punti precedenti sono corretti. Altrimenti, ridistribuire. |
| 060 | L'implementazione dell'operatore non è riuscita | Riavvia |
| 061 | L'implementazione dei servizi non è riuscita | Esegui il debug di base di Kubernetes, come get pods, get rs, get svc e così via, nel namespace ntv-system per maggiori dettagli e log degli errori su /var/log/ansible-perl-errors.log e /var/log/ansible-run.log e poi ridistribuisci. |
| 062 | La distribuzione dei servizi ONTAP tools non è riuscita | Consulta i log degli errori in /var/log/ansible-perl-errors.log per ulteriori dettagli e ridistribuisci. |
| 065 | L'URL della pagina Swagger non è raggiungibile | Ridistribuisci |
| 066 | I passaggi post-distribuzione per il certificato gateway non sono riusciti | Per ripristinare/completare l'upgrade, procedi come segue:<br>• Abilita la shell diagnostica.<br>• Eseguire il comando 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'.<br>• Controlla i log in /var/log/post-deploy-upgrade.log. |
| 088 | Configurare la rotazione dei log per journald non è riuscito | Verifica che le impostazioni di rete della macchina virtuale siano compatibili con l'host su cui è ospitata. Puoi provare a migrare su un altro host e riavviare la macchina virtuale. |
| 089 | Modificare la proprietà del file di configurazione della rotazione del registro di riepilogo non è riuscito | Riavvia la macchina virtuale principale. |
| 096 | Installa il provisioner di archiviazione dinamica | - |
| 108 | Script di seeding non riuscito | - |

| | | |
|---|---|---|
| 114 | Aggiornamento interno del certificato nella collezione MongoDB non riuscito | Se la distribuzione non riesce con il codice di errore 114, completare i seguenti passaggi:<br>• Abilita la shell diagnostica.<br>• Eseguire il seguente comando: `sudo perl /home/maint/scripts/post-deploy-upgrade.pl --internal_cert_update_collection`<br>• Esamina i registri a `/var/log/otvng/post-deploy-upgrade.log` |

| Codice di errore di riavvio | Flusso di lavoro | Risoluzione |
|---|---|---|
| 067 | Attesa per rke2-server scaduta. | - |
| 101 | Impossibile reimpostare la password dell'utente manutenzione/console. | - |
| 102 | Impossibile eliminare il file delle password durante il reset della password utente Maint/Console. | - |
| 103 | Impossibile aggiornare la password del nuovo utente Maint/Console nel vault. | - |
| 088 | La configurazione della rotazione dei log per journald non è riuscita. | Verifica che le impostazioni di rete della macchina virtuale siano compatibili con l'host su cui è ospitata. Puoi provare a migrare su un altro host e riavviare la macchina virtuale. |
| 089 | La modifica della proprietà del file di configurazione di rotazione del log di riepilogo non è riuscita. | Riavvia la macchina virtuale. |

# Configura ONTAP tools for VMware vSphere

## Aggiungi istanze del server vCenter agli strumenti ONTAP

Aggiungi istanze vCenter Server a ONTAP tools for VMware vSphere per configurare, gestire e proteggere i tuoi datastore virtuali nell'ambiente vCenter Server. Quando aggiungi più istanze vCenter Server, sono necessari certificati CA personalizzati per una comunicazione sicura tra ONTAP tools e ciascuna istanza vCenter Server.

**Informazioni su questa attività**

ONTAP tools si integra con vCenter Server per eseguire attività di storage come provisioning, Snapshot e protezione dei dati direttamente dal client vSphere.

L'aggiunta di un'istanza del server vCenter agli ONTAP tools attiva automaticamente le seguenti azioni:

- ONTAP tools registra il plug-in client vCenter come plug-in remoto.
- I privilegi personalizzati per i plug-in e le API vengono applicati all'istanza del server vCenter.
- I ruoli personalizzati vengono creati per gestire gli utenti.
- Il plug-in appare come un collegamento rapido sull'interfaccia utente di vSphere.

**Prima di iniziare**

- Assicurarsi che il certificato del server vCenter includa un'estensione SAN (Subject Alternative Name) valida con voci sia DNS che indirizzo IP. Per esempio:

```
X509v3 extensions:
    X509v3 Subject Alternative Name:
        DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
```

  Se il certificato non include un'estensione SAN, o se l'estensione SAN non contiene i valori DNS o di indirizzo IP corretti, le operazioni di ONTAP tools potrebbero non riuscire a causa di errori di convalida del certificato.

- L'identificatore di rete primario (PNID) del vCenter Server deve essere incluso nei dettagli SAN. Il PNID e il nome DNS devono essere identici e risolvibili nel DNS.
- Si raccomanda di distribuire vCenter Server utilizzando il suo fully qualified domain name (FQDN), assicurandosi che il SAN nel certificato includa DNS Name=machine_FQDN per una compatibilità e un supporto ottimali.
- Per ulteriori informazioni, fare riferimento alla documentazione VMware:
  - "vSphere Certificate Requirements per diversi percorsi di soluzione"
  - "Sostituisci il certificato SSL della macchina vCenter con un certificato firmato da un'autorità di certificazione personalizzata"
  - "Errore: il campo Subject Alternate Name (SAN) non contiene il PNID. Fornire un certificato valido"

Se l'FQDN non è disponibile, puoi impostare il PNID sull'indirizzo IP e includere l'indirizzo IP nella SAN. Tuttavia, questo non è raccomandato da VMware.

**Passaggi**

1. Apri un browser web e vai all'URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona **vCenters** > **Aggiungi** per eseguire l'onboarding delle istanze del server vCenter. Fornisci l'indirizzo IP o il nome host vCenter, il nome utente, la password e i dettagli della porta.
4. Nelle opzioni avanzate, recupera automaticamente il certificato del server vCenter (autorizzalo) oppure caricalo manualmente.

> Non ti serve un account admin per aggiungere istanze vCenter agli ONTAP tools. Puoi creare un ruolo personalizzato senza l'account admin, con permessi limitati. Consulta "Usa vCenter Server RBAC con ONTAP tools for VMware vSphere 10" per i dettagli.

# Registrare il provider VASA con un'istanza del server vCenter negli ONTAP tools

Usa ONTAP tools for VMware vSphere per registrare il VASA Provider con un'istanza del vCenter Server. Questo abilita la gestione basata su policy dello storage, il supporto vVols e l'integrazione con gli appliance VMware Live Site Recovery sui sistemi ONTAP.

Le impostazioni del provider VASA mostrano lo stato di registrazione per il vCenter Server selezionato.

**Passaggi**

1. Accedi al vSphere client.
2. Seleziona **Collegamenti** > **NetApp ONTAP tools** nella sezione dei plug-in.
3. Seleziona **Impostazioni** > **Impostazioni del provider VASA**. Gli ONTAP tools visualizzano lo stato di registrazione del VASA Provider come non registrato.
4. Seleziona il pulsante **Registra** per registrare il VASA Provider.
5. Inserisci un nome e le credenziali per il VASA Provider. Il nome utente può contenere solo lettere, numeri e trattini bassi. La password deve essere compresa tra 8 e 256 caratteri.
6. Seleziona **Register**.
7. Dopo una registrazione e un aggiornamento della pagina andati a buon fine, ONTAP tools visualizza lo stato, il nome e la versione del VASA Provider registrato.

**Cosa c'è dopo**

Verifica che il VASA Provider integrato sia elencato sotto VASA Provider dal client vCenter:

**Passaggi**

1. Vai all'istanza del server vCenter.
2. Accedi con le credenziali dell'amministratore.
3. Seleziona **Storage Providers** > **Configure**. Verifica che il VASA Provider onboarded sia elencato correttamente.

# Installa il plug-in NFS VAAI usando ONTAP tools

Il plug-in NFS vStorage API for Array Integration (NFS VAAI) collega VMware vSphere agli array di storage NFS. Usa ONTAP tools for VMware vSphere per installare il plug-in VAAI. Questo permette all'array di storage NFS di gestire alcune operazioni di storage invece degli host ESXi.

**Prima di iniziare**

- Scarica il "NetApp NFS Plug-in per VMware VAAI" pacchetto di installazione.
- Assicurati di disporre di host ESXi con vSphere 7.0 U3 (ultima patch o successiva) e ONTAP 9.14.1 o successiva.
- Monta un datastore NFS.

**Passaggi**

1. Accedi al vSphere client.
2. Seleziona **Collegamenti** > **NetApp ONTAP tools** nella sezione dei plug-in.
3. Seleziona **Impostazioni** > **NFS VAAI Tools**.
4. Se hai già caricato il plug-in VAAI su vCenter Server, seleziona **Modifica** in **Versione esistente**. Se non lo hai fatto, seleziona **Carica**.
5. Sfoglia e seleziona il `.vib` file e seleziona **Carica** per caricare il file in ONTAP tools.
6. Seleziona **Installa sull'host ESXi**, seleziona l'host ESXi su cui desideri installare il plug-in NFS VAAI e quindi seleziona **Installa**.

   Il vSphere Web Client mostra solo gli host ESXi che possono installare il plug-in. Puoi monitorare l'avanzamento dell'installazione nella sezione delle attività recenti.

7. Riavvia manualmente l'host ESXi dopo l'installazione.

   Dopo il riavvio dell'host ESXi, ONTAP tools for VMware vSphere rileva e abilita automaticamente il plug-in NFS VAAI.

**E ora?**

Dopo aver installato il plug-in NFS VAAI e riavviato l'host ESXi, configura le policy di esportazione NFS per l'offload della copia VAAI. Assicurati che le regole della policy di esportazione soddisfino questi requisiti:

- Il volume ONTAP pertinente consente le chiamate NFSv4.
- L'utente root rimane root e NFSv4 è consentito in tutti i volumi padre di giunzione.
- L'opzione per il supporto VAAI è impostata sul server NFS pertinente.

Per ulteriori informazioni, consulta l' "Configura le policy di esportazione NFS corrette per l'offload della copia VAAI"articolo KB.

**Informazioni correlate**

"Supporto per VMware vStorage su NFS"

"Abilita o disabilita NFSv4.0"

"Supporto ONTAP per NFSv4.2"

# Configurare le impostazioni dell'host ESXi negli ONTAP tools

La configurazione delle impostazioni di multipath e timeout del server ESXi ti aiuta a mantenere la disponibilità e l'integrità dei dati. Ti permette il failover automatico su un percorso di storage per il backup se il percorso primario diventa non disponibile.

## Configura le impostazioni di multipath e timeout del server ESXi

ONTAP tools for VMware vSphere verifica e imposta le configurazioni multipath dell'host ESXi e le impostazioni di timeout dell'HBA che funzionano al meglio con i sistemi storage NetApp.

**Informazioni su questa attività**

Questo processo potrebbe richiedere del tempo, a seconda della configurazione e del carico di sistema. Puoi visualizzare l'avanzamento nel pannello Attività recenti.

**Passaggi**

1. Dalla home page del client Web vSphere di VMware, seleziona **Host e cluster**.
2. Nella pagina dei collegamenti rapidi del client Web VMware vSphere, seleziona **NetApp ONTAP tools** nella sezione dei plug-in.
3. Vai alla scheda **Conformità host ESXi** nella panoramica (dashboard) del plug-in ONTAP tools for VMware vSphere.
4. Seleziona il link **Applica impostazioni consigliate**.
5. Nella finestra **Applica le impostazioni host consigliate**, seleziona gli host che vuoi aggiornare per usare le impostazioni consigliate NetApp e seleziona **Avanti**.

   Puoi espandere l'host ESXi per vedere i valori attuali.

6. Nella pagina delle impostazioni, seleziona i valori consigliati come richiesto.
7. Nel riquadro di riepilogo, verifica i valori e seleziona **Fine**. Puoi monitorare l'avanzamento nel pannello delle attività recenti.

## Imposta i valori host di ESXi

Utilizza ONTAP tools for VMware vSphere per impostare timeout e altri valori sugli host ESXi per prestazioni e failover ottimali. Imposta questi valori in base ai test NetApp.

Puoi impostare i seguenti valori su un host ESXi:

**Impostazioni dell'adattatore HBA/CNA**

Imposta i seguenti parametri sui valori predefiniti:

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Timeout HBA Emulex FC
- Timeout dell'HBA QLogic FC

### Impostazioni MPIO

Le impostazioni MPIO scelgono i percorsi migliori per i sistemi di archiviazione NetApp. Le impostazioni MPIO selezionano il percorso migliore e lo utilizzano.

Per ambienti dalle performance elevate o quando testi con un singolo datastore LUN, regola l'impostazione di bilanciamento del carico della policy di selezione del percorso round-robin (VMW_PSP_RR) (PSP) per migliorare le prestazioni. Imposta il valore IOPS predefinito da 1000 a 1.

Le impostazioni MPIO non si applicano ai protocolli NVMe, NVMe/FC e NVMe/TCP.

### Impostazioni NFS

| Parametro | Imposta questo valore su… |
|---|---|
| Net.TcpipHeapSize | 32 |
| Net.TcpipHeapMax | 1024 MB |
| NFS.MaxVolumes | 256 |
| NFS41.MaxVolumes | 256 |
| NFS.MaxQueueDepth | 128 o superiore |
| NFS.HeartbeatMaxFailures | 10 |
| NFS.HeartbeatFrequency | 12 |
| NFS.HeartbeatTimeout | 5 |

# Configurare i ruoli e i privilegi utente ONTAP per ONTAP tools

Usa questa sezione per configurare i ruoli utente e i privilegi ONTAP per i backend di storage con ONTAP tools for VMware vSphere e ONTAP System Manager. Puoi assegnare ruoli utilizzando i file JSON forniti, creare manualmente utenti e ruoli e applicare i privilegi minimi richiesti per gli account non admin.

**Prima di iniziare**

- Scarica il file ONTAP Privileges da ONTAP tools for VMware vSphere usando *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*. Dopo aver scaricato il file zip, trovi due file JSON. Usa il file JSON specifico per ASA r2 quando configuri un sistema ASA r2.

  Puoi creare utenti a livello di cluster o direttamente a livello di storage virtual machines (SVM). Se non usi il file user_roles.json, assicurati che l'utente abbia le autorizzazioni SVM minime richieste.

- Accedi con i privilegi di amministratore al backend di archiviazione.

**Passaggi**

1. Estrai il file *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* che hai scaricato.
2. Accedi a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster.

3. Accedi al cluster con privilegi di amministratore. Per configurare un utente:
   a. Per configurare un utente degli ONTAP tools per il cluster, seleziona **Cluster** > **Impostazioni** > riquadro **Utenti e ruoli**.
   b. Per configurare un utente ONTAP tools SVM, seleziona **Storage SVM** > **Impostazioni** > riquadro **Utenti e ruoli**.
   c. Seleziona **Aggiungi** sotto Utenti.
   d. Nella finestra di dialogo **Aggiungi utente**, seleziona **Prodotti di virtualizzazione**.
   e. **Sfoglia** per selezionare e caricare il file JSON ONTAP Privileges. Per i sistemi non-ASA r2, seleziona il file users_roles.json e per i sistemi ASA r2, seleziona il file users_roles_ASAr2.json.

      ONTAP tools compila automaticamente il campo Product.

   f. Seleziona la funzionalità del prodotto come **VSC, VASA Provider e SRA** dal menu a tendina.

      ONTAP tools compila automaticamente il campo **Ruolo** in base alla funzionalità del prodotto che selezioni.

   g. Inserisci il nome utente e la password richiesti.
   h. Seleziona i privilegi (Rilevamento, Crea Storage, Modifica Storage, Elimina Storage, Ruolo NAS/SAN) di cui l'utente ha bisogno, quindi seleziona **Aggiungi**.

ONTAP tools aggiunge il nuovo ruolo e il nuovo utente. Puoi visualizzare i privilegi sotto il ruolo che hai configurato.

## Requisiti di mappatura degli aggregate SVM

Quando esegui il provisioning dei datastore utilizzando le credenziali utente SVM, ONTAP tools for VMware vSphere crea volumi sull'aggregate specificato nell'API POST dei datastore. ONTAP impedisce agli utenti SVM di creare volumi su aggregate non mappati all'SVM. Mappa l'SVM agli aggregate richiesti utilizzando l'API REST o la CLI di ONTAP prima di creare i volumi.

API REST:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

CLI di ONTAP:

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

## Crea manualmente l'utente e il ruolo ONTAP

Crea utenti e ruoli manualmente senza il file JSON.

1. Accedi a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster.
2. Accedi al cluster con privilegi di amministratore.
   a. Per configurare i ruoli degli ONTAP tools per il cluster, seleziona **Cluster** > **Impostazioni** > **Utenti e ruoli**.
   b. Per configurare i ruoli degli strumenti ONTAP SVM del cluster, seleziona **Storage SVM** > **Impostazioni** > **Utenti e ruoli**.
3. Crea ruoli:
   a. Seleziona **Aggiungi** nella tabella **Ruoli**.
   b. Inserisci i dettagli relativi al **nome del ruolo** e agli **attributi del ruolo**.

      Aggiungi il **Percorso REST API** e scegli l'accesso dall'elenco a discesa.

   c. Aggiungi tutte le API necessarie e salva le modifiche.
4. Crea utenti:
   a. Seleziona **Aggiungi** nella tabella **Users**.
   b. Nella finestra di dialogo **Aggiungi utente**, seleziona **System Manager**.
   c. Inserisci il **nome utente**.
   d. Seleziona **Role** tra le opzioni create nella fase **Create Roles** descritta sopra.
   e. Inserisci le applicazioni a cui desideri concedere l'accesso e il metodo di autenticazione. ONTAPI e HTTP sono le applicazioni richieste e il tipo di autenticazione è **Password**.
   f. Imposta la **password per l'utente** e **salva** l'utente.

**Elenco dei privilegi minimi richiesti per un utente cluster con ambito globale non amministratore**

Questa pagina elenca i privilegi minimi richiesti per un utente di cluster con ambito globale non amministratore senza un file JSON. Se un cluster è in ambito locale, usa il file JSON per creare gli utenti perché ONTAP tools for VMware vSphere richiede più dei soli privilegi di lettura per il provisioning su ONTAP.

Puoi accedere alla funzionalità tramite le API:

| API | Livello di accesso | Utilizzato per |
|---|---|---|
| /api/cluster | Sola lettura | Rilevamento della configurazione del cluster |
| /api/cluster/licensing/licenses | Sola lettura | Verifica delle licenze specifiche del protocollo |
| /api/cluster/nodes | Sola lettura | Rilevamento del tipo di piattaforma |
| /api/security/accounts | Sola lettura | Scoperta dei privilegi |
| /api/security/roles | Sola lettura | Scoperta dei privilegi |
| /api/storage/aggregates | Sola lettura | Verifica dello spazio aggregato durante il provisioning del datastore/volume |
| /api/storage/cluster | Sola lettura | Per ottenere i dati relativi allo spazio e all'efficienza a livello di cluster |

| | | |
|---|---|---|
| /api/storage/disks | Sola lettura | Per ottenere i dischi associati in un aggregato |
| /api/storage/qos/policies | Leggi/Crea/Modifica | Gestione delle policy QoS e VM |
| /api/svm/svms | Sola lettura | Per ottenere la configurazione SVM quando il cluster viene aggiunto localmente. |
| /api/network/ip/interfaces | Sola lettura | Aggiungi backend di archiviazione - Per identificare l'ambito della LIF di gestione è cluster/SVM |
| /api/storage/availability-zones | Sola lettura | Rilevamento SAZ. Applicabile alla release ONTAP 9.16.1 e successive e ai sistemi ASA r2. |
| /api/cluster/metrocluster | Sola lettura | Recupera lo stato e i dettagli di configurazione di MetroCluster. |

**Crea un utente con ambito cluster basato su API ONTAP per ONTAP tools for VMware vSphere**

Per le operazioni PATCH e il rollback automatico sui datastore sono necessari i privilegi di discovery, create, modify e destroy. La mancanza di tali privilegi potrebbe causare problemi al workflow e alla pulizia.

Un utente basato su API ONTAP con privilegi di individuazione, creazione, modifica ed eliminazione può gestire i workflow degli ONTAP tools.

Per creare un utente con ambito cluster dotato di tutti i privilegi sopra menzionati, esegui i seguenti comandi:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all
```

```
security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
```

```
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly
```

```
security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -access readonly
```

Inoltre, per le versioni di ONTAP 9.16.0 e successive, eseguire il seguente comando:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

Per i sistemi ASA r2 con versioni di ONTAP 9.16.1 e successive, eseguire il seguente comando:

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

**Crea un utente SVM con ambito basato su API ONTAP per ONTAP tools for VMware vSphere**

Esegui i seguenti comandi per creare un utente con ambito SVM e tutti i privilegi:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
```

```
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>
```

```
security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

Inoltre, per le versioni di ONTAP 9.16.0 e successive, eseguire il seguente comando:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

Per creare un nuovo utente basato su API utilizzando i ruoli basati su API creati in precedenza, eseguire il seguente comando:

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

Esempio:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

Esegui il seguente comando per sbloccare l'account e abilitare l'accesso all'interfaccia di gestione:

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

Esempio:

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

## Aggiorna ONTAP tools for VMware vSphere 10.1 user a 10.3 user

Per gli utenti di ONTAP tools for VMware vSphere 10.1 con un utente a livello di cluster creato tramite file JSON, usa i seguenti comandi ONTAP CLI con privilegi admin per eseguire l'aggiornamento alla release 10.3.

Per le funzionalità del prodotto:

- VSC
- VSC e VASA Provider
- VSC e SRA
- VSC, VASA Provider e SRA.

Privilegi del cluster:

*security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all*

Per gli utenti di ONTAP tools for VMware vSphere 10.1 con un utente con ambito SVM creato tramite file json, usa i comandi CLI di ONTAP con privilegi di amministratore per eseguire l'aggiornamento alla release 10.3.

Privilegi SVM:

*security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>*

*security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>*

Per abilitare i seguenti comandi, aggiungi i comandi *vserver nvme namespace show* e *vserver nvme subsystem show* al ruolo esistente.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

## Aggiorna ONTAP tools for VMware vSphere utente 10.3 a utente 10.4

A partire da ONTAP 9.16.1, aggiorna l'utente di ONTAP tools for VMware vSphere 10.3 a utente 10.4.

Per ONTAP tools for VMware vSphere 10.3, se hai un utente con ambito cluster creato tramite file JSON e versione di ONTAP 9.16.1 o superiore, usa il comando ONTAP CLI con privilegi di amministratore per eseguire l'aggiornamento alla release 10.4.

Per le funzionalità del prodotto:

- VSC
- VSC e VASA Provider
- VSC e SRA

- VSC, VASA Provider e SRA.

Privilegi del cluster:

```
security login role create -role <existing-role-name> -cmddirname "storage
availability-zone show" -access all
```

# Aggiungi un backend di storage a ONTAP tools

Usa ONTAP tools per VMware vSphere per aggiungere e gestire i backend di storage per i tuoi host ESXi. Puoi aggiungere cluster o SVM, abilitare il supporto MetroCluster e convalidare i certificati per una connettività sicura. Puoi configurare i backend di storage usando ONTAP tools Manager o il client vSphere, monitorare lo stato dei certificati e riscoprire manualmente le risorse dopo le modifiche al cluster.

Per aggiungere un backend di storage in locale, usa le credenziali del cluster o dell'SVM nell'interfaccia di ONTAP tools. I backend di storage locali sono disponibili solo per il vCenter Server selezionato. ONTAP tools mappa gli SVM al vCenter Server per la gestione dei datastore vVols o VMFS. Per i datastore VMFS e i workflow SRA, puoi usare le credenziali dell'SVM senza mappare un cluster a livello globale.

Per aggiungere un backend di storage globale, usa le credenziali del cluster ONTAP in ONTAP tools Manager. I backend di storage globali abilitano i workflow di discovery per identificare le risorse del cluster necessarie per la gestione dei vVol. Negli ambienti multi-tenant, puoi aggiungere localmente un utente SVM per gestire i datastore vVols.

Consultare l'articolo della Knowledge Base: "OTV 10: Cos'è l'ambito globale e locale del backend di archiviazione" per ulteriori informazioni sui backend di archiviazione globali e locali.

Se il supporto MetroCluster è abilitato in ONTAP, integra sia il cluster di origine che quello di destinazione come backend di storage locali o globali.

**Prima di iniziare**

Verifica che il certificato includa un campo Subject Alternative Name (SAN) valido. I sistemi ONTAP utilizzano il campo SAN per identificare le LIF di gestione del cluster e delle SVM.

**Usare ONTAP tools Manager**

In una configurazione multi-tenant, puoi aggiungere un cluster di backend dello storage a livello globale e SVM a livello locale per usare le credenziali utente di SVM.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona **Storage Backends** dalla barra laterale.
4. Aggiungi il backend di storage e fornisci l'indirizzo IP del server o il FQDN, il nome utente e la password.

   Sono supportate le LIF di gestione degli indirizzi IPv4 e IPv6.

5. Recupera automaticamente i certificati del cluster ONTAP e autorizza il certificato, oppure caricalo manualmente accedendo alla sua posizione.

   Se necessario, puoi disabilitare la convalida del Subject Alternative Name (SAN) dalla console di manutenzione. Per istruzioni, vedi "Modifica il flag di convalida del certificato".

6. Se il backend di storage che aggiungi fa parte di una configurazione MetroCluster, ONTAP tools Manager mostra un messaggio pop-up per aggiungere il cluster peer. Seleziona **Aggiungi** e inserisci i dettagli per il backend di storage peer MetroCluster.

   Dopo che il sistema ONTAP ha eseguito uno switchover e uno switchback, esegui manualmente la discovery degli ONTAP tools.

**Utilizzando l'interfaccia utente del client vSphere**

I datastore vVols non supportano l'aggiunta diretta di un utente SVM tramite l'interfaccia utente client vSphere.

1. Accedi al vSphere client.
2. Nella pagina dei collegamenti rapidi, seleziona **NetApp ONTAP tools** nella sezione dei plug-in.
3. Seleziona **Storage Backends** dalla barra laterale.
4. Aggiungi il backend di storage e fornisci l'indirizzo IP del server, il nome utente, la password e i dettagli della porta.

   Puoi aggiungere un backend di storage utilizzando credenziali basate su cluster con LIF di gestione IPv4 o IPv6. Per aggiungere direttamente un utente SVM, fornisci credenziali basate su SVM insieme a un LIF di gestione SVM. Se un cluster è già stato integrato, non puoi integrare nuovamente un utente SVM da quel cluster.

5. Recupera automaticamente i certificati del cluster ONTAP e autorizza il certificato, oppure caricalo manualmente accedendo alla sua posizione.

6. Se il backend di storage aggiunto fa parte della configurazione MetroCluster, ONTAP tools visualizza la schermata **Add MetroCluster peer**. Seleziona **Add peer** per aggiungere il backend di storage peer.

> Dopo che il sistema ONTAP ha eseguito uno switchover e uno switchback, esegui manualmente la discovery degli ONTAP tools.

ONTAP tools elenca il nuovo storage backend aggiunto nella pagina **Storage backends**. Se un certificato scade entro 30 giorni o meno, ONTAP tools mostra un avviso nella colonna della data di scadenza del certificato. Dopo la scadenza, ONTAP tools segna lo storage backend come sconosciuto perché non può connettersi al sistema storage.

**Informazioni correlate**

"OTV 10: Cos'è l'ambito globale e locale del backend di archiviazione"

"Configurare i cluster in una configurazione MetroCluster"

# Associare un backend di storage a un'istanza del vCenter Server negli ONTAP tools

Associa un backend di storage a un'istanza vCenter Server per consentire l'accesso a tutte le istanze vCenter Server. Per la configurazione MetroCluster, quando associ un cluster di backend di storage, assicurati di associare anche il relativo cluster peer al vCenter Server.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona vCenter dalla barra laterale.
4. Seleziona i puntini di sospensione verticali accanto all'istanza del vCenter Server che vuoi connettere ai backend di storage.
5. Dal menu a tendina, scegli il backend di storage che vuoi associare all'istanza di vCenter Server selezionata.

# Configurare l'accesso alla rete negli ONTAP tools

Per impostazione predefinita, tutti gli indirizzi IP rilevati dall'host ESXi vengono aggiunti automaticamente alla policy di esportazione, a meno che tu non configuri l'accesso di rete. Puoi modificare la policy di esportazione per consentire l'accesso solo da specifici indirizzi IP. Se un host ESXi escluso tenta un'operazione di mount, l'operazione fallisce.

**Passaggi**

1. Accedi al vSphere client.
2. Seleziona **NetApp ONTAP tools** nella pagina dei collegamenti rapidi, nella sezione dei plug-in.

3. Nel riquadro sinistro di ONTAP tools, vai su **Impostazioni** > **Gestisci accesso alla rete** > **Modifica**.

   Per aggiungere più indirizzi IP, separa l'elenco con virgole, intervalli, Classless Inter-Domain Routing (CIDR) o una combinazione di tutti e tre.

4. Seleziona **Salva**.

# Creare un datastore in ONTAP tools

Quando crei un datastore a livello di cluster host, ONTAP tools lo monta su tutti gli host di destinazione e abilita l'azione solo se hai i privilegi necessari.

**Interoperabilità tra datastore nativi con vCenter Server e datastore gestiti dagli ONTAP tools**

A partire da ONTAP tools per VMware vSphere 10.4, ONTAP tools crea igroup nidificati per i datastore, con igroup padre specifici per i datastore e igroup figlio mappati agli host. Puoi creare igroup flat da ONTAP System Manager e usarli per creare datastore VMFS senza usare ONTAP tools. Consulta "Gestisci gli iniziatori SAN e gli igroup" per ulteriori informazioni.

Dopo aver integrato lo storage ed eseguito il rilevamento dei datastore, ONTAP tools converte gli igroup flat nei datastore VMFS in igroup nidificati. Non puoi utilizzare gli igroup flat precedenti per creare nuovi datastore. Usa l'interfaccia di ONTAP tools o la REST API per riutilizzare gli igroup nidificati.

**Crea un datastore vVols**

A partire da ONTAP tools for VMware vSphere 10.3, puoi creare un datastore vVols su sistemi ASA r2 con efficienza dello spazio impostata su thin vVol. Il VASA Provider crea un container e gli endpoint di protocollo desiderati durante la creazione del datastore vVol. Il VASA Provider non assegna alcun volume di supporto a questo container.

**Prima di iniziare**

- Assicurarsi che gli aggregati radice non siano mappati sull'SVM.
- Assicurati che il VASA Provider sia registrato con il vCenter selezionato.
- Nel sistema storage ASA r2, l'SVM deve essere mappato all'aggregato per l'utente SVM.

**Passaggi**

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un sistema host, un cluster o un data center e seleziona **NetApp ONTAP tools** > **Create Datastore**.
3. Selezionare vVols come **Tipo di archivio dati**.
4. Inserisci il **nome del datastore** e le informazioni sul **protocollo**.

   Il sistema ASA r2 supporta i protocolli iSCSI e FC per vVols.

5. Seleziona la storage VM in cui vuoi creare il datastore.
6. Nelle opzioni avanzate:
   - Se selezioni la **Custom export policy**, assicurati di eseguire il rilevamento in vCenter per tutti gli oggetti. Si consiglia di non usare questa opzione.
   - È possibile selezionare un nome **Custom initiator group** per i protocolli iSCSI e FC.

   Nel sistema storage ASA di tipo SVM, le unità di storage (LUN/namespace) non vengono create perché il datastore è solo un container logico.

7. Nel riquadro **Attributi di archiviazione**, puoi creare nuovi volumi o utilizzare quelli esistenti. Tuttavia, non puoi combinare questi due tipi di volumi per creare un datastore vVols.

   Quando si crea un nuovo volume, è possibile abilitare il QoS sul datastore. Per impostazione predefinita, viene creato un volume per ogni richiesta di creazione di LUN. Saltare questo passaggio per i datastore vVols sui sistemi di storage ASA r2.

8. Rivedi la tua selezione nel riquadro **Riepilogo** e seleziona **Fine**.

**Crea un datastore NFS**

Un datastore NFS collega gli host ESXi allo storage condiviso utilizzando il protocollo NFS. Sono semplici e flessibili e vengono utilizzati negli ambienti VMware vSphere.

**Passaggi**

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un sistema host, un cluster o un data center e seleziona **NetApp ONTAP tools** > **Create datastore**.
3. Seleziona NFS nel campo **Tipo di datastore**.

4. Nel riquadro **Nome e protocollo**, inserisci il nome del datastore, le dimensioni e le informazioni sul protocollo. Nelle opzioni avanzate, seleziona **Datastore cluster** e **Kerberos authentication**.

   L'autenticazione Kerberos è disponibile solo quando il protocollo NFS 4.1 è selezionato.

5. Nel riquadro **Storage**, seleziona **Platform** e **Storage VM**.
6. Se selezioni **Custom export policy** nelle opzioni avanzate, esegui la discovery in vCenter per tutti gli oggetti. Si consiglia di non usare questa opzione.

   Non puoi creare un datastore NFS utilizzando la policy predefinita o di volume root della SVM.

   - Nelle opzioni avanzate, il pulsante di attivazione **Asimmetrico** è visibile solo se sono selezionate prestazioni o capacità nel menu a tendina della piattaforma.
   - Quando scegli l'opzione **Any** nel menu a tendina della piattaforma, puoi vedere tutti gli SVM nel vCenter. La piattaforma e il flag asimmetrico non influiscono sulla visibilità.
7. Seleziona l'aggregato per la creazione del volume nel riquadro **Attributi di storage**. Nelle opzioni avanzate, scegli **Riserva spazio** e **Abilita QoS** come richiesto.
8. Rivedi le selezioni nel riquadro **Riepilogo** e seleziona **Fine**.

ONTAP tools crea il datastore NFS e lo monta su tutti gli host.

#### Crea un datastore VMFS

VMFS è un file system cluster per l'archiviazione dei file delle macchine virtuali. Più host ESXi possono accedere simultaneamente agli stessi file VM per le funzionalità vMotion e High Availability.

Su un cluster protetto:

- Puoi creare solo datastore VMFS. Aggiungendo un datastore VMFS a un cluster protetto, viene automaticamente protetto.
- Non puoi creare un datastore in un data center con uno o più cluster host protetti.
- Non puoi creare un datastore su un host ESXi se il cluster host principale è protetto da una "Automated Failover Duplex policy" (configurazione uniforme o non uniforme).
- Puoi creare un datastore VMFS solo su un host ESXi protetto da una relazione asincrona. Non puoi creare e montare un datastore su un host ESXi che fa parte di un cluster protetto dalla policy "Automated Failover Duplex".

#### Prima di iniziare

- Abilita i servizi e i LIF per ciascun protocollo sul lato storage ONTAP.
- Mappa SVM all'aggregato per l'utente SVM nel sistema storage ASA.
- Configura l'host ESXi se usi il protocollo NVMe/TCP:
  a. Esaminare il "Guida alla compatibilità VMware"

     VMware vSphere 7.0 U3 e versioni successive supportano il protocollo NVMe/TCP. Tuttavia, si consiglia di utilizzare VMware vSphere 8.0 e versioni successive.

  b. Verifica se il fornitore della scheda di interfaccia di rete (NIC) supporta la NIC ESXi con il

protocollo NVMe/TCP.

c. Configura la scheda di rete ESXi per NVMe/TCP secondo le specifiche del fornitore della scheda di rete.

d. Quando si utilizza VMware vSphere 7, seguire le istruzioni sul sito VMware "Configura il binding VMkernel per l'adattatore NVMe over TCP" per configurare il binding della porta NVMe/TCP. Quando si utilizza VMware vSphere 8, seguire "Configurare NVMe over TCP su ESXi" per configurare il binding della porta NVMe/TCP.

e. Per la release di VMware vSphere 7, segui le istruzioni nella pagina "Abilita gli adattatori software NVMe over RDMA o NVMe over TCP" per configurare gli adattatori software NVMe/TCP. Per la release di VMware vSphere 8, segui "Aggiungi adattatori software NVMe over RDMA o NVMe over TCP" per configurare gli adattatori software NVMe/TCP.

f. Eseguire "Scopri i sistemi storage e gli host" l'azione sull'host ESXi. Per ulteriori informazioni, consulta "Come configurare NVMe/TCP con vSphere 8.0 Update 1 e ONTAP 9.13.1 per i datastore VMFS".

- Se usi il protocollo NVMe/FC, segui questi passaggi per configurare l'host ESXi:

  a. Se non è già abilitato, abilita NVMe over Fabrics (NVMe-oF) sul tuo host ESXi.

  b. Zonizzazione SCSI completa.

  c. Assicurati che gli host ESXi e il sistema ONTAP siano connessi sia a livello fisico che logico.

Per configurare un ONTAP SVM per il protocollo FC, fare riferimento a "Configura un SVM per FC".

Per ulteriori informazioni sull'utilizzo del protocollo NVMe/FC con VMware vSphere 8.0, fare riferimento a "Configurazione host NVMe-oF per ESXi 8.x con ONTAP".

Per ulteriori informazioni sull'utilizzo di NVMe/FC con VMware vSphere 7.0, fare riferimento a "Guida alla configurazione dell'host ONTAP NVMe/FC" e "TR-4684".

**Passaggi**

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un sistema host, un cluster o un data center e seleziona **NetApp ONTAP tools** > **Create Datastore**.
3. Selezionare il tipo di datastore VMFS.
4. Nel riquadro **Nome e protocollo**, inserisci il nome, le dimensioni e le informazioni sul protocollo del datastore. Per aggiungere il nuovo datastore a un cluster VMFS esistente, seleziona il cluster di datastore in Opzioni avanzate.
5. Seleziona una VM di archiviazione nel riquadro **Archiviazione**. Fornisci il **Custom initiator group name** nella sezione **Advanced options** se necessario. Puoi scegliere un igroup esistente per il datastore oppure crearne uno nuovo con un nome personalizzato.

   Quando selezioni il protocollo NVMe/FC o NVMe/TCP, viene creato un nuovo sottosistema di namespace che viene utilizzato per la mappatura dei namespace. ONTAP tools crea il sottosistema di namespace utilizzando il nome generato automaticamente che include il nome del datastore. Puoi rinominare il sottosistema di namespace nel campo **custom namespace subsystem name** nelle opzioni avanzate del pannello **Storage**.

6. Dal riquadro **attributi dello storage**:

   a. Seleziona **Aggregate** dal menu a tendina.

Per i sistemi di storage ASA r2, l'opzione **Aggregate** non viene visualizzata perché lo storage è disaggregato. Quando scegli un sistema di storage ASA r2 di tipo SVM, la pagina degli attributi di storage mostra le opzioni per abilitare il QoS.

b. Gli strumenti ONTAP creano un'unità di archiviazione (LUN/Namespace) con una riserva di spazio ridotta in base al protocollo selezionato.

A partire da ONTAP 9.16.1, i sistemi storage ASA r2 supportano fino a 12 nodi per cluster.

c. Seleziona il **livello di servizio Prestazioni** per i sistemi storage ASA r2 con SVM a 12 nodi che fanno parte di un cluster eterogeneo. Questa opzione non è disponibile se l'SVM selezionato è un cluster omogeneo o utilizza un utente SVM.

'Any' è il valore predefinito del livello di servizio prestazionale (PSL). Questa impostazione crea l'unità di storage utilizzando l'algoritmo di posizionamento bilanciato di ONTAP. Tuttavia, puoi selezionare l'opzione "performance" o "extreme" a seconda delle esigenze.

d. Seleziona **Usa volume esistente**, **Abilita QoS** se necessario e fornisci i dettagli.

Nel tipo di storage ASA r2, la creazione o la selezione del volume non si applica alla creazione dell'unità di storage (LUN/Namespace). Pertanto, queste opzioni non vengono visualizzate.

Non puoi utilizzare il volume esistente per creare un datastore VMFS con protocollo NVMe/FC o NVMe/TCP. Crea un nuovo volume per il datastore VMFS.

7. Esamina i dettagli del datastore nel riquadro **Riepilogo** e seleziona **Fine**.

Se crei il datastore su un cluster protetto, puoi vedere un messaggio di sola lettura: "Il datastore è in fase di montaggio su un cluster protetto."

**Risultato**

Gli strumenti ONTAP creano il datastore VMFS e lo montano su tutti gli host.

# Proteggi i datastore e le macchine virtuali

## Proteggere un cluster host negli ONTAP tools

ONTAP tools for VMware vSphere gestisce la protezione dei cluster host. Tutti i datastore appartenenti alla SVM selezionata e montati su uno o più host del cluster sono protetti nell'ambito di un cluster host.

**Prima di iniziare**

Assicurati di soddisfare questi requisiti prima di proteggere un cluster host:

- Il cluster host contiene archivi dati provenienti da una sola SVM.
- I datastore presenti sul cluster non vengono montati su host esterni al cluster.
- I datastore montati sul cluster host sono datastore VMFS con protocollo iSCSI o FC. Non puoi usare vVols, NFS o datastore VMFS con protocolli NVMe/FC e NVMe/TCP.
- I datastore basati su volumi FlexVol/LUN montati su un host non fanno parte di alcun gruppo di coerenza.
- I datastore basati su volumi FlexVol/LUN montati su un host non fanno parte di alcuna relazione SnapMirror.
- Il cluster host contiene almeno un datastore.

**Passaggi**

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un cluster e seleziona **NetApp ONTAP tools** > **Protect Cluster**.
3. Nella finestra di protezione del cluster, il sistema compila automaticamente il tipo di datastore e i dettagli della macchina virtuale (VM) di origine dello storage. Seleziona il collegamento dei datastore per visualizzare i datastore protetti.
4. Seleziona **Aggiungi relazione**.
5. Nella finestra **Aggiungi relazione SnapMirror**, seleziona la **storage VM di destinazione** e il tipo di **policy**.

   Il tipo di policy può essere asincrono o AutomatedFailOverDuplex.

   Quando si aggiunge la relazione SnapMirror come policy di tipo AutomatedFailOverDuplex, è necessario aggiungere la VM di storage di destinazione come backend di storage allo stesso vCenter in cui ONTAP tools for VMware vSphere è distribuito.

   Nel tipo di policy AutomatedFailOverDuplex, sono presenti configurazioni host uniformi e non uniformi. Quando si seleziona il pulsante di attivazione **Configurazione host uniforme**, la configurazione del gruppo initiator host viene replicata implicitamente sul sito di destinazione. Per ulteriori informazioni, consulta "Concetti e termini chiave".

6. Se scegli di avere una configurazione host non uniforme, seleziona l'accesso host (origine/destinazione) per ciascun host all'interno di quel cluster.
7. Seleziona **Aggiungi**.
8. Puoi modificare la protezione del cluster host usando l'operazione **Modifica protezione cluster host**. Puoi modificare o eliminare le relazioni usando le opzioni del menu con i puntini di sospensione.

9. Seleziona il pulsante **Proteggi**.

   Il sistema crea un'attività di vCenter con i dettagli dell'ID del lavoro e ne mostra l'avanzamento nel pannello delle attività recenti. Questa è un'attività asincrona; l'interfaccia utente mostra solo lo stato di invio della richiesta e non attende il completamento dell'attività.

10. Per visualizzare i cluster host protetti, vai su **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**. Seleziona un gruppo di coerenza per visualizzarne la capacità, i datastore associati e i gruppi di coerenza figlio.

> Se devi rimuovere la protezione entro un'ora dalla creazione, esegui prima la rilevazione dello storage.

**Informazioni correlate**

"VMware vSphere Metro Storage Cluster (vMSC)"

# Proteggi usando la protezione SRA

## Configurare SRA negli ONTAP tools per proteggere i datastore

ONTAP tools for VMware vSphere offre la possibilità di abilitare la funzionalità SRA per configurare il disaster recovery.

**Prima di iniziare**

- Dovresti aver già configurato la tua istanza del server vCenter e gli host ESXi.
- Dovresti aver implementato ONTAP tools for VMware vSphere.
- Dovresti aver scaricato il file dell'adattatore SRA `.tar.gz` dal "Sito di supporto NetApp".
- Dovresti avere le stesse pianificazioni personalizzate di SnapMirror sia sul cluster ONTAP di origine che su quello di destinazione prima di eseguire i flussi di lavoro SRA.
- "Abilita i servizi di ONTAP tools per VMware vSphere" per abilitare la funzionalità SRA.

**Passaggi**

1. Accedi all'interfaccia di gestione dell'appliance VMware Live Site Recovery utilizzando l'URL: `https://<srm_ip>:5480`, quindi vai su Storage Replication Adapters nell'interfaccia di gestione dell'appliance VMware Live Site Recovery.
2. Seleziona **Nuovo adattatore**.
3. Carica il file di installazione *.tar.gz* del plug-in SRA su VMware Live Site Recovery.
4. Esegui una nuova scansione degli adattatori per verificare che i dettagli siano aggiornati nella pagina Adattatori di replica dello storage di VMware Live Site Recovery.

> Dopo un failover, azioni come espansione, montaggio ed eliminazione potrebbero non essere disponibili per i datastore. Esegui l'individuazione del datastore per aggiornare e visualizzare le azioni appropriate del menu contestuale.

> Dopo ogni operazione di riprotezione, devi eseguire la rilevazione dello storage su entrambi i siti.

In una nuova configurazione con protezione SRA, esegui sempre un failover di prova. Saltare il failover di prova potrebbe causare il fallimento dell'operazione di riprotezione.

In una configurazione fan-out, dopo un failover Active Sync di SnapMirror in cui la fonte di SnapMirror passa al sito B per Automated Failover Duplex e Asynchronous SnapMirror, esegui un test failover tra i siti B e C. Saltare questo passaggio può causare un errore nell'operazione di riprotezione.

**Informazioni correlate**

"Configura il disaster recovery per i datastore NFS usando VMware Site Recovery Manager"

## Configurare SRA in ONTAP tools for VMware vSphere per ambienti SAN e NAS

Dovresti configurare i sistemi di storage prima di eseguire Storage Replication Adapter (SRA) per VMware Live Site Recovery.

### Configura SRA per ambienti SAN

I gruppi di coerenza nei flussi di lavoro SRA sono supportati solo con protocolli SAN (iSCSI e Fibre Channel) sia sui sistemi di storage Unified che ASA r2.

**Prima di iniziare**

Dovresti avere i seguenti programmi installati sul sito protetto e sul sito di recovery:

- VMware Live Site Recovery: Il sito VMware fornisce la documentazione per l'installazione di VMware Live Site Recovery.

  "Informazioni su VMware Live Site Recovery"

- SRA: Installa l'adattatore su VMware Live Site Recovery.

Per le configurazioni del protocollo iSCSI, prima di eseguire i flussi di lavoro SRA, tenere presente quanto segue:

- **Sito protetto**: gli adattatori di storage iSCSI e i dettagli LIF dei dati vengono configurati automaticamente durante il provisioning dei datastore. Non è richiesta alcuna configurazione manuale.
- **Sito di ripristino**: gli adattatori di storage iSCSI devono essere configurati manualmente su ciascun host ESXi incluso nella mappatura delle risorse per il ripristino di emergenza. Per evitare di configurare gli adattatori singolarmente su ciascun host, crea un datastore segnaposto di tipo iSCSI sul sito di ripristino utilizzando la SVM su cui sono configurati i workflow SRA. Questo aggiunge automaticamente l'adattatore iSCSI e gli indirizzi IP LIF dei dati necessari a tutti gli host ESXi mappati. Consultare "Configurare i datastore segnaposto negli ONTAP tools" per maggiori dettagli.

**Passaggi**

1. Verifica che gli host ESXi primari siano connessi alle LUN nel sistema di storage primario del sito protetto.
2. Verificare che le LUN siano presenti in igroups che hanno l' `ostype`opzione impostata su *VMware* sul sistema di storage primario.
3. Verifica che gli host ESXi del sito di recovery abbiano una connettività iSCSI e Fibre Channel appropriata verso la storage virtual machine (SVM). Gli host ESXi del sito secondario devono avere accesso allo storage del sito secondario, e gli host ESXi del sito primario devono avere accesso allo storage del sito primario.

   Puoi farlo verificando che gli host ESXi abbiano LUN locali connessi sull'SVM oppure tramite il comando

`iscsi show initiators` sugli SVM. Controlla l'accesso ai LUN per i LUN mappati nell'host ESXi per verificare la connettività iSCSI.

### Configura SRA per gli ambienti NAS

I gruppi di coerenza non sono supportati per NFS nei flussi di lavoro SRA. Se i volumi di datastore NFS vengono inseriti in un gruppo di coerenza e protetti, l'operazione Discover Devices non andrà a buon fine. Non utilizzare i gruppi di coerenza quando si proteggono i datastore NFS con SRA.

#### Prima di iniziare

Dovresti avere i seguenti programmi installati sul sito protetto e sul sito di recovery:

- VMware Live Site Recovery: Puoi trovare la documentazione di installazione di VMware Live Site Recovery sul sito VMware "Informazioni su VMware Live Site Recovery"
- SRA: Installa l'adattatore su VMware Live Site Recovery e sul server SRA.

#### Passaggi

1. Verifica che i datastore del sito protetto contengano macchine virtuali registrate con vCenter Server.
2. Verificare che gli host ESXi nel sito protetto abbiano montato i volumi di esportazione NFS dalla storage virtual machine (SVM).
3. Verificare che nel campo **NFS Addresses** siano specificati indirizzi IP validi su cui sono presenti le esportazioni NFS quando si utilizza la procedura guidata di Array Manager per aggiungere array a VMware Live Site Recovery. Non utilizzare il nome host NFS o il FQDN nel campo **NFS Addresses**.
4. Usa il comando `ping` su ogni host ESXi nel sito di recovery per verificare che l'host abbia una porta VMkernel che può accedere agli indirizzi IP utilizzati per servire le esportazioni NFS dalla SVM.

## Configurare SRA in ONTAP tools per ambienti altamente scalabili

Dovresti configurare gli intervalli di timeout di storage secondo le impostazioni consigliate per Storage Replication Adapter (SRA) per ottenere prestazioni ottimali in ambienti altamente scalati.

### Impostazioni del provider di archiviazione

Dovresti impostare i seguenti valori di timeout su VMware Live Site Recovery per ambienti scalabili:

| Impostazioni avanzate | Valori di timeout |
|---|---|
| `StorageProvider.resignatureTimeout` | Aumenta il valore dell'impostazione da 900 secondi a 12000 secondi. |
| `storageProvider.hostRescanDelaySec` | 60 |
| `storageProvider.hostRescanRepeatCnt` | 20 |
| `storageProvider.hostRescanTimeoutSec` | Imposta un valore elevato (per esempio: 99999) |

Dovresti anche abilitare l'opzione `StorageProvider.autoResignatureMode`.

Consultare "Modifica le impostazioni del provider di storage" per ulteriori informazioni sulla modifica delle impostazioni del provider di archiviazione.

**Impostazioni di archiviazione**

Quando si verifica un timeout, aumenta i valori di `storage.commandTimeout` e `storage.maxConcurrentCommandCnt` a un valore più alto.

> L'intervallo di timeout specificato è il valore massimo. Non è necessario attendere che venga raggiunto il timeout massimo. La maggior parte dei comandi termina entro l'intervallo di timeout massimo impostato.

Consultare "Modifica le impostazioni di storage" per modificare le impostazioni del provider SAN.

## Configurare SRA sull'appliance VMware Live Site Recovery utilizzando ONTAP tools

Dopo aver distribuito l'appliance VMware Live Site Recovery, configura lo Storage Replication Adapter (SRA) per abilitare la gestione del disaster recovery.

Configurare SRA sull'appliance VMware Live Site Recovery salva le credenziali degli ONTAP tools for VMware vSphere all'interno dell'appliance, abilitando la comunicazione tra VMware Live Site Recovery e SRA.

**Prima di iniziare**

- Scarica il file *.tar.gz* da "Sito di supporto NetApp".
- Abilitare i servizi SRA in ONTAP tools Manager. Per ulteriori informazioni, consultare la sezione "Abilita i servizi".
- Aggiungi i server vCenter all'appliance ONTAP tools for VMware vSphere. Per ulteriori informazioni, consultare la sezione "Aggiungi vCenter Server".
- Aggiungere backend di storage a ONTAP tools for VMware vSphere. Per ulteriori informazioni, consultare la sezione "Aggiungi backend di storage".

> Se hai applicato la patch del certificato vCenter dagli ONTAP tools, aggiorna la configurazione vCenter nell'appliance VMware Live Site Recovery utilizzando la porta (:5480). Per istruzioni, consulta "Riconfigura l'appliance di Site Recovery Manager".

**Passaggi**

1. Nella schermata dell'appliance VMware Live Site Recovery, seleziona **Storage Replication Adapter** > **New Adapter**.
2. Carica il file *.tar.gz* su VMware Live Site Recovery.
3. Accedi all'appliance VMware Live Site Recovery utilizzando un account amministratore tramite un client SSH come PuTTY.
4. Passa all'utente root utilizzando il comando: `su root`
5. Esegui il comando `cd /var/log/vmware/srm` per accedere alla directory dei log.
6. Nella posizione del log, inserisci il comando per ottenere il Docker ID utilizzato da SRA: `docker ps -l`

7. Per accedere all'ID del container, inserisci il comando: `docker exec -it -u srm <container id> sh`
8. Configura VMware Live Site Recovery con ONTAP tools for VMware vSphere indirizzo IP e password utilizzando il comando: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - Inserisci la password tra virgolette singole in modo che lo script Perl consideri i caratteri speciali come parte della password, non come delimitatori.
   - Puoi impostare il nome utente e la password dell'applicazione (VASA Provider/SRA) in ONTAP tools Manager quando abiliti questi servizi per la prima volta. Usa queste credenziali per registrare SRA con VMware Live Site Recovery.
   - Per individuare il GUID di vCenter, vai alla pagina Server di vCenter in ONTAP tools Manager dopo aver aggiunto la tua istanza vCenter. Fai riferimento alla sezione "Aggiungi vCenter Server".
9. Esegui una nuova scansione degli adattatori per verificare che i dettagli aggiornati vengano visualizzati nella pagina Adattatori di replica dello storage di VMware Live Site Recovery.

**Risultati** Viene visualizzato un messaggio di conferma che indica che le credenziali di storage sono state salvate. Ora puoi usare SRA per comunicare con il server SRA utilizzando l'indirizzo IP, la porta e le credenziali specificati.

## Aggiorna le credenziali SRA negli strumenti ONTAP

Affinché VMware Live Site Recovery possa comunicare con SRA, dovresti aggiornare le credenziali di SRA sul server VMware Live Site Recovery se hai modificato le credenziali.

### Prima di iniziare

Dovresti aver eseguito i passaggi menzionati nell'argomento "Configurare SRA sull'appliance VMware Live Site Recovery".

### Passaggi

1. Eseguire i seguenti comandi per eliminare le credenziali degli ONTAP tools memorizzate nella cache dalla macchina VMware Live Site Recovery:
   a. `sudo su <enter root password>`
   b. `docker ps`
   c. `docker exec -it <container_id> sh`
   d. `cd conf/`
   e. `rm -rf *`
2. Esegui il comando Perl per configurare SRA con le nuove credenziali:
   a. `cd ..`
   b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv -password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`Devi mettere una singola virgoletta intorno al valore della password.

      Viene visualizzato un messaggio di conferma dell'avvenuta memorizzazione delle credenziali di archiviazione. SRA può comunicare con il server SRA utilizzando l'indirizzo IP, la porta e le credenziali fornite.

### Riconfigurare vCenter nell'appliance VMware Live Site Recovery dopo una modifica del certificato

Se il certificato vCenter cambia, ad esempio dopo un aggiornamento vCenter, è possibile che si verifichi un errore di mancata corrispondenza dell'impronta digitale nell'estensione Site Recovery. Eseguire i seguenti passaggi per risolverlo.

**Passaggi**

1. Riconfigurare vCenter nell'appliance VMware Live Site Recovery
   a. Aprire l'interfaccia di gestione dell'appliance VMware Live Site Recovery in un browser: `https://<SRM_IP>:5480`
   b. Seleziona la scheda **Riepilogo**.
   c. Seleziona **Riconfigura** per la connessione al server vCenter.

      Questo recupera e accetta l'impronta digitale del certificato più recente da vCenter.
2. Riconnetti l'associazione del sito (se l'errore persiste)

   Se l'errore di mancata corrispondenza dell'impronta digitale persiste dopo la riconfigurazione:

   a. Accedi all'interfaccia utente di vCenter.
   b. Accedere all'estensione **Site Recovery**.
   c. Individua la sezione **Associazione siti**.
   d. Seleziona **Riconnetti** per ristabilire l'associazione del sito con il certificato aggiornato.

## Configura i siti protetti e di ripristino negli ONTAP tools

Dovresti creare gruppi di protezione per proteggere un gruppo di macchine virtuali sul sito protetto.

Quando aggiungi un nuovo datastore, puoi includerlo nel gruppo di datastore esistente oppure aggiungere un nuovo datastore e creare un nuovo volume o gruppo di coerenza per la protezione. Dopo aver aggiunto un nuovo datastore a un gruppo di coerenza o a un volume protetto, aggiorna SnapMirror ed esegui la discovery dello storage sia sul sito protetto che su quello di recovery. Puoi eseguire la discovery manualmente o secondo una pianificazione per assicurarti che il nuovo datastore venga rilevato e protetto.

### Abbina siti protetti e di recovery

Dovresti associare i siti protetti e di recovery creati usando il vSphere Client per permettere allo Storage Replication Adapter (SRA) di rilevare i sistemi storage.

> Storage Replication Adapter (SRA) supporta il fan-out con una relazione sincrona di tipo Automated Failover Duplex e una relazione asincrona SnapMirror sul gruppo di coerenza. Tuttavia, il fan-out con due relazioni asincrone SnapMirror sui gruppi di coerenza o relazioni fan-out SnapMirror sui volumi non è supportato. Le relazioni di tipo vault SnapMirror non sono considerate all'interno di queste restrizioni di fan-out. Il supporto dei gruppi di coerenza in SRA è limitato ai protocolli SAN (iSCSI e fibre channel) sui sistemi di storage Unified e ASA r2. I gruppi di coerenza non sono supportati per NFS. Se i volumi del datastore NFS vengono inseriti in un gruppo di coerenza, l'operazione di rilevamento dei dispositivi non andrà a buon fine.

**Prima di iniziare**

- Dovresti avere VMware Live Site Recovery installato sia sul sito protetto che su quello di recovery.
- Dovresti avere SRA installato sia sul sito protetto che su quello di recovery.

**Passaggi**

1. Nella pagina iniziale del client vSphere, doppio click sull'icona **Ripristino sito** e quindi seleziona **Siti**.
2. Seleziona **Oggetti** > **Azioni** > **Associa siti**.
3. Nella finestra di dialogo **Associa server di Site Recovery Manager**, inserisci l'indirizzo del Platform Services Controller del sito protetto, quindi seleziona **Avanti**.
4. Nella sezione Seleziona vCenter Server, procedi come segue:
   a. Verifica che il server vCenter del sito protetto appaia come candidato corrispondente per l'accoppiamento.
   b. Inserisci le credenziali amministrative SSO e poi seleziona **Fine**.
5. Se richiesto, seleziona **Sì** per accettare i certificati di sicurezza.

**Risultato**

La finestra di dialogo **Oggetti** visualizza sia i siti protetti che quelli di recovery.

### Configura i gruppi di protezione

**Prima di iniziare**

Dovresti assicurarti che sia il sito di origine che quello di destinazione siano configurati come segue:

- Stessa versione di VMware Live Site Recovery installata
- Macchine virtuali
- Siti protetti e di recovery abbinati
- I datastore di origine e di destinazione devono essere montati sui rispettivi siti

**Passaggi**

1. Accedi al vCenter Server e seleziona **Ripristino del sito** > **Gruppi di protezione**.
2. Nel riquadro **Gruppi di protezione**, seleziona **Nuovo**.
3. Specifica un nome e una descrizione per il gruppo di protezione, la direzione e seleziona **Avanti**.
4. Nel campo **Tipo**, selezionare l'opzione **Tipo campo…** come gruppi di datastore (replica basata su array) per i datastore NFS e VMFS. Il dominio di errore è costituito da SVM con replica abilitata. Vengono visualizzati gli SVM che hanno implementato solo il peering e non presentano problemi.
5. Nella scheda Gruppi di replica, seleziona la coppia di array abilitata o i gruppi di replica che hanno la macchina virtuale che hai configurato, quindi seleziona **Avanti**.

   Tutte le macchine virtuali presenti nel gruppo di replica vengono aggiunte al gruppo di protezione.
6. Puoi selezionare un piano di recovery esistente oppure crearne uno nuovo selezionando **Aggiungi a un nuovo piano di recovery**.
7. Nella scheda Pronto per il completamento, rivedi i dettagli del gruppo di protezione che hai creato e poi seleziona **Fine**.

## Configura le risorse del sito protetto e del sito di ripristino

### Configurare le mappature di rete negli ONTAP tools

Dovresti configurare le mappature delle risorse, come reti VM, host ESXi e cartelle, su entrambi i siti per permettere la mappatura di ogni risorsa dal sito protetto alla risorsa appropriata nel sito di recovery.

Dovresti completare le seguenti configurazioni delle risorse:

- Mappature di rete
- Mappatura delle cartelle
- Mappature delle risorse
- Datastore segnaposto

**Prima di iniziare**

Dovresti aver collegato i siti protetto e di recovery.

**Passaggi**

1. Accedi al vCenter Server e seleziona **Ripristino del sito** > **Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Seleziona **Mappature di rete** > **Nuovo** nella scheda Gestisci per creare una nuova mappatura di rete.
4. Nella procedura guidata Crea mappatura di rete, fai quanto segue:
   a. Seleziona **Prepara automaticamente le mappature per le reti con nomi corrispondenti** e seleziona **Avanti**.
   b. Seleziona gli oggetti del data center necessari per i siti protetti e di recovery e seleziona **Aggiungi mappature**.
   c. Seleziona **Avanti** dopo che le mappature sono state create con successo.
   d. Seleziona l'oggetto utilizzato in precedenza per creare la mappatura inversa e poi seleziona **Finish**.

**Risultato**

La pagina Mappature di rete visualizza le risorse del sito protetto e le risorse del sito di ripristino. Puoi seguire gli stessi passaggi per le altre reti nel tuo ambiente.

### Configurare i mapping delle cartelle negli ONTAP tools

Dovresti mappare le cartelle sul sito protetto e sul sito di recovery per abilitare la comunicazione tra di loro.

**Prima di iniziare**

Dovresti aver collegato i siti protetto e di recovery.

**Passaggi**

1. Accedi al vCenter Server e seleziona **Ripristino del sito** > **Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Seleziona **Mappature cartelle** > icona **Cartella** nella scheda Gestisci per creare una nuova mappatura di cartella.

4. Nella procedura guidata Crea mappatura cartelle, esegui le seguenti operazioni:
    a. Seleziona **Prepara automaticamente le mappature per le cartelle con nomi corrispondenti** e seleziona **Avanti**.
    b. Seleziona gli oggetti del data center necessari per i siti protetti e di recovery e seleziona **Aggiungi mappature**.
    c. Seleziona **Avanti** dopo che le mappature sono state create con successo.
    d. Seleziona l'oggetto utilizzato in precedenza per creare la mappatura inversa e poi seleziona **Finish**.

**Risultato**

La pagina Mappature cartelle visualizza le risorse del sito protetto e le risorse del sito di ripristino. È possibile seguire gli stessi passaggi per le altre cartelle presenti nell'ambiente.

### Configurare le mappature delle risorse negli ONTAP tools

Dovresti mappare le tue risorse sul sito protetto e sul sito di ripristino in modo che le macchine virtuali siano configurate per eseguire il failover su un gruppo di host o sull'altro.

**Prima di iniziare**

Dovresti aver collegato i siti protetto e di recovery.

> In VMware Live Site Recovery, le risorse possono essere pool di risorse, host ESXi o vSphere cluster.

**Passaggi**

1. Accedi al vCenter Server e seleziona **Ripristino del sito** > **Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Seleziona **Mappature risorse** > **Nuovo** nella scheda Gestisci per creare una nuova mappatura delle risorse.
4. Nella procedura guidata Crea mappatura risorse, esegui le seguenti operazioni:
    a. Seleziona **Prepara automaticamente le mappature per le risorse con nomi corrispondenti** e seleziona **Avanti**.
    b. Seleziona gli oggetti del data center necessari per i siti protetti e di recovery e seleziona **Aggiungi mappature**.
    c. Seleziona **Avanti** dopo che le mappature sono state create con successo.
    d. Seleziona l'oggetto utilizzato in precedenza per creare la mappatura inversa e poi seleziona **Finish**.

**Risultato**

La pagina Mappatura risorse visualizza le risorse del sito protetto e le risorse del sito di ripristino. È possibile seguire gli stessi passaggi per le altre risorse presenti nell'ambiente.

### Configurare i datastore segnaposto negli ONTAP tools

Configura un datastore segnaposto per riservare spazio nell'inventario di vCenter nel sito di recovery per le macchine virtuali (VM) protette. I datastore segnaposto richiedono una capacità minima, perché le VM segnaposto sono piccole e di solito usano solo poche

centinaia di kilobyte.

**Prima di iniziare**

- Assicurati che i siti protetti e di recovery siano collegati.
- Verifica che le mappature delle risorse siano state configurate.

**Passaggi**

1. Accedi al vCenter Server e seleziona **Ripristino del sito** > **Siti**.
2. Seleziona il tuo sito protetto e seleziona **Gestisci**.
3. Nella scheda Gestisci, seleziona **Placeholder Datastores** > **New** per creare un nuovo placeholder datastore.
4. Seleziona l'archivio dati appropriato e seleziona **OK**.

> I datastore segnaposto possono risiedere su storage locale o remoto, ma non richiedono la replica.

5. Ripeti i passaggi da 3 a 5 per configurare un datastore segnaposto per il sito di recovery.

**Configurare SRA utilizzando il gestore array in ONTAP tools**

Puoi configurare Storage Replication Adapter (SRA) usando la procedura guidata Array Manager di VMware Live Site Recovery per abilitare le interazioni tra VMware Live Site Recovery e le macchine virtuali di storage (SVM).

**Prima di iniziare**

- Dovresti aver associato i siti protetti e i siti di recovery in VMware Live Site Recovery.
- Dovresti aver configurato lo storage integrato prima di configurare l'array manager.
- Dovresti aver configurato e replicato le relazioni di SnapMirror tra i siti protetti e i siti di recovery.
- Dovresti aver abilitato i LIF di gestione SVM per abilitare il multitenancy.

SRA supporta la gestione a livello di cluster e la gestione a livello di SVM. Se aggiungi storage a livello di cluster, puoi individuare ed eseguire operazioni su tutte le SVM presenti nel cluster. Se aggiungi storage a livello di SVM, puoi gestire solo quella specifica SVM.

**Passaggi**

1. In VMware Live Site Recovery, seleziona **Gestori array** > **Aggiungi gestore array**.
2. Inserisci le seguenti informazioni per descrivere l'array in VMware Live Site Recovery:
    a. Inserisci un nome per identificare il gestore dell'array nel campo **Nome visualizzato**.
    b. Nel campo **Tipo SRA**, seleziona **NetApp Storage Replication Adapter for ONTAP**.
    c. Inserisci le informazioni per connetterti al cluster o all'SVM:
        - Se ti stai connettendo a un cluster, dovresti inserire la LIF di gestione del cluster.
        - Se ti connetti direttamente a un SVM, devi immettere l'indirizzo IP del LIF di gestione dell'SVM.

Quando configuri l'array manager, dovresti usare la stessa connessione (indirizzo IP) per il sistema storage che hai usato per l'onboarding del sistema storage in ONTAP tools for VMware vSphere. Ad esempio, se la configurazione dell'array manager è a livello SVM, allora lo storage sotto ONTAP tools for VMware vSphere dovrebbe essere aggiunto a livello SVM.

d. Se ti connetti a un cluster, specifica il nome dell'SVM nel campo **Nome SVM** oppure lascialo vuoto per gestire tutti gli SVM del cluster.

e. Inserisci i volumi da rilevare nel campo **Volume include list**.

   Puoi inserire il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di recovery.

   Ad esempio, se vuoi individuare il volume src_vol1 che è in una relazione di SnapMirror con il volume dst_vol1, dovresti specificare src_vol1 nel campo del sito protetto e dst_vol1 nel campo del sito di recovery.

f. **(Facoltativo)** Inserisci i volumi da escludere dalla discovery nel campo **Volume exclude list**.

   Puoi inserire il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di recovery.

Ad esempio, se vuoi escludere il volume *src_vol1* che è in una relazione di SnapMirror con il volume *dst_vol1*, dovresti specificare *src_vol1* nel campo del sito protetto e *dst_vol1* nel campo del sito di recovery.

3. Seleziona **Avanti**.
4. Verifica che l'array venga rilevato e visualizzato nella parte inferiore della finestra Aggiungi gestore array e seleziona **Fine**.

Puoi seguire gli stessi passaggi per il sito di recovery utilizzando gli indirizzi IP di gestione SVM e le credenziali appropriate. Nella schermata Abilita coppie di array della procedura guidata Aggiungi gestore array, dovresti verificare che sia selezionata la coppia di array corretta e che risulti pronta per essere abilitata.

## Verificare i sistemi di archiviazione replicati negli ONTAP tools

Dovresti verificare che il sito protetto e il sito di ripristino siano stati associati correttamente dopo aver configurato Storage Replication Adapter (SRA). Il sistema storage replicato deve essere rilevabile sia dal sito protetto che dal sito di ripristino.

**Prima di iniziare**

- Dovresti aver configurato il tuo sistema storage.
- Dovresti aver associato il sito protetto e il sito di ripristino utilizzando VMware Live Site Recovery array manager.
- Dovresti aver abilitato la licenza FlexClone e la licenza SnapMirror prima di eseguire l'operazione di test failover e l'operazione di failover per SRA.
- Dovresti avere le stesse politiche e pianificazioni SnapMirror sia sul sito di origine che su quello di destinazione.
- Se si utilizzano criteri SnapMirror personalizzati con una pianificazione personalizzata, è necessario configurare la stessa pianificazione e gli stessi criteri sia sul sito protetto che su quello di ripristino.
- Se si utilizzano criteri SnapMirror personalizzati (con pianificazione predefinita o personalizzata), è

necessario eseguire il rilevamento dello storage dagli strumenti ONTAP affinché il nuovo criterio venga riconosciuto. In caso contrario, i flussi di lavoro SRA, inclusi il failover di test e il failover effettivo, non andranno a buon fine. Eseguire il rilevamento dello storage nei seguenti punti:

- Dopo aver creato i criteri personalizzati sul sito di ripristino.
- Dopo un'operazione di riprotezione, che ricrea i criteri sul sito protetto.

**Passaggi**

1. Accedi al tuo vCenter Server.
2. Vai su **Ripristino del sito** > **Replica basata su array**.
3. Seleziona la coppia di array richiesta e verifica i dettagli corrispondenti.

   I sistemi di archiviazione dovrebbero essere rilevati nel sito protetto e nel sito di ripristino con lo stato **Enabled**.

## Protezione fan-out negli ONTAP tools

In uno scenario di protezione fan-out, il gruppo di coerenza è protetto due volte: con una relazione sincrona sul primo cluster ONTAP di destinazione e con una relazione asincrona sul secondo cluster ONTAP di destinazione. I workflow di creazione, modifica ed eliminazione della protezione SnapMirror active sync mantengono la protezione sincrona. I workflow di failover e riprotezione dell'appliance VMware Live Site Recovery mantengono la protezione asincrona.

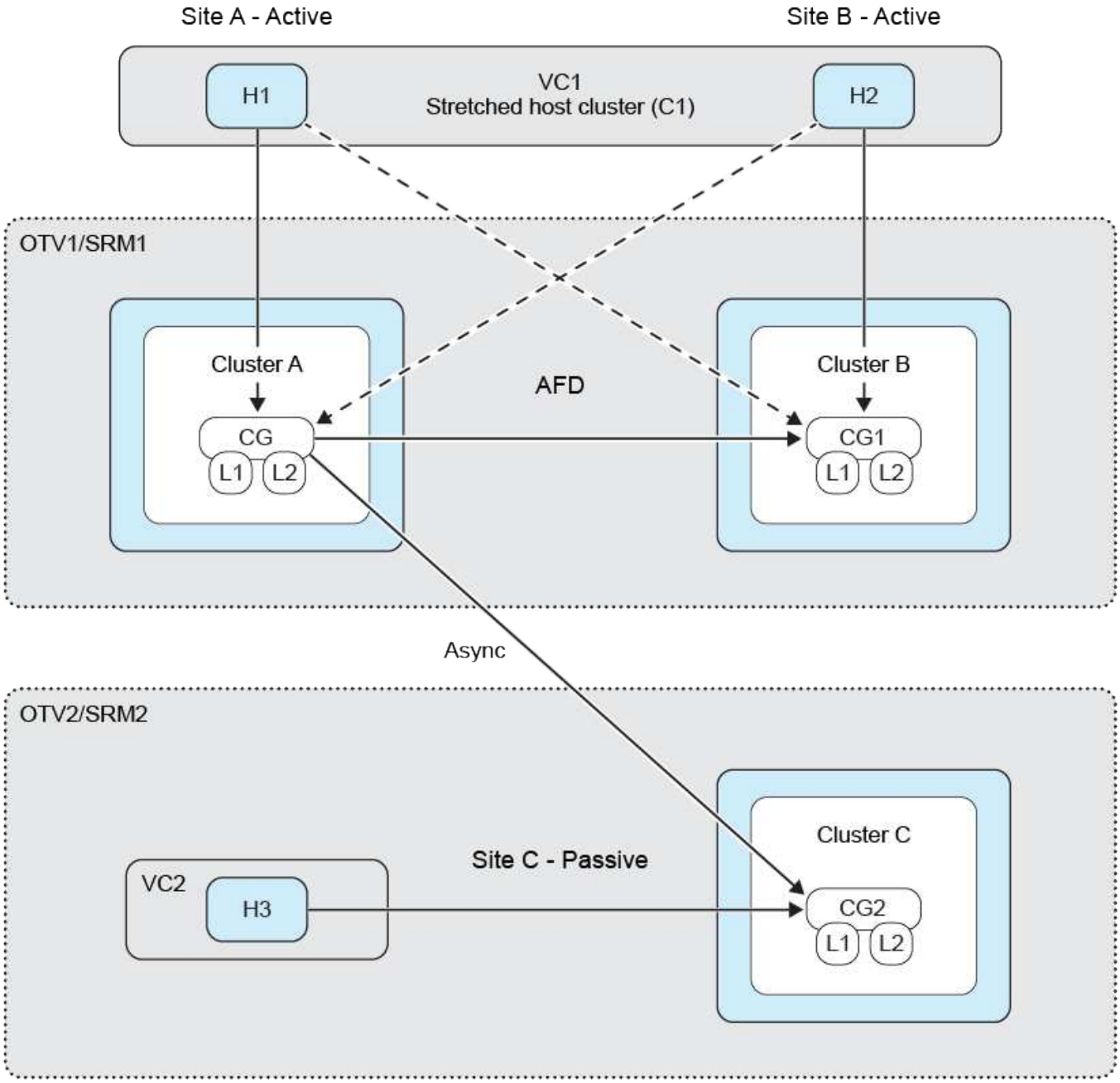
La funzionalità fan-out non è supportata per gli utenti SVM.

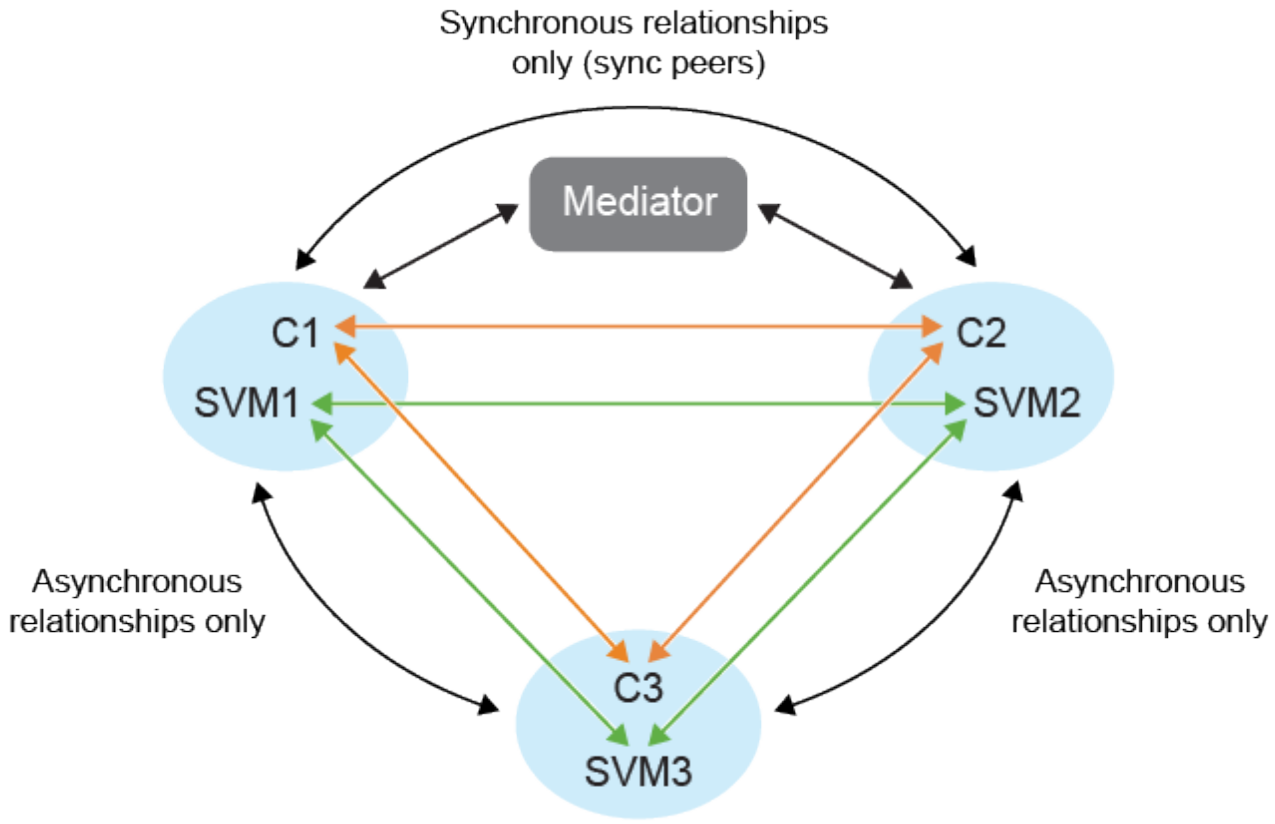
Per configurare la protezione fan-out, effettua il peering tra i tre cluster del sito e gli SVM.

Esempio:

| Se | Poi |
|---|---|
| • Il gruppo di coerenza della fonte si trova sul cluster c1 e sulla SVM svm1<br>• Il primo gruppo di coerenza di destinazione si trova sul cluster c2 e sull'SVM svm2 e<br>• Il secondo gruppo di coerenza di destinazione si trova sul cluster c3 e sull'SVM svm3 | • Il peering del cluster sul cluster ONTAP di origine sarà (C1, C2) e (C1, C3).<br>• Il cluster peering sul primo cluster di destinazione ONTAP sarà (C2, C1) e (C2, C3) e<br>• Il peering del cluster sul secondo cluster di destinazione ONTAP sarà (C3, C1) e (C3, C2).<br>• Il peering SVM sull'SVM sorgente sarà (svm1, svm2) e (svm1, svm3).<br>• Il peering SVM sulla prima SVM di destinazione sarà (svm2, svm1) e (svm2, svm3) e<br>• Il peering SVM sulla seconda SVM di destinazione sarà (svm3, svm1) e (svm3, svm2). |

Il diagramma seguente mostra la configurazione della protezione fan-out:


Site A - Active
Site B - Active
VC1
Stretched host cluster (C1)
H1
H2
OTV1/SRM1
Cluster A
AFD
Cluster B
CG
L1
L2
CG1
L1
L2
Async
OTV2/SRM2
Cluster C
Site C - Passive
VC2
H3
CG2
L1
L2




**Passaggi**

1. Selezionare un nuovo archivio dati segnaposto. I criteri di selezione dell'archivio dati segnaposto per la protezione graduale sono:
   - Non posizionare il datastore segnaposto nel cluster che stai proteggendo.
   - Se è necessario includere il datastore segnaposto nel cluster host, aggiungerlo all'appliance VMware Live Site Recovery prima di configurare la protezione della sincronizzazione attiva SnapMirror. Con questa configurazione, è possibile escludere il datastore segnaposto dalla protezione.

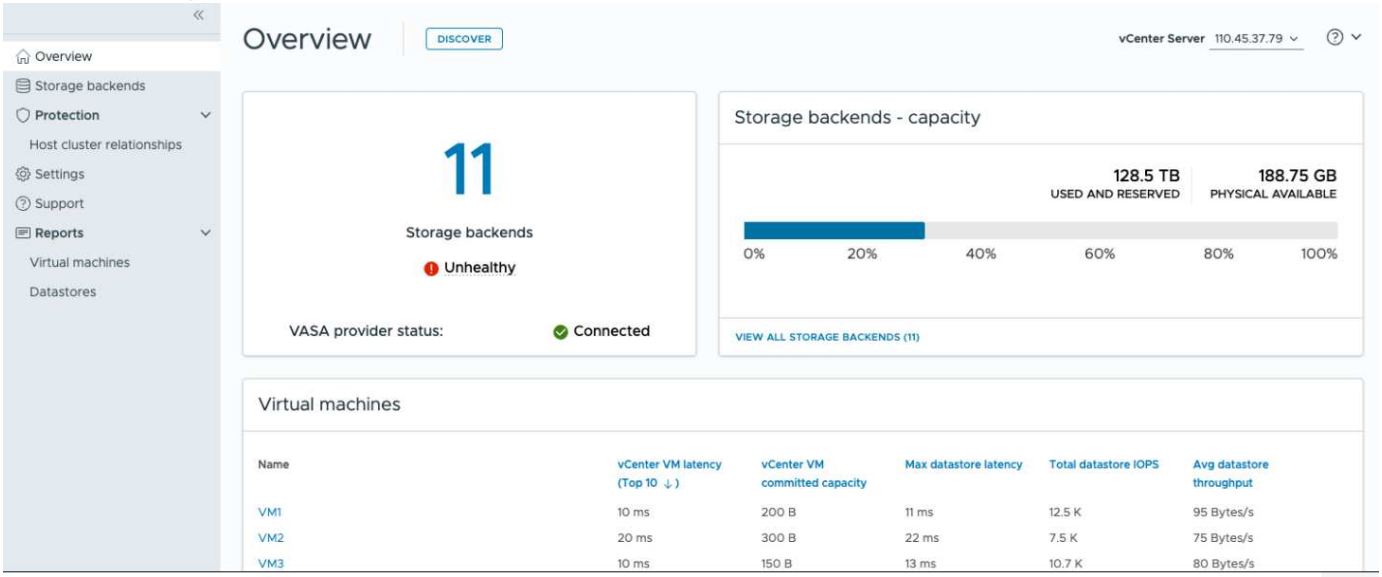
     Per ulteriori informazioni, fare riferimento a "Seleziona un datastore segnaposto"
2. Aggiungere i datastore alla protezione del cluster host seguendo "Modifica cluster protetto". Aggiungere sia i tipi di policy asincroni che sincroni.

# Gestisci ONTAP tools for VMware vSphere

## Scopri la dashboard degli strumenti ONTAP

Selezionando l'icona del plug-in ONTAP tools per VMware vSphere dalla sezione dei collegamenti rapidi nel client vCenter si apre la pagina di panoramica. Questa dashboard fornisce un riepilogo del plug-in ONTAP tools per VMware vSphere.

In modalità Enhanced Linked Mode (ELM), viene visualizzato il menu a tendina vCenter Server. Scegli un vCenter Server per visualizzarne i dati. Il menu a tendina è disponibile in tutte le visualizzazioni elenco del plug-in. Quando selezioni un vCenter Server in una pagina, la selezione rimane invariata anche quando cambi scheda nel plug-in.




Dalla pagina di panoramica, puoi eseguire l'azione **Rilevamento**. L'azione di rilevamento individua i backend di storage, gli host, i datastore e lo stato o le relazioni di protezione aggiunti o aggiornati di recente a livello di vCenter. Esegui il rilevamento su richiesta senza attendere quello pianificato.

Il pulsante **Rilevamento** è abilitato solo se si dispone del privilegio necessario per eseguire il rilevamento.

Dopo aver inviato la richiesta di rilevamento, puoi monitorare lo stato di avanzamento dell'azione nel pannello delle attività recenti.

Il pannello di controllo contiene diverse schede che mostrano differenti elementi del sistema. La tabella seguente mostra le diverse schede e cosa rappresentano.

| Scheda | Descrizione |
| --- | --- |

| | |
|---|---|
| Stato | La scheda Stato mostra il numero di backend di archiviazione e lo stato di salute generale dei backend di archiviazione e del VASA Provider. Lo stato dei backend di archiviazione viene visualizzato come **Integro** quando tutti gli stati dei backend di archiviazione sono normali e come **Non integro** se uno qualsiasi dei backend di archiviazione presenta un problema (stato Sconosciuto/Irraggiungibile/Degradato). Seleziona il tool tip per aprire i dettagli sullo stato dei backend di archiviazione. Puoi selezionare qualsiasi backend di archiviazione per maggiori dettagli. Il collegamento **Altri stati del VASA Provider** mostra lo stato corrente del VASA Provider registrato nel vCenter Server. |
| Backend di storage - Capacità | Questa scheda mostra la capacità aggregata utilizzata e disponibile di tutti i backend di storage per l'istanza del server vCenter selezionata. Per i sistemi di storage ASA r2, i dati relativi alla capacità non vengono visualizzati perché lo storage è disaggregato. |
| Macchine virtuali | Questa scheda mostra le 10 migliori VM ordinate in base a una metrica di prestazioni. Puoi selezionare l'intestazione per visualizzare le 10 migliori VM per la metrica selezionata, ordinate in ordine crescente o decrescente. Le modifiche di ordinamento e filtro apportate alla scheda persistono finché non cambi o cancelli la cache del browser. |
| Datastore | Questa scheda mostra i 10 principali datastore ordinati in base a una metrica delle prestazioni. Puoi selezionare l'intestazione per ottenere i 10 principali datastore per la metrica selezionata, ordinati in ordine crescente o decrescente. Le modifiche di ordinamento e filtro apportate alla scheda persistono finché non cambi o cancelli la cache del browser. È presente un menu a discesa Tipo di datastore per selezionare il tipo di datastore: NFS, VMFS o vVols. |
| Scheda di conformità host ESXi | Questa scheda mostra se tutti gli host ESXi (per il vCenter selezionato) seguono le impostazioni host consigliate NetApp per gruppo o categoria. È possibile selezionare il collegamento **Applica impostazioni consigliate** per applicare le impostazioni consigliate. È possibile selezionare lo stato di conformità degli host per visualizzare l'elenco degli host. |

# Come ONTAP tools gestisce gli igroup e le policy di esportazione

I gruppi di iniziatori (igroup) sono tabelle di World Wide Port Name (WWPN) dell'host del protocollo FC o di nomi di nodo qualificati dell'host iSCSI. Puoi definire gli igroup e

mapparli alle LUN per controllare quali iniziatori hanno accesso alle LUN.

In ONTAP tools for VMware vSphere 9.x, gli igroup venivano creati e gestiti in una struttura piatta, in cui ogni datastore in vCenter era associato a un singolo igroup. Questo modello limitava la flessibilità e il riutilizzo degli igroup tra più datastore. ONTAP tools for VMware vSphere introduce gli igroup nidificati, in cui ogni datastore in vCenter è associato a un igroup padre, mentre ogni host è collegato a un igroup figlio sotto quel padre. Puoi definire igroup padre personalizzati con nomi scelti dall'utente per riutilizzarli tra i datastore e rendere più semplice la gestione degli igroup. Comprendi il flusso di lavoro degli igroup per gestire LUN e datastore in ONTAP tools for VMware vSphere. Flussi di lavoro diversi generano configurazioni di igroup differenti, come mostrato nei seguenti esempi:

> I nomi menzionati sono solo a scopo illustrativo e non si riferiscono a nomi di igroup reali. Gli igroup gestiti da ONTAP tools utilizzano il prefisso "otv_". Agli igroup personalizzati può essere assegnato qualsiasi nome.

| Termine | Descrizione |
|---|---|
| DS<number> | Datastore |
| iqn<number> | IQN dell'iniziatore |
| host<number> | Host MoRef |
| lun<number> | ID LUN |
| <DSName>Igroup<number> | Gruppo igroup padre predefinito (gestito da ONTAP tools) |
| <Host-Moref>Igroup<number> | Gruppo igroup figlio |
| CustomIgroup<number> | igroup padre personalizzato definito dall'utente |
| ClassicIgroup<number> | Igroup utilizzato nelle versioni 9.x degli ONTAP tools. |

**Esempio 1:**

Crea un datastore su un singolo host con un solo initiator

**Flusso di lavoro**: [Create] DS1 (lun1): host1 (iqn1)

**Risultato**:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)

ONTAP crea l'igroup padre DS1Igroup per DS1 e mappa l'igroup figlio host1Igroup a lun1. Il sistema mappa sempre le LUN agli igroup figli.

**Esempio 2:**

Monta il datastore esistente su un host aggiuntivo

**Workflow**: [Mount] DS1 (lun1): host2 (iqn2)

**Risultato**:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)

    - host2Igroup → (iqn2: lun1)

Gli strumenti ONTAP per VMware vSphere creano un igroup figlio host2Igroup e lo aggiungono all'igroup padre esistente DS1Igroup.

**Esempio 3:**

Smonta un datastore da un host

**Flusso di lavoro**: [Unmount] DS1 (lun1): host1 (iqn1)

**Risultato**:

- DS1Igroup:
    - host2Igroup → (iqn2: lun1)

ONTAP tools for VMware vSphere rimuovono host1Igroup dalla gerarchia. Il sistema non elimina esplicitamente gli igroup figli. Li elimina in presenza di queste due condizioni:

- Se non sono mappate LUN, il sistema ONTAP elimina l'igroup figlio.
- Un'attività di pulizia pianificata rimuove gli igroup figlio orfani privi di mappature LUN. Questi scenari si applicano solo agli igroup gestiti da ONTAP tools, non a quelli creati su misura.

**Esempio 4:**

Elimina il datastore

**Flusso di lavoro**: [Elimina] DS1 (lun1): host2 (iqn2)

**Risultato**:

- DS1Igroup:
    - host2Igroup → (iqn2: lun1)

Gli igroup padre e figlio vengono rimossi a meno che un altro datastore non riutilizzi l'igroup padre. Gli igroup figlio non vengono eliminati esplicitamente

**Esempio 5:**

Crea più datastore sotto un igroup padre personalizzato

**Flusso di lavoro**:

- [Crea] DS2 (lun2): host1 (iqn1), host2 (iqn2)
- [Crea] DS3 (lun3): host1 (iqn1), host3 (iqn3)

**Risultato**:

- CustomIgroup1:
    - host1Igroup → (iqn1: lun2, lun3)
    - host2Igroup → (iqn2: lun2)
    - host3Igroup → (iqn3: lun3)

CustomIgroup1 viene creato per DS2 e riutilizzato per DS3. Gli igroup figli vengono creati o aggiornati sotto l'igroup padre condiviso, con ogni igroup figlio mappato alle relative LUN.

**Esempio 6:**

Elimina un datastore sotto un igroup padre personalizzato.

**Flusso di lavoro**: [Elimina] DS2 (lun2): host1 (iqn1), host2 (iqn2)

**Risultato**:

- CustomIgroup1:
  - host1Igroup → (iqn1: lun3)
  - host3Igroup → (iqn3: lun3)
- Anche se CustomIgroup1 non viene riutilizzato, non viene eliminato.
- Se non sono mappate LUN, il sistema ONTAP elimina host2Igroup.
- host1Igroup non viene eliminato perché è mappato a lun3 di DS3. Gli igroup personalizzati non vengono mai eliminati, indipendentemente dallo stato di riutilizzo.

**Esempio 7:**

Espandi il datastore vVols (Aggiungi volume)

**Flusso di lavoro**:

Prima dell'espansione:

[Espandi] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

Dopo l'espansione:

[Espandi] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

Viene creato un nuovo LUN e mappato all'igroup figlio esistente host4Igroup.

**Esempio 8:**

Riduci il datastore vVols (Rimuovi volume)

**Flusso di lavoro**:

Prima del restringimento:

[Riduci] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

Dopo il restringimento:

[Riduci] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

La LUN specificata (lun5) viene scollegata dall'igroup figlio. L'igroup rimane attivo finché ha almeno una LUN mappata.

**Esempio 9:**

Migrazione da ONTAP tools 9 a 10 (normalizzazione igroup)

**Flusso di lavoro**

Gli ONTAP tools for VMware vSphere versioni 9.x non supportano gli igroup gerarchici. Durante la migrazione alle versioni 10.3 o successive, gli igroup devono essere normalizzati nella struttura gerarchica.

Prima della migrazione:

[Migrazione] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

La logica di ONTAP tools 9.x consente più initiator per igroup senza imporre una mappatura host uno a uno.

Dopo la migrazione:

[Migrazione] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → ClassicIgroup1: otv_ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

Durante la migrazione:

- Viene creato un nuovo igroup padre (ClassicIgroup1).
- L'igroup originale viene rinominato con il prefisso otv_ e diventa un igroup figlio.

Questo garantisce la conformità al modello gerarchico.

A partire da ONTAP tools 10.5P2, gli igroup migrati vengono eliminati quando non sono più in uso. Nelle versioni precedenti, gli igroup migrati non venivano mai rimossi. Nota quanto segue:

- Gli igroup migrati non possono essere riutilizzati tra datastore diversi.
- Gli igroup personalizzati (definiti dall'utente) non vengono mai eliminati e possono essere riutilizzati.

**Argomenti correlati**

"Informazioni sugli igroups"

## Politiche di esportazione

Le policy di esportazione controllano l'accesso ai datastore NFS e le autorizzazioni dei client in ONTAP tools for VMware vSphere. Le policy di esportazione vengono create e gestite nei sistemi ONTAP e possono essere utilizzate con i datastore NFS per imporre il controllo degli accessi. Ogni policy di esportazione è composta da regole che specificano i client (indirizzi IP o subnet) a cui è consentito l'accesso e le autorizzazioni concesse (sola lettura o lettura/scrittura).

Quando crei un datastore NFS in ONTAP tools for VMware vSphere, puoi selezionare una policy di esportazione esistente o crearne una nuova. La policy di esportazione viene quindi applicata al datastore, assicurando che solo i client autorizzati possano accedervi.

Quando monti un datastore NFS su un nuovo host ESXi, ONTAP tools per VMware vSphere aggiunge l'indirizzo IP dell'host alla policy di esportazione associata al datastore. Questo permette al nuovo host di accedere al datastore senza creare una nuova policy di esportazione.

Quando elimini o smonti un datastore NFS da un host ESXi, ONTAP tools for VMware vSphere rimuove l'indirizzo IP dell'host dalla policy di esportazione. Se nessun altro host utilizza quella policy di esportazione, verrà eliminata. Quando elimini un datastore NFS, ONTAP tools for VMware vSphere rimuove la policy di

esportazione associata a quel datastore se non viene riutilizzata da altri datastore. Se la policy di esportazione viene riutilizzata, mantiene l'indirizzo IP dell'host e non cambia. Quando elimini i datastore, la policy di esportazione rimuove l'indirizzo IP dell'host e assegna una policy di esportazione predefinita, così che i sistemi ONTAP possano accedervi se necessario.

L'assegnazione della policy di esportazione è diversa quando viene riutilizzata tra diversi datastore. Quando riutilizzi la policy di esportazione, puoi aggiungere il nuovo indirizzo IP dell'host alla policy. Quando elimini o smonti un datastore che utilizza una policy di esportazione condivisa, la policy non viene eliminata. Rimane invariata e l'indirizzo IP dell'host non viene rimosso, perché è condiviso con gli altri datastore. Non è consigliato riutilizzare le policy di esportazione, perché può causare problemi di accesso e di latenza.

**Argomenti correlati**

"Creare una policy di esportazione"

# Come ONTAP tools gestisce gli igroup

Se gestisci sia le macchine virtuali ONTAP tools che i sistemi di storage ONTAP, è importante comprendere il comportamento degli igroup, soprattutto quando si spostano datastore da ambienti non gestiti da ONTAP tools a quelli che lo sono. Questa pagina spiega come ONTAP tools per VMware vSphere rappresenta e gestisce gli igroup. Si tratta di informazioni concettuali utili per comprendere le differenze di comportamento tra le versioni precedenti e l'attuale modello di igroup annidato.

A partire da ONTAP tools for VMware vSphere 10.4, ONTAP tools for VMware crea e gestisce automaticamente oggetti ONTAP e vCenter, semplificando la gestione dei datastore negli ambienti datacenter VMware. A partire da ONTAP tools for VMware vSphere 10.5 P2, anche gli igroup migrati vengono eliminati automaticamente quando non sono più in uso.

## Riepilogo rapido del comportamento

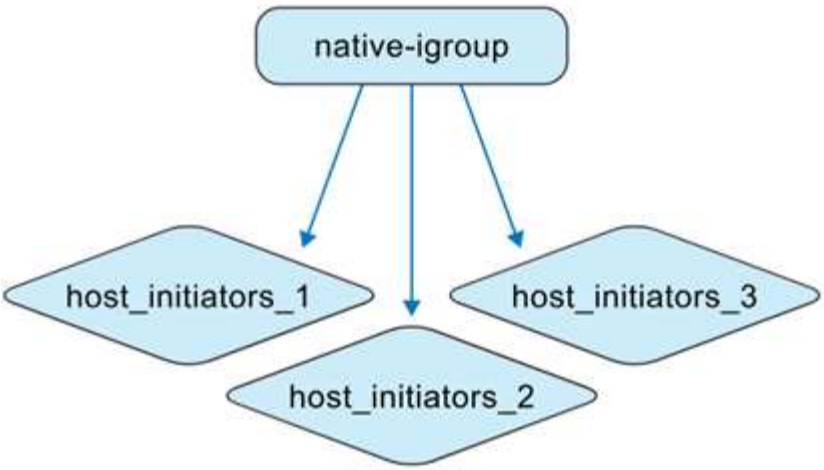
- I datastore VMFS gestiti dagli strumenti ONTAP utilizzano igroup nidificati: un igroup padre per ogni contesto di datastore e igroup figli per ogni host.
- Le mappature LUN vengono applicate agli igroup figli.
- Gli igroup padre personalizzati possono essere riutilizzati in diversi datastore.
- Gli igroup migrati da ONTAP tools 9.x non possono essere riutilizzati.

## Contesti di gruppo

ONTAP tools for VMware vSphere gestisce gli igroup in due contesti.

**Igroup gestiti da strumenti non ONTAP**

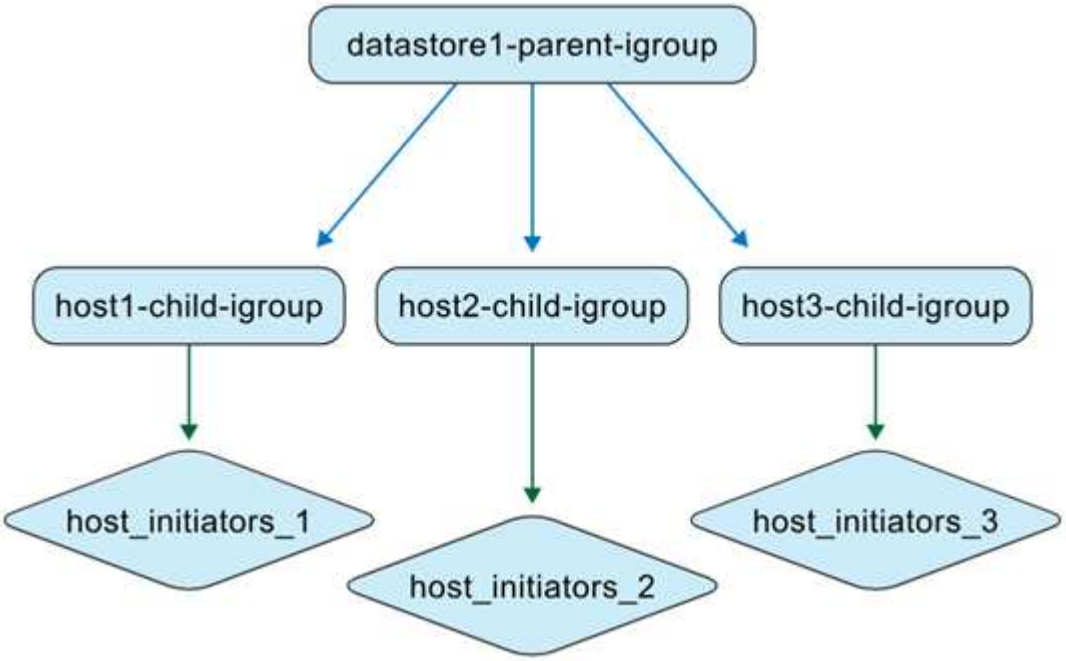
In qualità di amministratore dello storage, puoi creare igroup sul sistema ONTAP come strutture piatte o nidificate. L'illustrazione seguente mostra un igroup piatto creato direttamente in ONTAP.

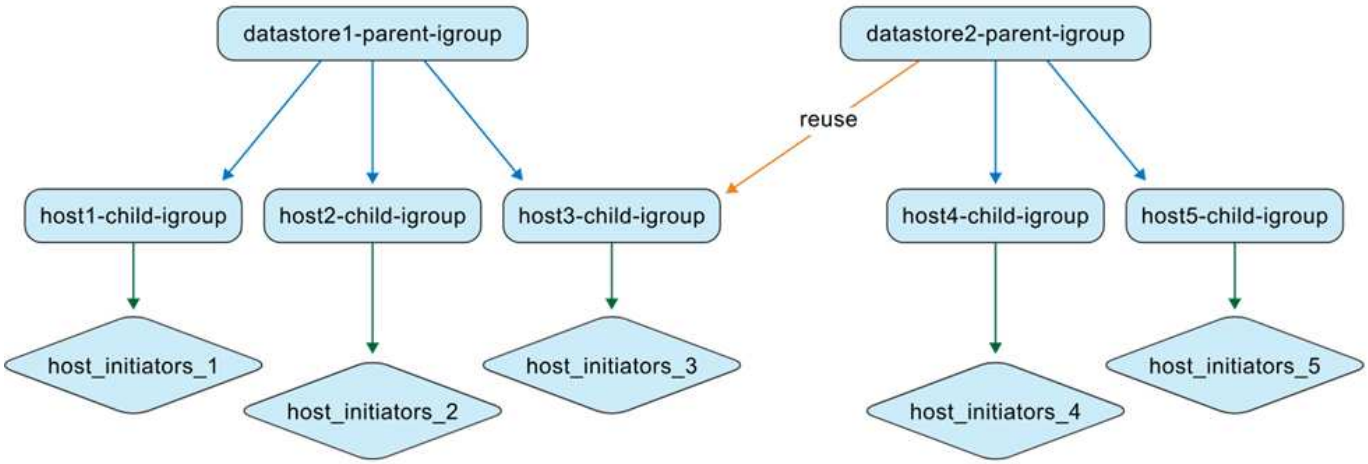



**igroup gestiti da ONTAP tools**

Quando si creano datastore, ONTAP tools for VMware vSphere crea igroups in una struttura annidata.

Ad esempio, quando datastore1 viene creato e montato sugli host 1, 2 e 3, e un nuovo datastore (datastore2) viene creato e montato sugli host 3, 4 e 5, ONTAP tools riutilizza l'igroup a livello di host per una gestione efficiente.






## Comportamento di denominazione

Quando si crea un datastore e si lascia vuoto il campo igroup, ONTAP tools crea una struttura igroup nidificata predefinita.

- Schema di denominazione dell'igroup padre: `otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>`
- Schema di denominazione degli igroup figlio: `otv_<hostMoref>_<vcguid>`

L'interfaccia di sistema ONTAP mostra la relazione tra igroup padre e figlio nel campo **Gruppo iniziatore padre**.

## Comportamento in base allo scenario

| Scenario | Comportamento del gruppo igroup genitore | Comportamento del gruppo figlio | Mappatura e visibilità delle LUN |
|---|---|---|---|
| Datastore creato con l'impostazione predefinita dell'igroup | Viene creato un igroup padre predefinito gestito dagli ONTAP tools. | Gli igroup figlio a livello host vengono creati secondo necessità. | Le LUN vengono mappate agli igroup figlio. Il datastore viene visualizzato nell'inventario del server vCenter. |
| Datastore creato con nome igroup personalizzato | Viene creato un igroup padre personalizzato con il nome specificato. | Gli igroup figlio a livello host esistenti vengono riutilizzati quando gli host si sovrappongono. | Il nuovo LUN del datastore viene mappato all'igroup figlio riutilizzato o appena creato. Il datastore appare in vCenter Server. |
| Gruppo igroup personalizzato esistente riutilizzato durante la creazione del datastore | Viene selezionato e riutilizzato un igroup padre personalizzato esistente. | Gli igroup figlio vengono riutilizzati o estesi in base all'appartenenza all'host. | Il nuovo LUN del datastore viene mappato tramite l'igroup figlio associato. Il datastore appare in vCenter Server. |

| Scenario | Comportamento del gruppo igroup genitore | Comportamento del gruppo figlio | Mappatura e visibilità delle LUN |
|---|---|---|---|
| Datastore e igroup creati nativamente in ONTAP e vCenter, quindi rilevati dagli ONTAP tools | ONTAP tools crea un igroup padre nel proprio contesto di gestione e mantiene il nome originale dell'igroup. | ONTAP tools rinomina l'igroup originale con il `otv_` prefix e lo rappresenta come igroup figlio nella gerarchia. | Le mappature degli initiator rimangono invariate. Solo gli igroups mappati ai datastores vengono convertiti durante il rilevamento. |

## Riutilizzo personalizzato degli igroup e comportamento delle API

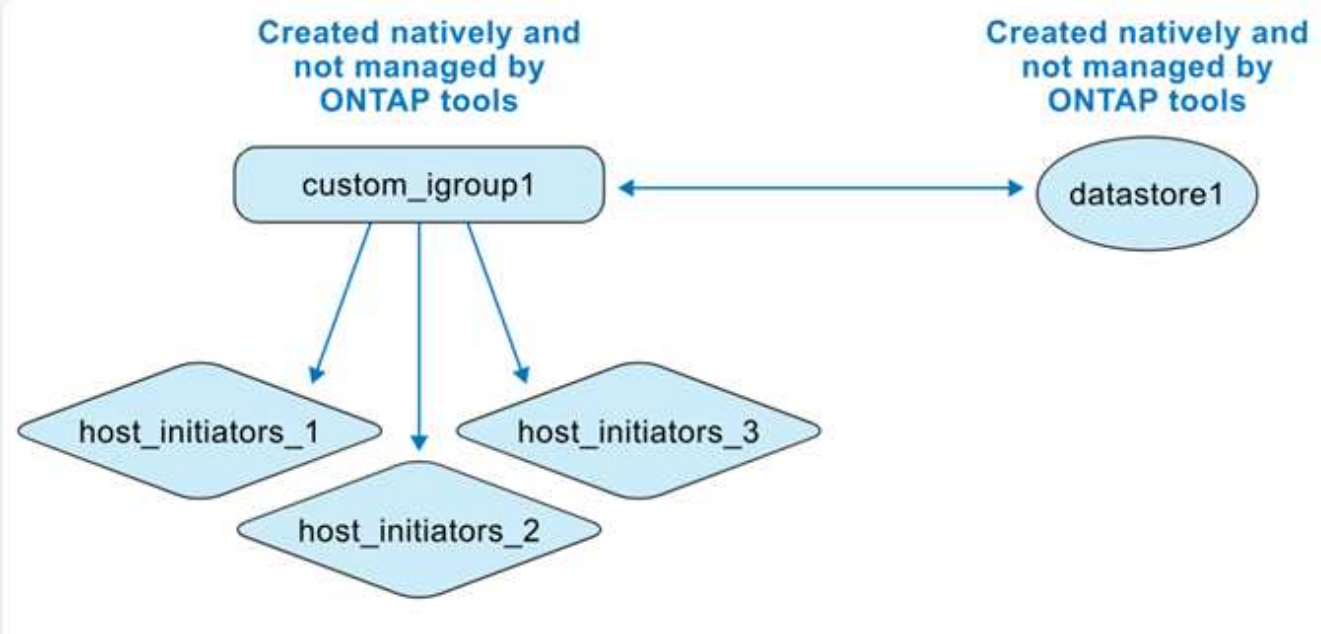
Nell'interfaccia utente degli strumenti ONTAP, è possibile riutilizzare un igroup padre personalizzato esistente dall'elenco a discesa durante la creazione di un datastore.

Lo stesso comportamento è supportato tramite API. Per riutilizzare un igroup esistente durante la creazione del datastore, fornire l'UUID dell'igroup nella richiesta payload dell'API.

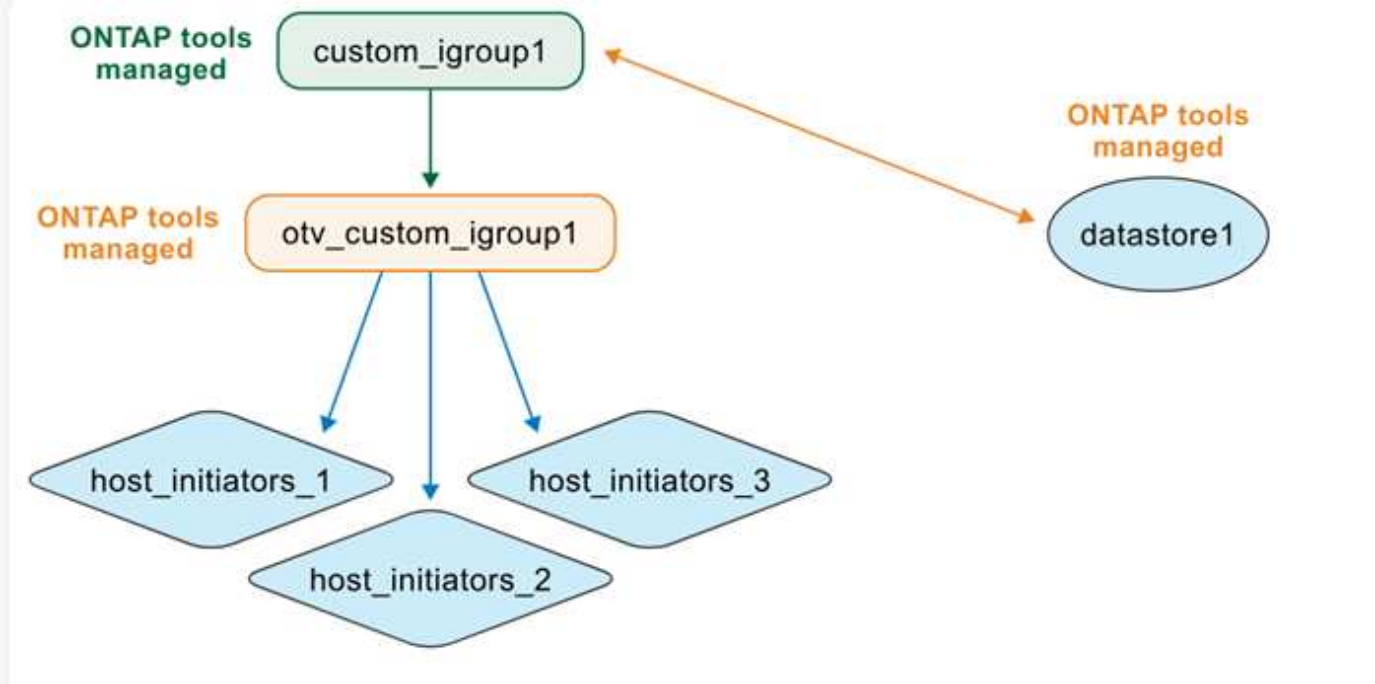
ⓘ È possibile riutilizzare solo gli igroup personalizzati. Gli igroup migrati da ONTAP tools 9.x non possono essere riutilizzati e, a partire da ONTAP tools 10.5 P2, vengono eliminati automaticamente quando non sono più in uso.

## Vista di conversione da nativo a gestito

Se si creano igroup e datastore direttamente nei sistemi ONTAP e negli ambienti VMware, ONTAP tools inizialmente non gestisce questi oggetti. Ciò si traduce in una struttura igroup piatta.




Dopo il rilevamento del datastore, ONTAP tools identifica e registra gli igroup mappati al datastore, quindi li rappresenta in un modello annidato. L'igroup padre è rappresentato a livello di datastore, l'igroup esistente viene rinominato con il `otv_` prefisso come igroup figlio e le mappature dell'initiator rimangono invariate.




ONTAP tools for VMware vSphere non rileva né gestisce gli igroup creati nei sistemi ONTAP ma non mappati a un datastore o collegati a ONTAP tools. Durante la fase di rilevamento, ONTAP tools converte solo gli igroup mappati ai datastore rilevati; gli altri igroup rimangono non gestiti.

### Riutilizzo degli igroup nativi scoperti

Dopo che ONTAP tools gestisce un igroup nativo rilevato, tale igroup è disponibile nell'elenco a discesa del nome del gruppo initiator personalizzato per la creazione del datastore.

Il nuovo LUN del datastore viene mappato all'igroup figlio normalizzato, ad esempio, `otv_NativeIgroup1`.

ONTAP tools for VMware vSphere non rileva né utilizza gli igroups creati nei sistemi ONTAP che non sono gestiti da ONTAP tools o non sono collegati a un datastore.

# Scopri l'interfaccia utente di ONTAP tools Manager

ONTAP tools for VMware vSphere supporta il multi-tenancy, permettendo la gestione di più istanze di vCenter Server.

ONTAP tools Manager è una console basata sul web per gestire ONTAP tools per VMware vSphere, vCenter Server, backend di storage e configurazione dell'appliance come High Availability (HA) e il dimensionamento dei nodi.

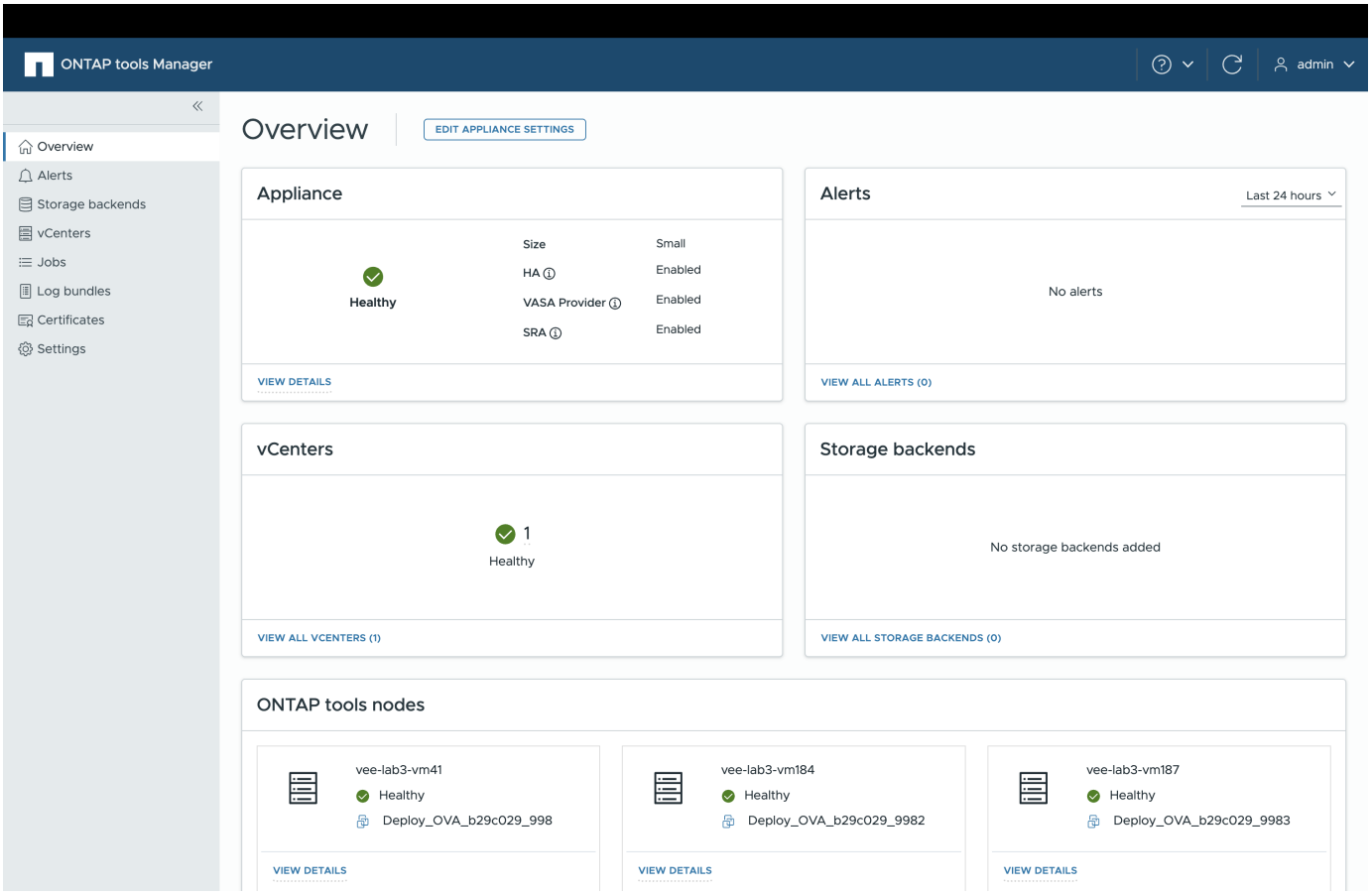
ONTAP tools Manager offre le seguenti funzionalità:

- Gestisci gli avvisi: visualizza e filtra gli avvisi generati dagli ONTAP tools for VMware vSphere.
- Gestisci i backend di storage: aggiungi e gestisci i cluster di storage ONTAP e mappali alle istanze del server vCenter a livello globale.
- Gestisci le istanze del server vCenter - aggiungi e gestisci le istanze del server vCenter all'interno degli ONTAP tools.
- Monitora i processi: monitora ed esegui il debug dei processi asincroni avviati sia dall'interfaccia del plug-in

ONTAP tools che dall'interfaccia di ONTAP tools Manager. Puoi filtrare i processi per periodo di tempo, regolare la dimensione della pagina e visualizzare i dettagli del processo, inclusi errori e sotto-attività. Fai clic sullo stato "Non riuscito" per visualizzare i dettagli dell'errore. Per i processi con sotto-attività, espandi la riga per visualizzare descrizioni e stati. Per i sotto-processi, utilizza la funzione di drilldown del processo per visualizzarne i dettagli.

- Scarica i pacchetti di log - raccogli i file di log per risolvere i problemi degli ONTAP tools for VMware vSphere.
- Gestisci i certificati: sostituisci il certificato autofirmato con un certificato CA personalizzato e rinnova o aggiorna i certificati per VASA Provider e ONTAP tools.
- Reimposta password - Cambia la password per il VASA Provider e SRA.
- Gestisci le impostazioni dell'appliance: configura l'appliance ONTAP tools, inclusa l'abilitazione dell'HA e l'aumento delle dimensioni dei nodi.

Per accedere a ONTAP tools Manager, avvia `https://<ONTAPtoolsIP>:8443/virtualization/ui/` dal browser ed effettua l'accesso con le credenziali di amministratore di ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.



| Scheda | Descrizione |
| --- | --- |
| Scheda appliance | La scheda Appliance mostra lo stato generale dell'appliance ONTAP tools, i dettagli di configurazione e lo stato dei servizi abilitati. Per visualizzare ulteriori informazioni, seleziona il link **Visualizza dettagli**. Se cambi un'impostazione dell'appliance, la scheda mostra lo stato e i dettagli del job fino al completamento della modifica. |
| Scheda avvisi | La scheda Avvisi mostra gli avvisi di ONTAP tools categorizzati per tipo, inclusi gli avvisi a livello di nodo HA. Puoi visualizzare gli avvisi dettagliati facendo clic sul hyperlink, che ti porta alla pagina degli avvisi filtrata in base al tipo di avviso selezionato. |
| Scheda vCenters | La scheda vCenters mostra lo stato di salute di tutte le istanze vCenter Server gestite da ONTAP tools. Puoi visualizzare i dettagli di ciascun vCenter selezionando il collegamento corrispondente, che porta a una pagina con ulteriori informazioni sull'istanza selezionata. |
| Scheda backend di storage | La scheda Storage backends mostra lo stato di integrità e connettività di tutti i cluster di storage ONTAP configurati in ONTAP tools. Puoi visualizzare i dettagli per ciascun storage backend selezionando il link corrispondente, che ti porta a una pagina con più informazioni sul cluster selezionato. |
| Scheda nodi ONTAP tools | La scheda dei nodi di ONTAP tools mostra tutti i nodi dell'appliance, inclusi nome del nodo, nome della VM, stato e informazioni di rete. Seleziona **Visualizza dettagli** per vedere più dettagli su un nodo specifico. [NOTA] In una configurazione non HA, appare un solo nodo. In una configurazione HA, vengono visualizzati tre nodi. |

# Gestisci le impostazioni di ONTAP tools Manager

## Modifica le impostazioni di AutoSupport degli strumenti ONTAP

Quando configuri ONTAP tools for VMware vSphere per la prima volta, AutoSupport è abilitato per impostazione predefinita. Invia messaggi al supporto tecnico 24 ore dopo che è stato abilitato.

### Disabilita AutoSupport

Quando disattivi AutoSupport, non ricevi più supporto e monitoraggio proattivi.

Si consiglia di mantenere AutoSupport attiva, perché aiuta ad accelerare l'individuazione e la risoluzione dei problemi. Anche quando AutoSupport è disabilitato, il sistema continua a raccogliere e memorizzare informazioni localmente, ma non invia report sulla rete.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona l'opzione **Impostazioni** > **Telemetria** > **Modifica**.
4. Deseleziona l'opzione **AutoSupport** e salva le modifiche.

#### Aggiorna l'URL del proxy AutoSupport

Aggiorna l'URL del proxy AutoSupport così la funzionalità AutoSupport instrada i dati attraverso il proxy server per una trasmissione sicura.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona **Impostazioni** dalla barra laterale.
4. Seleziona l'opzione **Impostazioni** > **Telemetria** > **Modifica**.
5. Inserisci un URL **Proxy** valido e salva le modifiche.

   Se disabiliti AutoSupport, anche l'URL del proxy viene disabilitato.

## Aggiungi server NTP agli strumenti ONTAP

Inserisci i dettagli del server NTP per sincronizzare gli orologi dell'appliance ONTAP tools.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona l'opzione **Impostazioni** > **server NTP** > **Modifica**.
4. Inserisci il fully qualified domain name (FQDN), gli indirizzi IPv4 o IPv6 separati da virgole.

   Aggiorna la schermata per visualizzare i valori aggiornati.

## Reimposta le credenziali del provider VASA e SRA negli strumenti ONTAP

Se dimentichi le tue credenziali VASA Provider o SRA, puoi reimpostarle con una nuova password tramite l'interfaccia ONTAP tools Manager. La nuova password deve essere lunga tra 8 e 256 caratteri.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona l'opzione **Impostazioni** > **VASA Provider / SRA credentials** > **Reset Password**.
4. Inserisci la nuova password e confermala.
5. Seleziona **Salva** per applicare le modifiche.

### Modifica le impostazioni di backup di ONTAP tools

A partire da ONTAP tools for VMware vSphere 10.5, la funzione di backup è abilitata per impostazione predefinita e viene creato un backup ogni 10 minuti. Puoi disabilitare il backup o modificarne la frequenza.

Non disabilitare il backup perché impedisce agli ONTAP tools di mantenere un RPO basso. Disabilitare il backup non elimina i file di backup esistenti. Puoi modificare la frequenza del backup impostandola su un valore tra 10 e 60 minuti.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona l'opzione **Impostazioni** > **Backup** > **Modifica**.
4. Nella finestra di modifica puoi disabilitare il backup o modificarne la frequenza.

# Abilita i servizi di ONTAP tools

Puoi cambiare la password dell'amministratore usando ONTAP tools Manager per abilitare servizi come VASA Provider, l'importazione della configurazione vVols e il disaster recovery (SRA) usando ONTAP tools Manager.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Nella sezione Panoramica, seleziona **Modifica impostazioni dell'appliance**.
4. Nella sezione **Servizi**, puoi abilitare servizi opzionali come VASA Provider, importazione della configurazione vVols e disaster recovery (SRA) secondo necessità.

   Quando abiliti i servizi per la prima volta, devi creare le credenziali del VASA Provider e dell'SRA. Queste vengono utilizzate per registrare o abilitare i servizi del VASA Provider e dell'SRA sul vCenter Server. Il nome utente può contenere solo lettere, numeri e trattini bassi. La lunghezza della password deve essere compresa tra 8 e 256 caratteri.

Prima di disabilitare qualsiasi servizio opzionale, assicurati che i server vCenter gestiti da ONTAP tools non li utilizzino.

L'opzione **Consenti importazione della configurazione vVols** viene visualizzata solo quando il servizio VASA Provider è abilitato. Questa opzione consente la migrazione dei dati vVols da ONTAP tools 9.xx a ONTAP tools 10.5.

# Modificare le impostazioni dell'appliance ONTAP tools

Usa ONTAP tools Manager per scalare la configurazione di ONTAP tools for VMware vSphere, aumentando il numero di nodi oppure abilitando l'High Availability (HA). Per impostazione predefinita, l'appliance ONTAP tools for VMware vSphere viene distribuita come configurazione a nodo singolo, non-HA.

**Prima di iniziare**

- Assicurati che il tuo modello OVA abbia la stessa versione OVA del Node 1. Il Node 1 è il nodo predefinito in cui l'OVA degli ONTAP tools for VMware vSphere viene inizialmente distribuito.
- Assicurati che le funzioni di hot add della CPU e hot plug della memoria siano abilitate.
- Nel vCenter Server, imposta il livello di automazione del Disaster Recovery Service (DRS) su parzialmente automatizzato. Dopo aver implementato HA, riportalo su completamente automatizzato.
- I nomi host dei nodi nella configurazione HA devono essere in minuscolo.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Nella sezione Panoramica, seleziona **Modifica impostazioni dell'appliance**.
4. Nella sezione **Configurazione**, aumenta la dimensione del nodo e abilita la configurazione HA. Usa le credenziali del server vCenter per apportare modifiche.

   Nella configurazione HA, puoi modificare i dettagli dell'archivio di contenuti. Inserisci la password per ogni modifica.

   In ONTAP tools for VMware vSphere, puoi solo aumentare le dimensioni del nodo; non puoi ridurle. In una configurazione non HA, è supportata solo una configurazione di medie dimensioni. In una configurazione HA, sono supportate configurazioni di medie e grandi dimensioni.

5. Usa il pulsante di attivazione/disattivazione HA per abilitare la configurazione HA. Nella pagina **Impostazioni HA**, assicurati che:
   - L'archivio di contenuti appartiene allo stesso vCenter Server in cui sono in esecuzione le VM dei nodi di ONTAP tools. Le credenziali del vCenter Server vengono utilizzate per convalidare e scaricare il template OVA per le modifiche all'appliance.
   - La macchina virtuale che ospita gli ONTAP tools non viene distribuita direttamente su un host ESXi. La VM deve essere distribuita su un cluster o un pool di risorse.

Una volta abilitata la configurazione HA, non puoi tornare a una configurazione a nodo singolo non HA.

6. Nella sezione **Impostazioni HA** della finestra **Modifica impostazioni appliance**, puoi inserire i dettagli dei nodi 2 e 3. ONTAP tools per VMware vSphere supporta tre nodi in una configurazione HA.

   Gli ONTAP tools precompilano la maggior parte delle opzioni di input con i dettagli di rete del Nodo 1 per semplificare il flusso di lavoro. Puoi modificare i dati di input prima di andare all'ultima pagina della procedura guidata. Puoi inserire i dettagli dell'indirizzo IPv6 per gli altri due nodi solo quando l'indirizzo IPv6 è abilitato sul nodo di gestione degli ONTAP tools.

   Assicurati che ogni host ESXi contenga solo una macchina virtuale ONTAP tools. Gli input vengono convalidati ogni volta che passi alla finestra successiva.

7. Rivedi i dettagli nella sezione **Riepilogo** e **Salva** le modifiche.

**E ora?**

La pagina **Panoramica** mostra lo stato della distribuzione. Puoi anche monitorare lo stato del job di modifica delle impostazioni dell'appliance dalla vista dei job usando l'ID del job.

Se la distribuzione HA non riesce e lo stato del nuovo nodo è "Nuovo", elimina la nuova VM in vCenter prima di provare ad abilitare nuovamente HA.

La scheda **Avvisi** nel pannello di sinistra elenca gli avvisi per ONTAP tools for VMware vSphere.

# Aggiungere host VMware vSphere a ONTAP tools

Aggiungi nuovi host VMware vSphere agli ONTAP tools for VMware vSphere per gestire e proteggere i datastore sugli host.

**Passaggi**

1. Aggiungi un host al tuo cluster VMware vSphere seguendo il flusso di lavoro nella pagina: "Documentazione Tecnica Broadcom".
2. Dopo aver aggiunto l'host, vai al menu principale di ONTAP tools e seleziona **Discover** nel pannello Overview. Attendi che il processo di discovery sia terminato. In alternativa, puoi aspettare che il discovery host pianificato sia completato.

**Risultato**

Il nuovo host è ora rilevato e gestito da ONTAP tools for VMware vSphere. Puoi procedere a gestire il datastore sul nuovo host.

**Argomenti correlati**

- "Monta un datastore vVols" su nuovi host.
- "Monta i datastore NFS e VMFS" su nuovi host.

# Gestisci i datastore

## Montare i datastore NFS e VMFS negli ONTAP tools

Il montaggio di un datastore consente accesso allo storage a host aggiuntivi. Puoi montare il datastore sugli host aggiuntivi dopo averli aggiunti all'ambiente VMware.

> Quando aggiungi un nuovo host ESXi usando "Documentazione Tecnica Broadcom", aspetta che il rilevamento host pianificato sia completato prima che venga visualizzato in ONTAP tools. In alternativa, puoi avviare manualmente il rilevamento dalla schermata di panoramica di NetApp ONTAP tools.

**Informazioni su questa attività**

- Alcune azioni associate al clic destro del mouse sono disabilitate o non disponibili a seconda della versione del client vSphere e del tipo di datastore selezionato.
  - Se usi il client vSphere 8.0 o versioni successive, alcune delle opzioni del menu clic destro sono nascoste.
  - Dalla versione vSphere 7.0U3 alla vSphere 8.0, anche se le opzioni vengono visualizzate, l'azione sarà disabilitata.
- vSphere disabilita l'opzione di montaggio del datastore quando il cluster è protetto con configurazioni uniformi.

**Passaggi**

1. Dalla home page del client vSphere, seleziona **Host e cluster**.
2. Nel riquadro di navigazione a sinistra, seleziona i data center che contengono gli host.
3. Per montare i datastore NFS/VMFS su un host o un cluster, fai clic con il pulsante destro del mouse e seleziona **NetApp ONTAP tools** > **Mount Datastores**.
4. Seleziona gli archivi dati che vuoi montare e seleziona **Monta**.

**E ora?**

Puoi monitorare l'avanzamento nel pannello delle attività recenti.

**Argomento correlato**

"Aggiungi nuovi host vSphere VMware"

## Smonta i datastore NFS e VMFS negli ONTAP tools

L'azione Smonta datastore rimuove un datastore NFS o VMFS dagli host ESXi. È disponibile per i datastore rilevati o gestiti da ONTAP tools for VMware vSphere.

**Passaggi**

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un oggetto datastore NFS o VMFS e seleziona **Smonta datastore**.

   Il vSphere client apre una finestra di dialogo e elenca gli host ESXi che montano il datastore. Quando l'operazione viene eseguita su un datastore protetto, viene visualizzato un messaggio di avviso sullo schermo.

3. Seleziona uno o più host ESXi da cui smontare il datastore.

Non puoi smontare il datastore da tutti gli host. L'interfaccia utente suggerisce di usare invece l'operazione di eliminazione del datastore.

4. Seleziona il pulsante **Smonta**.

   Se il datastore fa parte di un cluster host protetto, viene visualizzato un messaggio di avviso.

> Se il datastore protetto viene smontato, l'impostazione di protezione corrente potrebbe comportare una protezione parziale. Consulta "Modifica cluster protetto" per abilitare la protezione completa.

**E ora?**

Puoi monitorare l'avanzamento nel pannello delle attività recenti.

## Montare un datastore vVols negli ONTAP tools

Puoi montare un datastore VMware Virtual Volumes (vVols) su uno o più host aggiuntivi per fornire accesso allo storage ad altri host. Puoi smontare il datastore vVols solo tramite le API.

> Quando aggiungi un nuovo host ESXi usando "Documentazione Tecnica Broadcom", aspetta che il rilevamento host pianificato sia completato prima che venga visualizzato in ONTAP tools. In alternativa, puoi avviare manualmente il rilevamento dalla schermata di panoramica di NetApp ONTAP tools.

**Passaggi**

1. Dalla home page del client vSphere, seleziona **Host e cluster**.
2. Nel riquadro di navigazione, seleziona il data center che contiene il datastore.
3. Fai clic con il pulsante destro del mouse sul datastore e seleziona **NetApp ONTAP tools** > **Monta datastore**.
4. Nella finestra di dialogo **Monta datastore sugli host**, seleziona gli host sui quali desideri montare il datastore, quindi seleziona **Monta**.

Il pannello delle attività recenti mostra lo stato di avanzamento.

**Argomento correlato**

"Aggiungi nuovi host vSphere VMware"

## Ridimensiona i datastore NFS e VMFS negli ONTAP tools

Il ridimensionamento di un datastore ti permette di aumentare lo spazio di archiviazione per i file delle tue macchine virtuali. Puoi modificare le dimensioni di un datastore quando cambiano i requisiti della tua infrastruttura.

**Informazioni su questa attività**

Puoi aumentare le dimensioni dei datastore NFS e VMFS. Un volume FlexVol in questi datastore non può ridursi al di sotto delle sue dimensioni attuali, ma può crescere fino al 120%.

**Passaggi**

1. Dalla home page del client vSphere, seleziona **Host e cluster**.
2. Nel riquadro di navigazione, seleziona il data center che contiene il datastore.
3. Fai clic con il pulsante destro del mouse sul datastore NFS o VMFS e seleziona **NetApp ONTAP tools** > **Ridimensiona datastore**.
4. Nella finestra di dialogo Ridimensiona, inserisci una nuova dimensione per il datastore e seleziona **OK**.

## Espandi gli datastore vVols negli ONTAP tools

Quando fai clic con il pulsante destro del mouse sull'oggetto datastore nella vista oggetti di vCenter, la sezione del plug-in mostra le azioni supportate per ONTAP tools for VMware vSphere. Azioni specifiche sono abilitate a seconda del tipo di datastore e dei privilegi dell'utente corrente.

L'operazione di espansione del datastore vVols non è applicabile ai datastore vVols basati su sistema ASA r2.

**Passaggi**

1. Dalla home page del client vSphere, seleziona **Host e cluster**.
2. Nel riquadro di navigazione, seleziona il data center che contiene il datastore.
3. Fai clic con il pulsante destro del mouse sul datastore e seleziona **NetApp ONTAP tools** > **Add storage to datastore**.
4. Nella finestra **Crea o seleziona volumi**, puoi creare nuovi volumi oppure scegliere tra quelli esistenti. Segui le istruzioni visualizzate sullo schermo per effettuare la selezione.
5. Nella finestra **Riepilogo**, rivedi le selezioni e seleziona **Espandi**. Puoi monitorare l'avanzamento nel pannello delle attività recenti.

## Ridurre un datastore vVols negli ONTAP tools

Questa pagina spiega come rimuovere i volumi da un vVols datastore.

Usa l'azione "rimuovi spazio di archiviazione dal datastore" su qualsiasi datastore vVols gestito da ONTAP tools in vCenter Server.

Non puoi rimuovere lo storage da un volume se contiene vVols; l'opzione di rimozione sarà disabilitata per tali volumi. Quando rimuovi i volumi dal datastore, hai anche l'opzione di eliminare i volumi selezionati dallo storage ONTAP.

L'operazione di riduzione del datastore vVols non è supportata per i datastore vVols basati su sistemi ASA r2.

**Passaggi**

1. Dalla home page del client vSphere, seleziona **Host e cluster**.
2. Nel riquadro di navigazione, seleziona il data center che contiene il datastore.
3. Fai clic con il pulsante destro del mouse sul datastore vVol e seleziona **NetApp ONTAP tools** > **Remove storage from datastore**.
4. Seleziona i volumi che non hanno vVols e seleziona **Rimuovi**.

L'opzione per selezionare il volume su cui vVols risiede è disabilitata.

5. Nella finestra a comparsa **Rimuovi storage**, seleziona la casella di controllo **Elimina volumi dal cluster ONTAP** per eliminare i volumi dal datastore e dallo storage ONTAP, quindi seleziona **Elimina**.

## Elimina i datastore in ONTAP tools

Questa pagina descrive come eliminare i datastore NFS, VMFS o vVols utilizzando gli ONTAP tools nel server vCenter.

Quando elimini un datastore, a seconda del tipo di datastore, vengono eseguite le seguenti azioni:

- Il vVol container è stato smontato.
- Se l'igroup non è in uso, i suoi initiator vengono rimossi dall'igroup.
- Il vVol container è eliminato.
- I volumi Flex rimangono sull'array di storage.

Puoi eliminare il datastore solo se non sono presenti vVols nel datastore selezionato.

**Passaggi**

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e seleziona **NetApp ONTAP tools** > **Elimina datastore**.

   Non puoi eliminare un datastore utilizzato da macchine virtuali. Sposta le macchine virtuali in un altro datastore prima di eliminarlo. Non puoi eliminare il volume se fa parte di un cluster host protetto.

   a. Nel caso di un datastore NFS o VMFS, viene visualizzata una finestra di dialogo con l'elenco delle VM che utilizzano il datastore.
   b. Se non sono associate macchine virtuali a un datastore VMFS, viene visualizzata una finestra di dialogo di conferma. Se la protezione del cluster host è abilitata ed esiste una relazione AFD, puoi eliminare gli elementi di storage secondario.
   c. Per i datastore VMFS protetti sui sistemi ASA r2, rimuovi la protezione prima di eliminarli. A partire da ONTAP 9.17.1 e ONTAP tools for VMware vSphere 10.5, puoi eliminare un datastore protetto. Se è l'unico datastore nel gruppo di protezione, la protezione del cluster host viene rimossa automaticamente.
   d. Per i datastore vVols, puoi eliminare il datastore solo se non sono presenti vVols. La finestra di dialogo **Elimina datastore** include un'opzione per rimuovere i volumi dal cluster ONTAP.
   e. Per i datastore vVols sui sistemi ASA r2, non puoi eliminare i volumi di supporto da ONTAP usando l'opzione **Elimina datastore**.
3. Per eliminare i volumi di supporto sullo storage ONTAP, seleziona **Elimina volumi su ONTAP cluster**.

   Per i datastore VMFS su storage ONTAP unificato che fanno parte di un cluster host protetto, non puoi eliminare il volume dal cluster ONTAP.

Quando elimini un datastore NFS, VMFS o vVols, gli igroup padre rimangono sul sistema ONTAP. Gli igroup figlio che non sono mappati a nessuna LUN vengono eliminati automaticamente. Gli ONTAP tools eseguono

una pulizia giornaliera per rimuovere gli igroup padre predefiniti non mappati. Elimina manualmente gli igroup padre personalizzati in ONTAP. Gli ONTAP tools non possono riutilizzare gli igroup padre obsoleti.

## Visualizzazioni dello storage ONTAP per i datastore negli ONTAP tools

ONTAP tools for VMware vSphere mostra la vista lato storage ONTAP dei datastore e dei loro volumi nella scheda di configurazione.

**Passaggi**

1. Dal client vSphere, vai al datastore.
2. Seleziona la scheda **Configura** nel riquadro di destra.
3. Seleziona **NetApp ONTAP tools** > **ONTAP Storage**. La visualizzazione cambia in base al tipo di datastore. Vedi la tabella qui sotto:

| Tipo di datastore | Informazioni disponibili |
|---|---|
| Datastore NFS | La pagina **Dettagli di archiviazione** contiene informazioni sui backend di storage, sugli aggregati e sui volumi. La pagina **Dettagli NFS** contiene dati relativi al datastore NFS. |
| Datastore VMFS | La pagina **Dettagli di archiviazione** contiene i dettagli relativi al backend di archiviazione, all'aggregato, al volume e alla zona di disponibilità dello storage (SAZ). La pagina **Dettagli dell'unità di archiviazione** contiene i dettagli dell'unità di archiviazione. |
| datastore vVols | Elenca tutti i volumi. Puoi espandere o rimuovere lo storage dal riquadro dello storage ONTAP. ONTAP tools non supporta questa visualizzazione per i datastore vVols basati su sistema ASA r2. |

## Visualizzazione dell'archiviazione della macchina virtuale in ONTAP tools

La vista di archiviazione mostra l'elenco dei vVols che la macchina virtuale crea.

Questa vista si applica alle VM con almeno un disco proveniente da un datastore vVols gestito da ONTAP tools for VMware vSphere.

**Passaggi**

1. Dal vSphere Client vai alla macchina virtuale.
2. Seleziona la scheda **Monitor** nel riquadro di destra.
3. Seleziona **NetApp ONTAP tools** > **Storage**. I dettagli di **Storage** vengono visualizzati nel riquadro di destra. Puoi vedere l'elenco di vVols presenti sulla VM.

   Puoi usare l'opzione "Gestisci colonne" per nascondere o mostrare diverse colonne.

# Gestire le soglie di archiviazione negli ONTAP tools

Puoi impostare la soglia per ricevere notifiche in vCenter Server quando il volume e la capacità aggregata raggiungono determinati livelli.

**Passaggi:**

1. Accedi al vSphere client.
2. Nella pagina dei collegamenti rapidi, seleziona **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro di ONTAP tools, vai su **Impostazioni** > **Impostazioni soglia** > **Modifica**.
4. Nella finestra **Modifica soglia**, inserisci i valori desiderati nei campi **Quasi pieno** e **Pieno** e seleziona **Salva**. Puoi ripristinare i valori di soglia predefiniti consigliati: 80 per Quasi pieno e 90 per Pieno.

# Gestire i backend di storage in ONTAP tools

I backend di archiviazione sono i sistemi che gli host ESXi utilizzano per l'archiviazione dei dati.

## Scopri lo storage

Puoi eseguire il rilevamento di un backend di storage su richiesta senza attendere un rilevamento pianificato, così da aggiornare immediatamente i dettagli dello storage. Per le configurazioni MetroCluster, esegui manualmente la discovery degli ONTAP tools dopo uno switchover.

Segui i passaggi seguenti per scoprire i backend di archiviazione.

**Passaggi**

1. Accedi al vSphere client.
2. Nella pagina dei collegamenti rapidi, seleziona **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro di ONTAP tools, vai su **Storage Backends** e seleziona un storage backend.
4. Seleziona il menu con i tre puntini verticali e seleziona **Discover storage**

Puoi monitorare l'avanzamento nel pannello delle attività recenti.

## Modifica i backend di archiviazione

Puoi modificare le credenziali del backend di storage o il nome della porta. Puoi anche modificare il backend di storage per i cluster ONTAP globali usando ONTAP tools Manager. Se il certificato scade tra 30 giorni o meno, ONTAP tools mostra un avviso. Modifica il backend di storage e carica il nuovo certificato dall'amministratore ONTAP.

Quando modifichi il backend di archiviazione, ONTAP tools for VMware vSphere esegue una scoperta del backend di archiviazione per aggiornare i dettagli di archiviazione.

Segui i passaggi in questa sezione per modificare un backend di archiviazione.

1. Accedi al vSphere client.
2. Nella pagina dei collegamenti rapidi, seleziona **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro di ONTAP tools, vai su **Storage Backends** e seleziona un storage backend.

4. Seleziona il menu con i tre puntini verticali e seleziona **Modifica** per modificare le credenziali o il nome della porta. Puoi monitorare l'avanzamento nel pannello delle attività recenti.

Modifica i cluster ONTAP globali con ONTAP tools Manager come segue.

1. Avvia ONTAP tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona i backend di archiviazione dalla barra laterale.
4. Seleziona il backend di archiviazione che vuoi modificare.
5. Seleziona il menu con le ellissi verticali e seleziona **Modifica**.
6. Puoi modificare le credenziali o la porta. Inserisci **Username** e **Password** per modificare il backend di storage.

## Rimuovi i backend di storage

Devi rimuovere tutti i datastore collegati al backend di storage prima di rimuoverlo. Segui i passaggi qui sotto per rimuovere un backend di storage.

1. Accedi al vSphere client.
2. Nella pagina dei collegamenti rapidi, seleziona **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro di ONTAP tools, vai su **Storage Backends** e seleziona un storage backend.
4. Seleziona il menu con i tre puntini verticali e scegli **Rimuovi**. Assicurati che il backend di storage non contenga alcun datastore. Puoi monitorare l'avanzamento nel pannello delle attività recenti.

È possibile rimuovere i cluster ONTAP globali utilizzando ONTAP tools Manager.

1. Avvia ONTAP tools Manager da un browser web: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona **Storage Backends** dalla barra laterale.
4. Seleziona il backend di storage che vuoi rimuovere
5. Seleziona il menu con i puntini di sospensione verticali e seleziona **Rimuovi**.

## Analisi dettagliata del backend di storage

La pagina dei backend di archiviazione elenca tutti i backend di archiviazione. Puoi eseguire operazioni di individuazione dello storage, modifica e rimozione sui backend di archiviazione che hai aggiunto, ma non sulle singole SVM figlie all'interno del cluster.

Seleziona il cluster padre o figlio per visualizzare il riepilogo dei componenti. Per il cluster padre, usa il menu a discesa delle azioni per individuare lo storage, modificarlo o rimuovere il backend di storage.

La pagina di riepilogo fornisce i seguenti dettagli:

- Stato del backend di storage

- Informazioni sulla capacità
- Informazioni di base sulla macchina virtuale
- Dettagli del certificato come lo stato del certificato e la data di scadenza.
- Informazioni di rete come l'indirizzo IP e la porta della rete. Per la SVM figlia, le informazioni sono le stesse del backend di storage padre.
- Privileges consentiti e limitati per il backend di storage. Per la SVM figlia, le informazioni sono le stesse del backend di storage padre. ONTAP tools visualizza i privilegi solo sui backend di storage basati su cluster. Se si aggiunge SVM come backend di storage, le informazioni sui privilegi non vengono visualizzate.
- La vista di dettaglio del cluster di sistema ASA r2 non include la scheda dei livelli locali quando la proprietà disaggregata è impostata su "true" per l'SVM o il cluster.
- Per i sistemi ASA r2 SVM, il portlet della capacità non viene visualizzato. Il portlet della capacità è necessario solo quando la proprietà disaggregata è impostata su "true" per l'SVM o il cluster.
- Per i sistemi ASA r2 SVM, la sezione con le informazioni di base mostra il tipo di piattaforma.

La scheda Interfaccia fornisce informazioni dettagliate sull'interfaccia.

La scheda "Livelli locali" fornisce informazioni dettagliate sull'elenco degli aggregati.

# Gestisci le istanze del server vCenter negli strumenti ONTAP

Le istanze di vCenter Server sono piattaforme di gestione centralizzate che ti permettono di controllare host, macchine virtuali e backend di storage.

## Dissocia i backend di storage con l'istanza del server vCenter

La pagina di elenco dei server vCenter mostra il numero di backend di storage associati. Ogni istanza del server vCenter offre la possibilità di associarsi o dissociarsi da un backend di storage.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona l'istanza del server vCenter richiesta dalla barra laterale.
4. Seleziona i puntini di sospensione verticali accanto al server vCenter che vuoi associare o dissociare ai backend di storage.
5. Seleziona **Dissocia storage backend**.

## Modifica un'istanza del server vCenter

Segui i passaggi seguenti per modificare un'istanza del server vCenter.

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante

la distribuzione.

3. Seleziona l'istanza del server vCenter appropriata dalla barra laterale
4. Seleziona i puntini di sospensione verticali accanto al vCenter Server che vuoi modificare e seleziona **Modifica**.
5. Nella finestra **Modifica vCenter**, inserisci nome utente, password e dettagli della porta.
6. Carica il certificato e seleziona **Modifica**.

## Rimuovi un'istanza del server vCenter

Rimuovi tutti i backend di storage dal vCenter Server prima di rimuoverlo.

1. Avvia ONTAP tools Manager da un browser web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona le istanze del server vCenter applicabili dalla barra laterale
4. Seleziona i puntini di sospensione verticali accanto al vCenter Server che vuoi rimuovere e seleziona **Rimuovi**.

> Dopo che rimuovi le istanze del server vCenter, non saranno più gestite dall'applicazione.

Quando rimuovi le istanze di vCenter Server negli ONTAP tools, vengono eseguite automaticamente le seguenti azioni:

- Il plug-in non è registrato.
- I privilegi e i ruoli dei plug-in sono stati rimossi.

## Rinnova il certificato del server vCenter

ONTAP tools ti avvisa quando il certificato vCenter sta per scadere o è già scaduto. Dopo aver rinnovato il certificato vCenter, carica il nuovo certificato su ONTAP tools seguendo questi passaggi:

1. Accedi alla shell di diagnostica remota degli ONTAP tools.
2. Ottieni il certificato vCenter rinnovato dalla shell diagnostica:

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN
CERTIFICATE/,/END CERTIFICATE/p'
```

3. Assicurati che il certificato sia in formato ASCII Base 64 e includa le righe di inizio e fine, ad esempio:

```
---{}BEGIN CERTIFICATE{}---
MIIFUzCCA7ugAwIBAgIJANOgLapcl5oSMA0GCSqGSIb3DQEBCwUAMIGJMQwwCgYD
VQQDDAN2YzExFDASBgoJkiaJk/IsZAEZFgRkZW1vMRUwEwYKCZImiZPyLGQBGRYF
bG9jYWwxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRwwGgYDVQQK
DBN2YzEuZGVtby5uZXRhcHAuY29tMQwwCgYDVQQLDANMT0QwHhcNMjQwNDA1MTgw
NTE4WhcNMjYwNDA1MTgwNTE4WjBzMRwwGgYDVQQDDBN2YzEuZGVtby5uZXRhcHAu
Y29tMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJ
UGFsbyBBbHRvMQ8wDQYDVQQKDAZOZXRBcHAxDDAKBgNVBAsMA0xPRDCCAaIwDQYJ
KoZIhvcNAQEBBQADggGPADCCAYoCggGBALU8OCWMtA2gvIC/OTw/7xucvPVuM+b8
DhzvNpQ2phjfr6ctEhbntPpqPdu+t2CKK7l0mzg3D9cJ/rvMvdDDXr0tgaD1oi2u
ZDW0CaF0QhLOpNfRXMoogBZ66csEhViAy3CHTcOse770mA/PyoHgrCPZngVlZIiQ
TIWpdQMbEEzFIkrLfC70UW2MzfublrsH7Dn/kOu/iCSlVJWixKf7SmZtVQ5ZxBTD
UlJSiqoX1eRXGyunArEvrIpOY9kkKXUElm3hGnk/ZmiuBJ+HqUYqYW+H+7vE3lKa
6NEqDX+tZotxTx2bXMjeiIWU30ZbshgeXlIG9qc49clBoC9iGjavhctOcaXg/W3h
dLKK5ds3rpRERgMg6VMkrfiqAJuiq+b3sTvXMAul/3hL7hz5QABAE/hP4ZvIHV02
WWDQRLiuVFAcDAyvCrO9Irx0Gk1RyRShKYakdWxZ3hhMdLuGq0yvRXqo1Ib94zwO
JfBJHjFToA/GqwromZgiTzJkKq5xbN8MFwIDAQABo4HSMIHPMAsGA1UdDwQEAwIF
4DA7BgNVHREENDAygRVlbWFpbEBkZW1vLm5ldGFwcC5jb22HBMCoAB+CE3ZjMS5k
ZW1vLm5ldGFwcC5jb20wHQYDVR0OBBYEFJ0V0zY+JRpFrEt31ovAY4BLFXmAMB8G
A1UdIwQYMBaAFENf6fRxWF3OJQNTPIdUpK6kjA78MEMGCCsGAQUFBwEBBDcwNTAz
BggrBgEFBQcwAoYnaHR0cHM6Ly92YzEuZGVtby5uZXRhcHAuY29tL2FmZC92ZWNz
L2NhMA0GCSqGSIb3DQEBCwUAA4IBgQBaDfk7GBM4vmhzYCqGrr6KB+h3qeTJ+Y0Y
5nIPRP1HucawDQ8QTay605ddJ8gFGoxkOQDn9tdXWXGjnTRFOT8R+Hw/nUfVSiDP
sYienb16copzUNwtqh+m9Ifow74Gf+ulRzEC0EAVO1X/nTEYH6NKM6Wy7y7F8g5J
lrpM3JY90ZChMqHO3Av/88rbErfQ/gU1brJ3u9Gks4e20Z7Ff312ZKhWRuJDlN2Z
0tc/gp90N9GxaVvELovq/pdjaZ8xiXCxa6piicrJd9WnqMH1gmxP2PIBDxMDBWBG
gwsfs5H7VG9MJYks6lViNsGclo0EwEdF0MfoB3JtsWpPWq6+jBua0Jm7/aFCU+Ht
mykr0gaV7muegoiBQuDma4EkAI31D7ZlUgJQaw157NTk4RW3TFcbtViBHJkM54Hr
iVm0cl+2BZNi/QTMh/MkWV2dYXJ3NuNlqqfzFY+bUfkzkR4SneMk0HX3joNNYDJv
siO7bL+k/Pxql27NVIhuCoVJAlcI7ak=
---{}END CERTIFICATE{}---
```

4. Copia l'output e salvalo come file di testo con un' `.pem`estensione sul tuo desktop.
5. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
6. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
7. Seleziona l'istanza del server vCenter appropriata dalla barra laterale
8. Seleziona i puntini di sospensione verticali accanto al vCenter Server che vuoi modificare e seleziona **Modifica**.
9. Nella finestra **Modifica vCenter**, inserisci nome utente, password e dettagli della porta.
10. Carica il certificato e seleziona **Modifica**.

**Informazioni correlate**

"Configura l’accesso diagnostico remoto"

# Gestisci i certificati degli strumenti ONTAP

Per impostazione predefinita, durante la distribuzione viene generato un certificato autofirmato per ONTAP tools e VASA Provider. Puoi usare l’interfaccia di ONTAP tools Manager per rinnovare questo certificato o sostituirlo con un certificato CA personalizzato. Nelle distribuzioni multi-vCenter, è necessario utilizzare certificati CA personalizzati.

**Prima di iniziare**

Dovresti avere quanto segue prima di iniziare:

- Il domain name associato all’indirizzo IP virtuale.
- nslookup riuscito del domain name, che conferma che si risolve nell’indirizzo IP corretto.
- Certificati creati con il domain name e l’indirizzo IP degli ONTAP tools.

Un indirizzo IP di ONTAP tools deve corrispondere a un fully qualified domain name (FQDN). I certificati devono contenere lo stesso FQDN associato all’indirizzo IP di ONTAP tools nel subject o nei subject alternative names.

Non puoi passare da un certificato firmato da una CA a un certificato autofirmato.

### Aggiorna il certificato degli ONTAP tools

La scheda ONTAP tools mostra dettagli come il tipo di certificato (autofirmato/firmato da CA) e domain name. Durante la distribuzione, viene generato per impostazione predefinita un certificato autofirmato. Puoi rinnovare il certificato o aggiornarlo a un certificato CA.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona **Certificates** > **ONTAP tools** > **Renew** per rinnovare i certificati.

   Puoi rinnovare il certificato se è scaduto o se la data di scadenza si avvicina. L'opzione di rinnovo è disponibile quando il tipo di certificato è CA-signed. Nella finestra pop-up, inserisci i dettagli del certificato del server, della chiave privata, della root CA e del certificato intermedio.

   Il sistema rimarrà offline fino al rinnovo del certificato e verrai disconnesso dall'interfaccia di ONTAP tools Manager.

4. Per aggiornare il certificato autofirmato a un certificato CA personalizzato, seleziona **Certificates** > **ONTAP tools** > **Upgrade to CA**.
   a. Nella finestra a comparsa, carica il certificato del server, la chiave privata del certificato del server, il certificato CA radice e i file del certificato intermedio.
   b. Inserisci il fully qualified domain (FQDN) dell'indirizzo IP del Load Balancer per cui hai generato questo certificato e aggiorna il certificato.

   Il sistema sarà offline fino al completamento dell'aggiornamento e verrai disconnesso dall'interfaccia di ONTAP tools Manager.

### Aggiorna il certificato del VASA Provider

ONTAP tools for VMware vSphere viene distribuito con un certificato autofirmato per VASA Provider. Con questo, è possibile gestire solo un'istanza di vCenter Server per i datastore vVols. Quando gestisci più istanze di vCenter Server e vuoi abilitare la funzionalità vVols su di esse, devi sostituire il certificato autofirmato con un certificato CA personalizzato.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere che hai fornito durante la distribuzione.
3. Seleziona **Certificati** > **VASA Provider** o **ONTAP tools** > **Rinnova** per rinnovare i certificati.
4. Seleziona **Certificates** > **VASA Provider** o **ONTAP tools** > **Upgrade to CA** per aggiornare il certificato autofirmato a un certificato CA personalizzato.
   a. Nella finestra a comparsa, carica il certificato del server, la chiave privata del certificato del server, il certificato CA radice e i file del certificato intermedio.
   b. Inserisci il fully qualified domain (FQDN) dell'indirizzo IP del Load Balancer per cui hai generato questo certificato e aggiorna il certificato.

Il sistema sarà offline fino al completamento dell'aggiornamento e verrai disconnesso dall'interfaccia di ONTAP tools Manager.

# Accedi alla console di manutenzione degli strumenti ONTAP per VMware vSphere

## Scopri la console di manutenzione di ONTAP tools

La console di manutenzione per ONTAP tools for VMware vSphere ti permette di gestire le impostazioni di applicazione, sistema e rete. Puoi aggiornare le password di amministratore e di manutenzione, generare pacchetti di supporto, configurare i livelli di log, gestire le impostazioni TLS e abilitare la diagnostica remota.

Dopo aver distribuito ONTAP tools for VMware vSphere, se la console di manutenzione non è accessibile, installa VMware tools dal vCenter Server. Accedi utilizzando il `maint` nome utente e la password impostati durante la distribuzione. Usa **nano** per modificare i file nella console di manutenzione o nella console di accesso root.

Dovresti impostare una password per l' `diag`utente mentre abiliti la diagnostica remota.

Dovresti usare la scheda **Riepilogo** degli ONTAP tools for VMware vSphere distribuiti per accedere alla console di manutenzione. Quando selezioni , si avvia la console di manutenzione.

| Menu della console | Opzioni |
|---|---|
| Configurazione dell'applicazione | 1. Visualizza il riepilogo dello stato del server<br>2. Modifica il livello di LOG per i servizi degli ONTAP tools<br>3. Modifica il flag di convalida del certificato |
| Configurazione del sistema | 1. Riavvia la macchina virtuale<br>2. Arresta la macchina virtuale<br>3. Modifica la password dell'utente "maint"<br>4. Cambia fuso orario<br>5. Aumenta la dimensione del disco della jail (/jail)<br>6. Aggiornamento<br>7. Installa VMware Tools |

| | |
|---|---|
| Configurazione di rete | 1. Visualizza le impostazioni dell'indirizzo IP<br>2. Visualizza le impostazioni di ricerca del domain name<br>3. Modifica le impostazioni di ricerca del domain name<br>4. Visualizza percorsi statici<br>5. Modifica i percorsi statici<br>6. Conferma le modifiche<br>7. Esegui il ping di un host<br>8. Ripristina le impostazioni predefinite |
| Supporto e diagnostica | 1. Accedi alla shell diagnostica<br>2. Abilita l'accesso diagnostico remoto<br>3. Fornisci le credenziali vCenter per il backup<br>4. Esegui un backup |

## Configurare l'accesso diagnostico remoto per ONTAP tools

Puoi configurare ONTAP tools for VMware vSphere per abilitare l'accesso SSH per l'utente diag.

**Prima di iniziare**

Abilita l'estensione VASA Provider per la tua istanza del server vCenter.

**Informazioni su questa attività**

L'utilizzo di SSH per accedere all'account utente diag presenta le seguenti limitazioni:

- Puoi avere solo un account di accesso per ogni attivazione di SSH.
- L'accesso SSH all'account utente diag viene disabilitato quando si verifica una delle seguenti condizioni:
  - Il tempo è scaduto.

    La sessione di accesso scade a mezzanotte del giorno successivo.
  - Accedi nuovamente come utente diag tramite SSH.

**Passaggi**

1. Dal vCenter Server, apri una console per VASA Provider.
2. Accedi come utente di manutenzione.
3. Premi `4` per selezionare **Supporto e diagnostica**.
4. Premi Invio `2` per selezionare **Abilita accesso alla diagnostica remota**.
5. Inserisci `y` nella finestra di dialogo di conferma per abilitare l'accesso diagnostico remoto.
6. Inserisci una password per l'accesso diagnostico remoto.

## Avvia SSH sugli altri nodi di ONTAP tools

Devi avviare SSH sugli altri nodi prima di eseguire l'upgrade.

**Prima di iniziare**

Abilita l'estensione VASA Provider per la tua istanza del server vCenter.

**Informazioni su questa attività**

Ripeti questa procedura su ogni nodo prima dell'aggiornamento.

**Passaggi**

1. Dal vCenter Server, apri una console per VASA Provider.
2. Accedi come utente di manutenzione.
3. Premi `4` per selezionare Supporto e diagnostica.
4. Premi `1` per selezionare Access diagnostic shell.
5. Premi `y` per procedere.
6. Esegui il comando *sudo systemctl restart ssh*.

## Aggiorna le credenziali del server vCenter negli ONTAP tools

Puoi aggiornare le credenziali dell'istanza vCenter Server usando la console di manutenzione.

**Prima di iniziare**

Devi avere le credenziali di accesso dell'utente di manutenzione.

**Informazioni su questa attività**

Se hai modificato le credenziali del server vCenter dopo la distribuzione, aggiornale seguendo questa procedura.

**Passaggi**

1. Dal vCenter Server, apri una console per VASA Provider.
2. Accedi come utente di manutenzione.
3. Premi Invio `2` per selezionare il menu Configurazione di sistema.
4. Inserisci `8` per modificare le credenziali di vCenter.

## Modificare il flag di convalida del certificato negli ONTAP tools

Per impostazione predefinita, il flag di convalida del certificato è abilitato (impostato su true). Puoi impostare il flag di convalida del certificato del backend di storage ONTAP su false se hai bisogno di bypassare i controlli del certificato SAN. Questa impostazione non si applica ai certificati del server vCenter.

**Prima di iniziare**

Devi avere le credenziali di accesso dell'utente di manutenzione.

**Passaggi**

1. Dal vCenter Server, apri una console per ONTAP tools.
2. Accedi come utente di manutenzione.
3. Premi Invio `1` per selezionare il menu **Application Configuration**.
4. Inserisci `3` per modificare il flag di convalida del certificato.

   La console di manutenzione mostra lo stato del flag di convalida del certificato e ti invita a modificarlo.

5. Digita 'y' per attivare/disattivare il flag o 'n' per annullare.

Quando abiliti il flag di convalida del certificato (impostato su true), ONTAP tools verifica che tutti i backend di storage utilizzino certificati con un Subject Alternative Name (SAN). Se un backend utilizza un certificato senza SAN, non puoi abilitare la convalida del certificato. Prima di abilitare questo flag, verifica che tutti i backend di storage utilizzino certificati basati su SAN. Se disabiliti il flag di convalida del certificato (impostato su false), ONTAP tools ignora la convalida del certificato per tutti i backend di storage configurati.

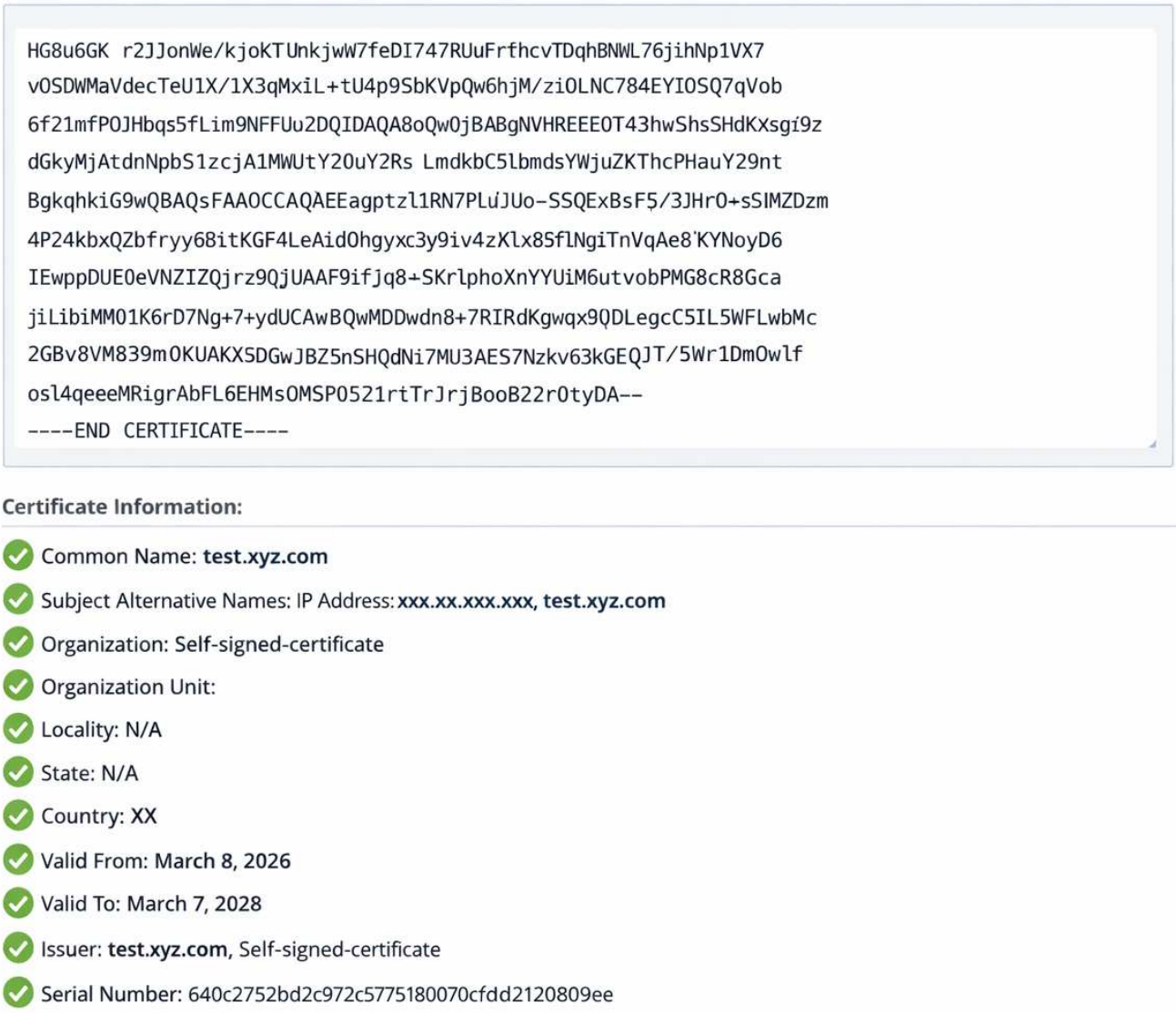
**Verificare i certificati basati su SAN per i backend di storage**

Per garantire una comunicazione sicura e una convalida adeguata, verificare che tutti i backend di archiviazione utilizzino certificati basati su SAN:

1. Verificare che il certificato di gestione ONTAP includa una voce Subject Alternative Name (SAN).
2. Confermare che le voci SAN corrispondano all'indirizzo IP di gestione ONTAP o al nome DNS, o a entrambi.
3. Assicurarsi che i dettagli utilizzati per integrare ONTAP corrispondano all'indirizzo IP o al nome DNS nella voce SAN del certificato.

Seguendo questi passaggi si evitano problemi di convalida dei certificati e si garantisce che il sistema ONTAP sia integrato in modo sicuro.

Il seguente certificato di esempio mostra le informazioni decodificate:




# Report degli strumenti ONTAP

Il plug-in ONTAP tools for VMware vSphere fornisce report per macchine virtuali e datastore. Quando selezioni l'icona del plug-in NetApp ONTAP tools for VMware vSphere nella sezione scorciatoie del client vCenter, l'interfaccia utente passa alla pagina Panoramica. Seleziona la scheda Report per visualizzare il report delle macchine virtuali e dei datastore.

Il report Macchine virtuali mostra l'elenco delle macchine virtuali rilevate (che devono avere almeno un disco proveniente da datastore basati su ONTAP storage) con metriche sulle prestazioni. Quando espandi il record della macchina virtuale, l'interfaccia visualizza tutte le informazioni relative al datastore e al disco.

Il report sui datastore elenca i datastore rilevati o riconosciuti dagli ONTAP tools for VMware vSphere che utilizzano qualsiasi storage ONTAP, con metriche sulle prestazioni.

Puoi usare l'opzione Gestisci colonne per nascondere o mostrare diverse colonne.

# Gestisci le macchine virtuali

## Considerazioni sulla migrazione e la clonazione di macchine virtuali per ONTAP tools

ONTAP tools for VMware vSphere supportano tutti i principali tipi di migrazione di macchine virtuali, incluse le migrazioni di sola elaborazione (vMotion), di sola archiviazione (Storage vMotion) e quelle combinate di elaborazione e archiviazione su tutti i datastore. Questo argomento illustra le considerazioni chiave e le best practice per garantire la corretta migrazione e clonazione delle macchine virtuali, indipendentemente dal tipo di datastore sottostante.

### Migra le macchine virtuali protette

È possibile migrare le macchine virtuali protette a:

- Lo stesso datastore su un host ESXi diverso
- Un datastore compatibile diverso sullo stesso host ESXi
- Un datastore compatibile diverso su un host ESXi diverso

Se si migra una macchina virtuale su un volume FlexVol diverso, il sistema aggiorna il file di metadati di tale volume con le informazioni della macchina virtuale. Se una macchina virtuale viene migrata su un host ESXi diverso ma sullo stesso storage, il file di metadati del volume FlexVol sottostante non verrà modificato.

Per informazioni sulla migrazione delle macchine virtuali, consulta la documentazione Broadcom: "Documentazione Tecnica Broadcom".

### Clona le macchine virtuali protette

Puoi clonare macchine virtuali protette nei seguenti:

- Lo stesso container dello stesso FlexVol volume utilizzando un gruppo di replica

  Il file di metadati dello stesso volume FlexVol viene aggiornato con i dettagli della macchina virtuale clonata.

- Lo stesso container di un volume FlexVol diverso utilizzando un gruppo di replica

  Nel volume FlexVol in cui è posizionata la macchina virtuale clonata, il file di metadati viene aggiornato con i dettagli della macchina virtuale clonata.

- Un container o vVols datastore diverso

  Nel volume FlexVol in cui è posizionata la macchina virtuale clonata, il file di metadati viene aggiornato con i dettagli della macchina virtuale.

Attualmente VMware non supporta le macchine virtuali clonate in un modello di macchina virtuale.

È supportata la clonazione di una clonazione di una macchina virtuale protetta.

Consultare la documentazione Broadcom: "Creazione di una macchina virtuale per la clonazione" per maggiori dettagli.

### Snapshot di macchine virtuali

ONTAP tools supporta gli snapshot delle macchine virtuali tramite i flussi di lavoro VMware standard. Gli snapshot sono punti di ripristino a breve termine, pensati per casi d'uso quali test e preparazione di patch. Non sono un sostituto del backup o della protezione dei dati basata sulla replica. L'esecuzione di una macchina virtuale su uno snapshot per periodi prolungati può causare instabilità e perdita di dati.

È possibile creare snapshot coerenti con gli arresti anomali (snapshot senza stato della memoria, utilizzabili per riavviare la macchina virtuale in uno stato coerente) su tutti i tipi di datastore supportati. Sono supportati anche gli snapshot quiescenti, che utilizzano VMware Tools per scrivere i dati in memoria su disco prima dell'acquisizione. Per una panoramica dei tipi di snapshot e del loro comportamento, consultare "Panoramica delle snapshot delle macchine virtuali in vSphere".

> Gli snapshot di memoria catturano lo stato della memoria in esecuzione e bloccano temporaneamente la macchina virtuale. Non sono supportati nei workflow degli ONTAP tools. Se una macchina virtuale dispone di uno snapshot di memoria, è necessario eliminarlo prima che la macchina virtuale possa essere inclusa in un gruppo di coerenza o in una relazione di cluster host gestita dagli ONTAP tools.

Nei sistemi di storage ASA r2, il comportamento degli snapshot delle macchine virtuali differisce da quello di altri tipi di storage. Gli snapshot sono di sola lettura. Quando si accende la macchina virtuale, VASA Provider crea una LUN dallo snapshot di sola lettura e abilita le IOPS. Quando si spegne la macchina virtuale, VASA Provider elimina la LUN e disabilita le IOPS.

Per informazioni sulla gestione degli snapshot delle macchine virtuali, consultare la documentazione Broadcom "Documentazione Tecnica Broadcom".

## Migrare le macchine virtuali negli archivi dati vVols in ONTAP tools

Puoi migrare le macchine virtuali dai datastore NFS e VMFS ai datastore Virtual Volumes (vVols) per sfruttare la gestione delle VM basata su policy e le altre funzionalità di vVols. I datastore vVols ti permettono di soddisfare requisiti di carico di lavoro più elevati.

#### Prima di iniziare

Assicurati che VASA Provider non sia in esecuzione su nessuna delle macchine virtuali che intendi migrare. Se migri una macchina virtuale su cui è in esecuzione VASA Provider verso un datastore vVols, non puoi eseguire nessuna operazione di gestione, incluso l'avvio delle macchine virtuali che si trovano sui datastore vVols.

#### Informazioni su questa attività

Quando migri da un datastore NFS e VMFS a un datastore vVols, il server vCenter utilizza le vStorage APIs for Array Integration (VAAI) per lo spostamento dei dati dai datastore VMFS, ma non da un file VMDK NFS. Gli offload VAAI normalmente riducono il carico sull'host.

#### Passaggi

1. Fai clic con il pulsante destro del mouse sulla macchina virtuale che desideri migrare e seleziona **Migra**.
2. Seleziona **Modifica solo lo storage** e poi seleziona **Avanti**.
3. Seleziona un formato di disco virtuale, una VM Storage Policy e un vVol datastore che corrispondano alle caratteristiche del datastore che stai migrando.
4. Rivedi le impostazioni e seleziona **Fine**.

## Pulisci le configurazioni VASA negli ONTAP tools

Per completare il processo di bonifica VASA, segui questi passaggi.

Si consiglia di rimuovere tutti i datastore vVols prima di avviare la pulizia di VASA.

**Passaggi**

1. Annulla la registrazione del plug-in andando in https://OTV_IP:8143/Register.html
2. Verifica che il plug-in non sia più disponibile sul vCenter Server.
3. Spegni la VM ONTAP tools for VMware vSphere.
4. Elimina la VM ONTAP tools for VMware vSphere.

## Collegare o scollegare un disco dati da una VM in ONTAP tools

Segui questi passaggi per collegare o scollegare i dischi dati dalle macchine virtuali in vSphere e gestirne le risorse di storage.

### Collega un disco dati a una macchina virtuale

Collega un disco dati a una macchina virtuale per aggiungere più storage.

**Passaggi**

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su una macchina virtuale nell'inventario e seleziona **Modifica impostazioni**.
3. Nella scheda **Hardware virtuale**, seleziona **Disco rigido esistente**.
4. Seleziona la macchina virtuale in cui si trova il disco.
5. Seleziona il disco che vuoi collegare e seleziona il pulsante **OK**.

**Risultato**

Il disco rigido compare nell'elenco dei dispositivi hardware virtuali.

### Scollega un disco dati dalla macchina virtuale

Scollega un disco dati da una macchina virtuale quando non ti serve più. Il disco non viene eliminato; rimane sul sistema storage ONTAP.

**Passaggi**

1. Accedi al vSphere client.
2. Fai clic con il pulsante destro del mouse su una macchina virtuale nell'inventario e seleziona **Modifica impostazioni**.
3. Posiziona il puntatore sul disco e seleziona **Rimuovi**.

Il disco viene rimosso dalla macchina virtuale. Se altre macchine virtuali condividono il disco, i file del disco non vengono eliminati.

**Informazioni correlate**

"Aggiungi un nuovo disco rigido a una macchina virtuale"

"Aggiungi un disco rigido esistente a una macchina virtuale"

# Scopri i sistemi di archiviazione e gli host negli ONTAP tools

Quando ONTAP tools for VMware vSphere viene avviato nel Client vSphere per la prima volta, rileva automaticamente gli host ESXi, le relative LUN e le esportazioni NFS, nonché i sistemi storage NetApp che possiedono queste risorse.

**Prima di iniziare**

- Assicurati che tutti gli host ESXi siano accesi e connessi.
- Assicurati che tutte le macchine virtuali di storage (SVM) da rilevare siano in esecuzione e che ogni nodo del cluster abbia almeno una LIF dati configurata per il protocollo storage in uso (NFS o iSCSI).

**Informazioni su questa attività**

Puoi individuare nuovi sistemi storage o aggiornare quelli esistenti per ottenere le ultime informazioni su capacità e configurazione. Puoi anche cambiare le credenziali di ONTAP tools for VMware vSphere per l'accesso ai sistemi storage.

Durante la fase di rilevamento dei sistemi storage, ONTAP tools for VMware vSphere raccoglie informazioni dagli host ESXi gestiti dall'istanza vCenter Server.

**Passaggi**

1. Dalla home page del client vSphere, seleziona **Host e cluster**.
2. Fare clic con il pulsante destro del mouse sul data center desiderato e selezionare **NetApp ONTAP tools** > **Aggiorna dati host**.

   Nella finestra di dialogo **Conferma**, conferma la tua scelta.

3. Seleziona i controller di storage rilevati che hanno lo stato `Authentication Failure` e seleziona **Azioni** > **Modifica**.
4. Inserisci le informazioni richieste nella finestra di dialogo **Modifica sistema storage**.
5. Ripeti i passaggi 4 e 5 per tutti i controller di storage con stato `Authentication Failure`.

Una volta completata la fase di rilevamento, esegui le seguenti azioni:

- Usa ONTAP tools for VMware vSphere per configurare le impostazioni dell'host ESXi per gli host che visualizzano l'icona di avviso nella colonna delle impostazioni dell'adattatore, nella colonna delle impostazioni MPIO o nella colonna delle impostazioni NFS.
- Fornisci le credenziali del sistema storage.

# Modifica le impostazioni dell'host ESXi usando ONTAP tools

Utilizza la dashboard degli ONTAP tools in VMware vSphere per identificare i problemi di configurazione, selezionare gli host ESXi, esaminare le impostazioni consigliate da

NetApp e applicarle.

**Prima di iniziare**

Il portlet dei sistemi host ESXi visualizza i problemi relativi alle impostazioni dell'host ESXi. Seleziona un problema per visualizzare l'host name o l'indirizzo IP.

**Passaggi**

1. Accedi al vSphere client.
2. Nella pagina dei collegamenti rapidi, seleziona **NetApp ONTAP tools** nella sezione dei plug-in.
3. Vai al portlet **Conformità host ESXi** nella Panoramica (dashboard) del plug-in ONTAP tools for VMware vSphere.
4. Seleziona il link **Applica impostazioni consigliate**.
5. Nella finestra **Applica impostazioni host consigliate**, seleziona gli host per cui vuoi usare le impostazioni host consigliate NetApp e seleziona **Avanti**.

   Puoi espandere l'host ESXi per vedere i valori attuali.

6. Nella pagina delle impostazioni, seleziona i valori consigliati come richiesto.
7. Nel riquadro di riepilogo, verifica i valori e seleziona **Fine**. Puoi monitorare l'avanzamento nel pannello delle attività recenti.

**Informazioni correlate**

"Configura le impostazioni dell'host ESXi"

# Gestisci le password

## Cambia la password di ONTAP tools Manager

Puoi cambiare la password dell'amministratore usando ONTAP tools Manager.

**Passaggi**

1. Avvia ONTAP tools Manager da un browser web:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con le credenziali di amministratore degli ONTAP tools for VMware vSphere.
3. Seleziona l'icona **administrator** nell'angolo in alto a destra dello schermo e seleziona **Change password**.
4. Nella finestra a comparsa per la modifica della password, inserisci la vecchia e la nuova password. La schermata dell'interfaccia utente mostra i requisiti della password.
5. Seleziona **Modifica** per applicare le modifiche.

## Reimposta la password di ONTAP tools Manager

Se dimentichi la password di ONTAP tools Manager, puoi ripristinare l'accesso amministratore usando un token di reset generato dalla console di manutenzione di ONTAP tools for VMware vSphere.

**Passaggi**

1. Apri un browser web e vai su `https://<ONTAPtoolsIP>:8443/virtualization/ui/` per accedere a ONTAP tools Manager.
2. Nella pagina di accesso, seleziona **Reimposta password**.
3. Genera un token di reimpostazione della password utilizzando la console di manutenzione di ONTAP tools for VMware vSphere:
   a. Accedi al vCenter Server e apri la console di manutenzione.
   b. Premi Invio `2` per selezionare **Configurazione di sistema**.
   c. Premi `3` per selezionare **Cambia password utente 'maint'**.
4. Nella finestra di dialogo per il ripristino della password, inserisci il token di ripristino, il nome utente e la nuova password.
5. Seleziona **Ripristina** per aggiornare le credenziali.
6. Accedi a ONTAP tools Manager con la nuova password.

## Reimposta la password utente dell'applicazione in ONTAP tools

Segui questi passaggi per reimpostare la password dell'utente dell'applicazione necessaria per la registrazione SRA e VASA Provider con vCenter Server utilizzando ONTAP tools for VMware vSphere.

**Passaggi**

1. Apri un browser web e vai a: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi utilizzando le credenziali di amministratore configurate durante la distribuzione degli ONTAP tools.
3. Dalla barra laterale, seleziona **Impostazioni**.
4. Nella pagina **Credenziali VASA/SRA**, seleziona **Reimposta password**.
5. Inserisci e conferma la nuova password.
6. Seleziona **Reset** per applicare la nuova password.

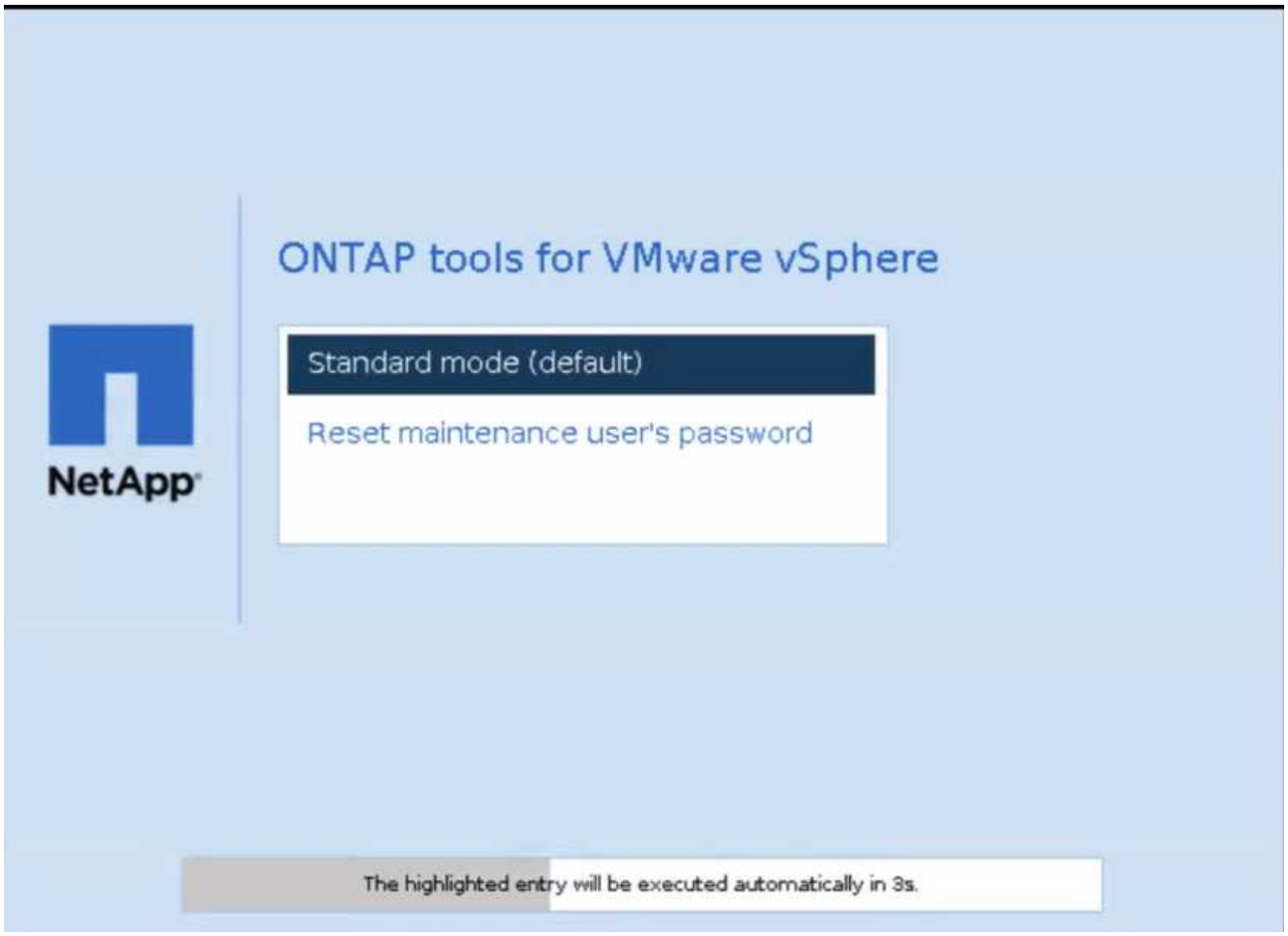
## Reimposta la password della console di manutenzione di ONTAP tools

Durante un'operazione di riavvio del sistema operativo guest, il menu GRUB visualizza un'opzione per reimpostare la password dell'utente della console di manutenzione. Utilizzare questa opzione per aggiornare la password dell'utente della console di manutenzione sulla VM. Dopo aver reimpostato la password, la VM si riavvia per impostare la nuova password. In uno scenario di distribuzione HA, dopo il riavvio della VM, la password viene aggiornata automaticamente sulle altre due VM.

> Per la distribuzione HA di ONTAP tools for VMware vSphere, dovresti cambiare la password dell'utente della console di manutenzione sul nodo di gestione di ONTAP tools, cioè node1.

**Passaggi**

1. Accedi al tuo vCenter Server
2. Fai clic con il pulsante destro del mouse sulla macchina virtuale e seleziona **Power** > **Restart Guest OS**. Durante il riavvio del sistema, viene visualizzata la seguente schermata:




Hai 5 secondi per scegliere la tua opzione. Premi un tasto qualsiasi per interrompere l'operazione e bloccare il menu GRUB.

3. Seleziona l'opzione **Reimposta la password dell'utente di manutenzione**. Si apre la console di manutenzione.
4. Nella console, inserisci e conferma la nuova password. Hai tre tentativi. Il sistema si riavvia dopo che hai inserito correttamente la nuova password.
5. Premi **Invio** per continuare. Il sistema aggiorna la password sulla VM.

Lo stesso menu GRUB appare all'avvio della macchina virtuale. Tuttavia, è consigliabile utilizzare l'opzione di reimpostazione della password solo con l'opzione **Riavvia il sistema operativo guest**.

# Gestisci la protezione del cluster host

## Modificare un cluster host protetto in ONTAP tools

Puoi modificare le impostazioni di protezione per un cluster host in un unico flusso di lavoro. Sono supportate le seguenti modifiche:

- Aggiungi nuovi datastore o host al cluster protetto.
- Aggiungi nuove relazioni di SnapMirror alle impostazioni di protezione.

- Elimina le relazioni SnapMirror esistenti dalle impostazioni di protezione.
- Modifica una relazione di SnapMirror esistente.

> Devi eseguire il rilevamento dello storage dopo aver creato, modificato o eliminato la protezione per un cluster di host, così da riflettere le modifiche. Se non esegui il rilevamento dello storage, le modifiche vengono riflesse solo dopo che viene attivato il rilevamento periodico dello storage.

### Monitora la protezione del cluster host

Monitora lo stato di protezione, le relazioni di SnapMirror, i datastore e lo stato di SnapMirror per ogni cluster protetto.

**Passaggi**

1. Accedi al vSphere client.
2. Vai a **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**.

   La colonna Protezione visualizza un'icona che mostra lo stato della protezione.

3. Passa il mouse sopra l'icona per visualizzare maggiori dettagli.

### Aggiungi nuovi datastore o host

Aggiungi host o crea datastore sul cluster protetto utilizzando l'interfaccia utente di vCenter.

**Passaggi**

1. Accedi al vSphere client.
2. Per modificare le proprietà di un cluster protetto, puoi
   a. Vai su **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, seleziona il menu con i puntini di sospensione accanto al cluster e seleziona **Modifica** oppure
   b. Fai clic con il pulsante destro del mouse su un cluster e seleziona **NetApp ONTAP tools** > **Protect Cluster**.
3. Se crei un datastore nell'interfaccia utente di vCenter, viene visualizzato come non protetto. Puoi visualizzare tutti i datastore nel cluster e il loro stato di protezione in una finestra di dialogo. Seleziona il pulsante **Proteggi** per abilitare la protezione.

   > Dopo aver creato un datastore nell'interfaccia utente del server vCenter, seleziona **Scopri** nella pagina di panoramica per visualizzare il datastore come candidato per la protezione nel cluster host. Lo stato di protezione si aggiorna a protetto dopo il successivo rilevamento periodico della protezione.

4. Se aggiungi un nuovo host ESXi, lo stato di protezione viene visualizzato come parzialmente protetto. Seleziona il menu con i tre puntini sotto le impostazioni di SnapMirror e seleziona **Modifica** per impostare la prossimità dell'host ESXi appena aggiunto.

   > Per le relazioni asincrone, la modifica non è supportata negli ONTAP tools perché l'SVM di destinazione per un sito terziario non può essere aggiunta alla stessa istanza. Per modificare la configurazione della relazione, usa System Manager o la CLI sull'SVM di destinazione.

5. Dopo aver apportato le modifiche, seleziona **Salva**.

6. Puoi vedere le modifiche nella finestra **Proteggi cluster**.

ONTAP tools crea un'attività vCenter e puoi monitorarne l'avanzamento nel pannello **Attività recenti**.

### Aggiungi una nuova SnapMirror relazione

**Passaggi**

1. Accedi al vSphere client.
2. Per modificare le proprietà di un cluster protetto, puoi
   a. Vai su **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, seleziona il menu con i puntini di sospensione accanto al cluster e seleziona **Modifica** oppure
   b. Fai clic con il pulsante destro del mouse su un cluster e seleziona **NetApp ONTAP tools** > **Protect Cluster**.
3. Seleziona **Aggiungi relazione**.
4. Aggiungi una nuova relazione come tipo di policy **Asincrona** o **AutomatedFailOverDuplex**.
5. Seleziona **Protect**.

   Puoi vedere le modifiche nella finestra **Proteggi cluster**.

ONTAP tools crea un'attività vCenter e puoi monitorarne l'avanzamento nel pannello **Attività recenti**.

### Elimina una relazione di SnapMirror esistente

Per eliminare una relazione asincrona di SnapMirror, assicurati che l'SVM o il cluster del sito secondario sia aggiunto come storage backend in ONTAP tools for VMware vSphere. Non puoi eliminare tutte le relazioni di SnapMirror contemporaneamente. Eliminando una relazione, viene rimossa anche la corrispondente relazione dal cluster ONTAP. Quando elimini una relazione di SnapMirror Automated Failover Duplex, il sistema annulla la mappatura dei datastore di destinazione ed elimina il consistency group, le LUN, i volumi e gli igroup dal cluster ONTAP di destinazione.

Quando elimini la relazione, il sistema esegue una nuova scansione del sito secondario per rimuovere il LUN non mappato come percorso attivo dagli host.

**Passaggi**

1. Accedi al vSphere client.
2. Per modificare le proprietà di un cluster protetto, puoi
   a. Vai su **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, seleziona il menu con i puntini di sospensione accanto al cluster e seleziona **Modifica** oppure
   b. Fai clic con il pulsante destro del mouse su un cluster e seleziona **NetApp ONTAP tools** > **Protect Cluster**.
3. Seleziona il menu con i tre puntini sotto le impostazioni di SnapMirror e seleziona **Elimina**.
   - Se elimini una relazione basata su policy asincrona di un cluster host protetto, devi rimuovere manualmente gli elementi di storage dal cluster di storage terziario. Gli elementi di storage includono gruppi di coerenza, volumi (per sistemi ONTAP), unità di storage (LUN/Namespaces) e snapshot.
   - Se elimini una relazione basata su policy Automated Failover Duplex (AFD) di un cluster protetto, puoi scegliere di rimuovere gli elementi di storage associati sullo storage secondario direttamente dall'interfaccia.

◦ Se elimini una relazione basata su policy Automated Failover Duplex (AFD) e il gruppo di coerenza è ora gerarchico per i backup a livello di applicazione, viene visualizzato un avviso relativo all'impatto sul backup. Conferma per procedere. Dopo la conferma, elimina gli elementi di storage associati nello storage secondario. Se non li rimuovi, rimangono nel sito secondario.

ONTAP tools crea un'attività vCenter e puoi monitorarne l'avanzamento nel pannello **Attività recenti**.

#### Modifica una relazione di SnapMirror esistente

Per modificare una relazione asincrona di SnapMirror, assicurati che l'SVM o il cluster del sito secondario sia aggiunto come storage backend in ONTAP tools for VMware vSphere. Per le relazioni di Automated Failover Duplex SnapMirror, puoi aggiornare la prossimità dell'host per le configurazioni uniformi o l'accesso dell'host per le configurazioni non uniformi. Il passaggio tra i tipi di policy Asynchronous e Automated Failover Duplex non è supportato. Puoi configurare le impostazioni di prossimità o di accesso per gli host appena scoperti nel cluster.

Non puoi modificare una relazione asincrona di SnapMirror esistente.

**Passaggi**

1. Accedi al vSphere client.
2. Per modificare le proprietà di un cluster protetto, puoi
   a. Vai su **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**, seleziona il menu con i puntini di sospensione accanto al cluster e seleziona **Modifica** oppure
   b. Fai clic con il pulsante destro del mouse su un cluster e seleziona **NetApp ONTAP tools** > **Protect Cluster**.
3. Se è selezionato il tipo di criterio AutomatedFailOverDuplex, aggiungi i dettagli di prossimità dell'host o di accesso all'host.
4. Seleziona il pulsante **Protect**.

Gli ONTAP tools creano un'attività vCenter. Monitora l'avanzamento nel pannello **Attività recenti**.

## Rimuovere la protezione del cluster host negli ONTAP tools

Quando rimuovi la protezione del cluster host, i datastore diventano non protetti.

**Passaggi**

1. Per visualizzare l'elenco dei cluster host protetti, vai su **NetApp ONTAP tools** > **Protection** > **Host cluster relationships**.

   In questa pagina è possibile monitorare i cluster host protetti, lo stato di protezione, la relazione di SnapMirror e lo stato. Selezionare i gruppi di coerenza per visualizzare la capacità, i datastore associati e i gruppi secondari.

2. Nella finestra **Protezione cluster host**, seleziona il menu con i puntini di sospensione accanto al cluster e seleziona **Rimuovi protezione**.
   ◦ Se rimuovi la protezione da un cluster host con solo una relazione SnapMirror asincrona, devi eliminare manualmente gli elementi di storage. Gli elementi di storage includono gruppi di coerenza, volumi (per sistemi ONTAP), unità di storage (LUN) e snapshot.
   ◦ Se rimuovi la protezione da un cluster host con solo una relazione di policy SnapMirror basata su failover automatico duplex e un gruppo di coerenza non gerarchico, puoi eliminare gli elementi di

storage associati sullo storage secondario direttamente dalla stessa schermata.

- Se rimuovi la protezione da un cluster host con sia criteri SnapMirror che un gruppo di coerenza gerarchica per i backup, viene visualizzato un avviso relativo all'impatto sui backup. Conferma per procedere. Dopo la conferma, elimina gli elementi di storage associati sullo storage secondario. Se non esegui la pulizia, gli elementi di storage rimangono sul sito secondario.

# Ripristina la configurazione degli ONTAP tools

## A partire da ONTAP tools for VMware vSphere 10.5, la funzionalità di backup è abilitata per impostazione predefinita.

Il datastore in cui distribuisci ONTAP tools for VMware vSphere macchine virtuali memorizza i file di backup. Una cartella denominata con l'indirizzo IP di ONTAP tools (i punti sono sostituiti da trattini bassi e il nome è suffisso *OTV_backup*) contiene i due file di backup più recenti (*OTV_backup_1.tar.enc* e *OTV_backup_2.tar.enc*) e un file info (*OTV_backup_info.txt*) che contiene il nome dell'ultimo backup.

Assicurati che la nuova macchina virtuale utilizzi lo stesso indirizzo IP degli ONTAP tools e corrisponda alla configurazione iniziale del sistema, inclusi i servizi abilitati, la dimensione del nodo e la modalità HA.

**Passaggi**

1. Scarica i file di backup dal datastore della macchina virtuale originale sul tuo sistema locale.
   a. Vai alla sezione di archiviazione e scegli il datastore che contiene i file di backup della macchina virtuale.
   b. Seleziona la sezione **File**.
   c. Scarica la directory di backup necessaria.
2. Spegni la macchina virtuale esistente. Poi distribuisci una nuova macchina virtuale usando lo stesso file OVA della distribuzione originale.
3. Dal vCenter Server, apri la console di manutenzione.
4. Accedi come utente di manutenzione.
5. Premi `4` per selezionare **Supporto e diagnostica**.
6. Premi Invio `2` per selezionare l'opzione **Abilita accesso diagnostico remoto** e creare una nuova password per l'accesso diagnostico.
7. Seleziona un file di backup dalla cartella di download. Consulta il file *OTV_backup_info.txt* per identificare il backup più recente.
8. Usa il seguente comando per trasferire il file di backup sulla nuova macchina virtuale. Quando richiesto, inserisci la password di diagnostica.

```
scp <OTV_backup_X.tar.enc>
diag@<node_ip>:/home/diag/system_recovery.tar.enc
```

> Non modificare il percorso di destinazione e il nome del file (/home/diag/system_recovery.tar.enc) indicati nel comando.

9. Dopo il trasferimento del file di backup, accedi alla shell diagnostica ed esegui il seguente comando:

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

I log vengono registrati nel file */var/log/post-deploy-upgrade.log*.

Dopo che hai completato il ripristino, ONTAP tools ripristina i servizi e gli oggetti vCenter.

# Disinstallare ONTAP tools

La disinstallazione di ONTAP tools for VMware vSphere elimina tutti i dati negli strumenti.

**Passaggi**

1. Rimuovi o sposta tutte le macchine virtuali dai datastore gestiti da ONTAP tools for VMware vSphere.
   - Per rimuovere le macchine virtuali, fare riferimento a "Rimuovi e registra nuovamente le macchine virtuali e i modelli di macchine virtuali"
   - Per spostarli in un archivio dati non gestito, consulta "Documentazione Tecnica Broadcom".
2. "Elimina i datastore" creato su ONTAP tools for VMware vSphere.
3. Se hai abilitato il provider VASA, seleziona **Impostazioni** > **Impostazioni provider VASA** > **Annulla registrazione** in ONTAP tools per annullare la registrazione dei provider VASA da tutti i vCenter server.
4. Disassocia tutti i backend di storage dall'istanza del server vCenter. Consulta "Dissocia i backend di storage con l'istanza del server vCenter".
5. Elimina tutti i backend di archiviazione. Consulta "Gestisci i backend di storage".
6. Rimuovi l'adattatore SRA da VMware Live Site Recovery:
   a. Accedi come admin all'interfaccia di gestione dell'appliance VMware Live Site Recovery utilizzando la porta 5480.
   b. Seleziona **Storage Replication Adapters**.
   c. Seleziona la scheda SRA appropriata e, dal menu a tendina, seleziona **Elimina**.
   d. Conferma che conosci i risultati dell'eliminazione dell'adattatore e seleziona **Elimina**.
7. Elimina le istanze del server vCenter aggiunte a ONTAP tools for VMware vSphere. Consulta "Gestisci le istanze del server vCenter".
8. Spegni le VM ONTAP tools for VMware vSphere dal server vCenter ed elimina le VM.

**E adesso?**

"Rimuovi i volumi FlexVol"

# Rimuovere i volumi FlexVol dopo aver disinstallato ONTAP tools

Quando usi un cluster ONTAP dedicato per la distribuzione di ONTAP tools for VMware, vengono creati molti volumi FlexVol inutilizzati. Dopo aver rimosso ONTAP tools for VMware vSphere, dovresti rimuovere i volumi FlexVol per evitare possibili impatti sulle prestazioni.

**Passaggi**

1. Scopri il tipo di distribuzione degli ONTAP tools for VMware vSphere dalla VM del nodo di gestione degli ONTAP tools. Esegui il seguente comando per verificare il tipo di distribuzione: *cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol*

   Se si tratta di una distribuzione iSCSI, elimina anche gli igroup.

2. Ottieni l'elenco dei volumi FlexVol. *kubectl describe persistentvolumes | grep internalName | awk -F'=' '{print $2}'*
3. Rimuovere le VM dal vCenter Server. Consulta "Rimuovi e registra nuovamente le macchine virtuali e i modelli di macchine virtuali".
4. Elimina i volumi FlexVol. Consulta "Elimina un volume FlexVol". Inserisci il nome esatto del volume FlexVol nel comando CLI per eliminare un volume.
5. Eliminare gli igroup SAN dal sistema storage ONTAP in caso di implementazione iSCSI. Consulta "Visualizza e gestisci gli iniziatori SAN e gli igroups".

# Aggiorna ONTAP tools per VMware vSphere

## Aggiorna da ONTAP tools for VMware vSphere 10.x a 10.5

Puoi eseguire l'aggiornamento da ONTAP tools for VMware vSphere 10.3 o 10.4 a 10.5. Tuttavia, per eseguire l'aggiornamento da ONTAP tools 10.0, 10.1 o 10.2 a 10.5, devi prima aggiornare a 10.3 o 10.4 prima di procedere a 10.5.

- Per i sistemi ASA r2, assicurarsi di aggiornare ONTAP tools for VMware vSphere alla versione 10.5 e ONTAP alla versione 9.16.1, prima di configurare ulteriori storage availability zones (SAZ).
- Se l'upgrade da ONTAP tools for VMware vSphere 10.3 o 10.4 a 10.5 non va a buon fine, non puoi eseguire il rollback. Usa un basso RPO o il ripristino tramite snapshot per ripristinare la configurazione. Per ONTAP tools for VMware vSphere 10.2 e versioni precedenti, usa zero-RPO per ripristinare la configurazione.

**Prima di iniziare**

- Assicurati che tutti i nodi siano attivi.
- Assicurati che il certificato di sistema ONTAP e i certificati vCenter integrati siano validi per almeno 5 giorni. Se i certificati scadono prima, l'aggiornamento fallisce.
- Assicurati di avere un quinto disco con una capacità di 100 GB su tutti i nodi.
- Verifica che la configurazione del nodo corrisponda alle specifiche riportate nella tabella sottostante.

| Tipo di implementazione | CPU (Core) per nodo | Memoria (GB) per nodo | Spazio su disco (GB) per nodo | CPU totale (Core) | Memoria (GB) | Spazio totale su disco (GB) |
|---|---|---|---|---|---|---|
| Non-HA Piccolo | 9 | 18 | 350 | 9 | 18 | 350 |
| Non-HA medio | 13 | 26 | 350 | 13 | 26 | 350 |
| HA Small | 9 | 18 | 350 | 27 | 54 | 1050 |
| HA Medium | 13 | 26 | 350 | 39 | 78 | 1050 |
| HA Large | 17 | 34 | 350 | 51 | 102 | 1050 |

- Assicurati che la funzionalità hot plug-in per CPU e RAM sia abilitata.
- Abilita il backup con RPO basso e assicurati che almeno un backup sia visibile nell'interfaccia del vCenter Client. Scarica la cartella di backup prima dell'upgrade.
- Si consiglia un backup con RPO basso. Tuttavia, nelle implementazioni non HA, puoi creare uno snapshot quiescente della macchina virtuale degli ONTAP tools prima dell'aggiornamento.

  Consulta "Modifica le impostazioni di backup" e "Ripristina la configurazione degli ONTAP tools" per maggiori informazioni su backup e ripristino.

**Passaggi**

1. Carica l'ISO di aggiornamento di ONTAP tools for VMware vSphere nell'archivio di contenuti.
2. Nella pagina della VM principale, seleziona **Azioni** > **Modifica impostazioni**. Per identificare il nome della VM principale:
   a. Abilita la shell di diagnostica su qualsiasi nodo
   b. Eseguire il seguente comando:
   `grep sourceHost /opt/netapp/meta/ansible_vars.yaml`
3. Nella finestra delle impostazioni di modifica, seleziona il file **ISO dell'archivio di contenuti** nel campo **unità CD/DVD**.
4. Seleziona il file ISO, seleziona la casella **Connesso** per il campo **CD/DVD drive** e fai clic su **OK**.
5. Dal vCenter Server, apri una console per ONTAP tools.
6. Accedi come utente di manutenzione.
7. Digita **2** per selezionare il menu **Configurazione di sistema**.
8. Digita **6** per selezionare l'opzione **Upgrade**.
9. Fornisci le credenziali vCenter quando richiesto. Questa è l'istanza vCenter in cui è ospitato ONTAP tools.

   Se si utilizzano gli strumenti ONTAP in una topologia a due vCenter Server, in cui l'appliance è ospitata in un'istanza vCenter e ne gestisce un'altra, è possibile assegnare un ruolo con restrizioni per l'istanza vCenter che ospita gli strumenti ONTAP. È possibile creare un utente e un ruolo vCenter dedicati con solo le autorizzazioni necessarie per la distribuzione del modello OVF. Per dettagli, consultare i ruoli elencati in "Ruoli inclusi con ONTAP tools for VMware vSphere 10".

   Per l'istanza vCenter che verrà gestita da ONTAP tools, assicurati che l'account utente vCenter abbia i privilegi di amministratore.

   Durante l'aggiornamento, se a uno qualsiasi dei certificati backend di storage integrati mancano le voci Subject Alternative Name (SAN), riceverai un messaggio che indica il SAN mancante. Se scegli di procedere senza convalidare il SAN, l'aggiornamento continuerà, ma questa scelta non è consigliata a causa dei potenziali rischi per la sicurezza.

10. Quando esegui l'aggiornamento, le seguenti azioni vengono eseguite automaticamente:
    a. Il certificato gateway viene rinnovato con un periodo di validità di 1 anno. Quando rimuovi il precedente adattatore SRA e carichi il nuovo adattatore 10.5, la validità del certificato SRA passa da 10 anni a 1 anno.
    b. Il plug-in remoto è stato aggiornato
    c. I certificati di ONTAP e del server vCenter vengono convalidati e aggiunti agli ONTAP tools
    d. Il backup è abilitato

**Cosa c'è dopo**

Dopo l'aggiornamento a ONTAP tools for VMware vSphere 10.5:

- Monitora gli avvisi di sistema e pianifica di rinnovare il certificato gateway prima che scada tra un anno.
- Rimuovi l'adattatore SRA di ONTAP tools 10.4 o 10.3 e carica il file tar dell'adattatore SRA 10.5.
- Esegui il comando di installazione dopo aver caricato il file tar dell'adattatore SRA. Poi, esegui una nuova scansione degli adattatori SRA per aggiornare la pagina Adattatori di replica dello storage di VMware Site Recovery.

Dopo l'aggiornamento potrai:

- Disabilita i servizi dall'interfaccia utente del manager
- Passa da una configurazione non HA a una configurazione HA
- Scala una configurazione piccola non HA a una media non HA, oppure a una configurazione media o grande HA.

**Informazioni correlate**

"Migra dagli ONTAP tools for VMware vSphere 9.xx alla versione 10.5"

# Codici di errore di aggiornamento di ONTAP tools

Potresti incontrare codici di errore durante l'operazione di aggiornamento degli ONTAP tools for VMware vSphere. I codici di errore sono composti da cinque cifre, dove le prime due cifre rappresentano lo script che ha riscontrato il problema e le ultime tre cifre rappresentano il flusso di lavoro specifico all'interno di quello script.

Tutti i log degli errori vengono registrati nel file di log ansible-perl-errors.log per facilitare l'individuazione e la risoluzione dei problemi. Questo file di log contiene il codice di errore e l'attività Ansible non riuscita.

I codici di errore riportati in questa pagina sono solo a scopo di riferimento. Contatta il team di supporto se l'errore persiste o se non viene indicata alcuna soluzione.

La tabella seguente elenca i codici di errore e i corrispondenti nomi dei file.

| Codice di errore | Nome script |
|---|---|
| 00 | firstboot-network-config.pl, modalità deploy |
| 01 | firstboot-network-config.pl, modalità upgrade |
| 02 | firstboot-inputs-validation.pl |
| 03 | firstboot-deploy-otv-ng.pl, deploy, HA |
| 04 | firstboot-deploy-otv-ng.pl, deploy, non-HA |
| 05 | firstboot-deploy-otv-ng.pl, reboot |
| 06 | firstboot-deploy-otv-ng.pl, aggiornamento, HA |
| 07 | firstboot-deploy-otv-ng.pl, aggiornamento, non-HA |
| 08 | firstboot-otv-recovery.pl |
| 09 | post-deploy-upgrade.pl |

Le ultime tre cifre del codice di errore indicano lo specifico errore del flusso di lavoro all'interno dello script:

| Codice errore aggiornamento | Flusso di lavoro | Risoluzione |
|---|---|---|
| 052 | L'immagine ISO potrebbe corrispondere alla versione corrente oppure essere fino a due versioni successive. | Utilizza una versione ISO compatibile per eseguire l'aggiornamento dalla versione corrente. |

| Codice errore aggiornamento | Flusso di lavoro | Risoluzione |
| --- | --- | --- |
| 068 | Il rollback dei pacchetti Debian non è riuscito | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 069 | Ripristino dei file non riuscito | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 070 | Impossibile eliminare il backup | - |
| 071 | Il cluster Kubernetes non era in buono stato | - |
| 074 | Montaggio ISO non riuscito | Controlla il file /var/log/upgrade-run.log e riprova l'upgrade. |
| 075 | I controlli preliminari dell'upgrade non sono riusciti | Riprova l'aggiornamento. |
| 076 | Aggiornamento del registro non riuscito | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 077 | Il ripristino del registro non è riuscito | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 078 | L'aggiornamento dell'operatore non è riuscito | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 079 | Il rollback dell'operatore non è riuscito | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 080 | L'aggiornamento dei servizi non è riuscito | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 081 | Il rollback dei servizi non è riuscito | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 082 | Eliminazione delle vecchie immagini dal container non riuscita | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 083 | Eliminazione del backup non riuscita | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |

| Codice errore aggiornamento | Flusso di lavoro | Risoluzione |
|---|---|---|
| 084 | Modificare JobManager di nuovo in Produzione non è riuscito | Esegui i seguenti passaggi per ripristinare/completare l'aggiornamento. 1. Abilita la Diagnostic Shell 2. Esegui il comando: *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Controllare i log in /var/log/post-deploy-upgrade.log |
| 087 | Le fasi successive all'aggiornamento non sono riuscite. | Esegui i seguenti passaggi per ripristinare/completare l'aggiornamento. 1. Abilita la Diagnostic Shell 2. Esegui il comando *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Controllare i log in /var/log/post-deploy-upgrade.log |
| 088 | Configurare la rotazione dei log per journald non è riuscito | Verifica che le impostazioni di rete della macchina virtuale siano compatibili con l'host su cui è ospitata. Puoi provare a migrare la macchina virtuale su un altro host e riavviarla. |
| 089 | Modificare la proprietà del file di configurazione della rotazione del registro di riepilogo non è riuscito | Riprova l'aggiornamento. |
| 095 | Aggiornamento del sistema operativo non riuscito | Nessun ripristino per l'aggiornamento del sistema operativo. I servizi di ONTAP tools vengono aggiornati e nuovi pod saranno in esecuzione. |
| 096 | Installa il provisioner di archiviazione dinamica | Controlla i log di aggiornamento e riprova l'upgrade. |
| 097 | La disinstallazione dei servizi per l'aggiornamento non è riuscita | Usa il ripristino basato su RPO zero o su snapshot e riprova l'upgrade. |
| 098 | Copiare il secret dockercred da ntv-system allo spazio dei nomi del dynamic storage provisioner non è riuscito | Controlla i log di aggiornamento e riprova l'upgrade. |
| 099 | Impossibile convalidare la nuova aggiunta dell'HDD | Aggiungi il nuovo HDD a tutti i nodi in caso di HA e a un solo nodo in caso di deployment non HA. |
| 109 | Il backup dei dati del volume persistente non è riuscito | Controlla i log di aggiornamento e riprova l'upgrade. |

| Codice errore aggiornamento | Flusso di lavoro | Risoluzione |
| --- | --- | --- |
| 110 | Il ripristino dei dati del volume persistente non è riuscito | Usa il ripristino zero-RPO o basato su snapshot e riprova l'aggiornamento. |
| 111 | Aggiornare i parametri di timeout di etcd per RKE2 non è riuscito | Controlla i log di aggiornamento e riprova l'upgrade. |
| 112 | La disinstallazione del dynamic storage provisioner non è riuscita. | - |
| 113 | Aggiornare le risorse sui nodi secondari non è riuscito | Controlla i log di aggiornamento e riprova l'upgrade. |
| 104 | Il riavvio del nodo secondario non è riuscito | Riavviare manualmente i nodi, uno alla volta. |
| 100 | Il rollback del kernel non è riuscito | - |
| 051 | L'aggiornamento del dynamic storage provisioner non è riuscito | Controlla i log di aggiornamento e riprova l'aggiornamento. |
| 056 | Eliminazione del backup di migrazione non riuscita | NA |
| 090 | convalida del certificato per i backend di archiviazione e vCenter non riuscita | Controlla i log di aggiornamento e il file di log in /var/log/cert_validation_error.log e riprova l'upgrade. |

| Codice errore aggiornamento | Flusso di lavoro | Risoluzione |
| --- | --- | --- |
| 114 | Aggiornamento interno del certificato nella collezione MongoDB non riuscito | Se l'upgrade non riesce e viene visualizzato il codice di errore 114, eseguire i seguenti passaggi:<br>1. Connettiti all'immagine ISO di aggiornamento sul nodo primario e abilita la shell diagnostica.<br>2. Monta l'immagine ISO dalla sessione SSH sul nodo primario:<br>`sudo mount /dev/cdrom`<br>`sudo mount -o loop,ro /dev/cdrom/APPLIANCE_UPGRADE.bin /upgrade`<br>3. Installa i pacchetti Debian:<br>`sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vplatform.deb`<br>`sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vpupgrader.deb`<br>`sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vmware-tools.deb`<br>4. Copia il file delle informazioni di build:<br>`sudo cp /upgrade/APPLIANCE_BUILD /`<br>Aggiungi i certificati alla raccolta abilitando la shell diagnostica ed eseguendo: |

A partire da ONTAP tools for VMware vSphere 10.3, zero RPO non è supportato.

Scopri di più su "Come ripristinare ONTAP tools for VMware vSphere se l'aggiornamento dalla versione 10.0 alla 10.1 non riesce"

5.

```
sudo perl
/home/maint/scripts
/post-deploy-
upgrade.pl
--internal_cert_upd
ate_collection
```

Controlla i registri su `/var/log/otvng/post-deploy-upgrade.log`.

6. Riavvia i nodi:

```
sudo bash
/home/maint/scripts
/vault_decrypt.sh
cd
/home/maint/rke2-pb
sudo ansible-
playbook site.yaml
--tags
restart_nodes
--skip-tags
debian_upgrade,kern
el_upgrade,rescan_s
csi_bus,source_iso,
eject_upgrade,mount
Iso,upgradeNodes,re
gistryUpg,deleteOld
Images,wait,checkRe
achability,delete_o
tv_cr,uninstall_tri
dent,del_trident_im
ages,refresh_resour
ces,ntp_configure,n
tpd_uninstall
```

7. Eseguire i passaggi successivi all'aggiornamento:

```
sudo perl
/home/maint/scripts
/post-deploy-
upgrade.pl
--postupgrade
```

# Migra ONTAP tools for VMware vSphere 9.xx a 10.5

## Migra dagli ONTAP tools for VMware vSphere 9.xx alla versione 10.5

Lo spostamento della configurazione di NetApp ONTAP tools for VMware vSphere dalla versione 9.xx alla 10.5 richiede un processo di migrazione a causa dei significativi aggiornamenti e miglioramenti del prodotto tra le versioni.

Puoi migrare da ONTAP tools for VMware vSphere 9.12D1, 9.13D2 e 9.13P2 a ONTAP tools for VMware vSphere 10.5.

Se nella configurazione sono presenti datastore NFS e VMFS e non sono presenti datastore vVols, è sufficiente disinstallare ONTAP tools 9.xx e distribuire ONTAP tools 10.5. Tuttavia, se la configurazione include datastore vVols, è necessario eseguire una procedura di migrazione del VASA Provider e dell'SRA.

La tabella seguente illustra il processo di migrazione in questi due diversi scenari.

| Se la configurazione prevede datastore vVols | Se la configurazione contiene solo datastore NFS e VMFS |
|---|---|
| Passaggi: 1. "Migra il provider VASA" 2. "Crea criteri di archiviazione delle macchine virtuali" | Passaggi: 1. Rimuovi ONTAP tools 9.xx dal tuo ambiente. Fare riferimento a "Come rimuovere OTV 9.xx dal tuo ambiente" NetApp articolo della Knowledge Base. 2. "Distribuisci e configura ONTAP tools for VMware vSphere 10.5" 3. "Aggiorna l'SRA" 4. "Crea criteri di archiviazione delle macchine virtuali" |

Dopo la migrazione da ONTAP tools for VMware vSphere 9.xx a 10.5, i datastore vVols che utilizzano il protocollo NVMe/FC diventano non operativi perché ONTAP tools 10.5 supporta il protocollo NVMe-oF solo con i datastore VMFS.

## Migrare il VASA Provider e aggiornare l'SRA negli ONTAP tools

Segui i passaggi in questa sezione per migrare il VASA Provider da ONTAP tools for VMware vSphere 9.xx a ONTAP tools for VMware vSphere 10.5 e aggiornare lo Storage Replication Adapter (SRA) sull'appliance VMware Live Site Recovery.

### Procedura per migrare il provider VASA

1. Per abilitare la porta Derby 1527 sugli ONTAP tools for VMware vSphere esistenti, abilita l'utente root ed effettua l'accesso alla CLI tramite SSH. Quindi, esegui il seguente comando:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Distribuisci l'OVA per ONTAP tools for VMware vSphere 10.5.
3. Aggiungi l'istanza del server vCenter che vuoi migrare a ONTAP tools for VMware vSphere release 10.5. Consulta "Aggiungi un'istanza di vCenter Server" per maggiori informazioni.
4. "Abilita il provider VASA" servizio su ONTAP tools for VMware vSphere 10.5.
5. Integra localmente il backend di storage dalle API del server vCenter per il plug-in ONTAP tools. Consulta "Aggiungi un backend di storage usando l'interfaccia client vSphere" per maggiori informazioni.
6. Ottieni un token di accesso per autenticare le richieste REST API. Usa il seguente esempio, sostituendo le variabili con i valori specifici del tuo ambiente.

```
curl --request POST \
  --location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/vcenter-
login" \
  --header "Content-Type: application/json" \
  --header "Accept: */*" \
  -d '{"username": "$MYUSER", "password": "$MYPASSWORD", "vcenter
hostname": "$MYVCENTER"}'
```

Copia e salva il token di accesso restituito nella risposta.

7. Esegui la seguente API da Swagger o Postman per eseguire la migrazione.

```
curl -X POST
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migra
tion-jobs`
```

Puoi accedere a Swagger tramite questo URL: `https://$FQDN_IP_PORT/`, per esempio: `https://10.67.25.33:8443/`.

8. Verifica l'avvenuta conclusione controllando i registri:

```
tail -f
/var/log/post-
deploy-upgrade.log
```

```
/dev/cdrom
sudo eject
/dev/cdrom
```

**Metodo ed endpoint HTTP**

Questa chiamata API REST utilizza il seguente metodo e endpoint.

| Metodo HTTP | Percorso |
|---|---|
| POST | /api/v1 |

**Tipo di elaborazione**

Asincrono

**Esempio di Curl**

```
curl -X POST 'https://<OTV-NG-
IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
  --header 'x-auth: <auth_token>' \
  --header 'Content-Type: application/json' \
  --data '{
    "otv_ip": "xx.xx.xx.xx",
    "vasa_provider_credentials": {
      "username": "xxxxx",
      "password": "******"
    },
    "database_password": "******"
  }'
```

Corpo della richiesta per la migrazione di altre release:

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*******"
  }
}
```

**Esempio di output JSON**

Il sistema restituisce un oggetto job. Salva l'identificativo del job per utilizzarlo nel passaggio successivo.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

8. Utilizza il seguente URI in Swagger per verificare lo stato:

```
curl
`\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobId
>?includeSubJobsAndTasks=true`
```

   Utilizzare il valore 'id' restituito dal job di migrazione nel passaggio precedente. Al termine del job, rivedere il report di migrazione nella risposta al job.

9. Registra il VASA Provider con ONTAP tools for VMware vSphere. Per le istruzioni, consulta "Registra il fornitore VASA".
10. Verificare la registrazione del VASA Provider:
    a. Nel vSphere Client, vai al vCenter Server.
    b. Seleziona **Configura** > **Storage Providers**.
    c. Confermare che il VASA Provider registrato nel passaggio precedente risulti online.
11. Arresta ONTAP tools for VMware vSphere storage provider 9.10/9.11/9.12/9.13 VASA Provider service usando questi passaggi:
    a. In ONTAP tools 9.x, apri la console web.
    b. Accedi alla console di manutenzione.
    c. Premi Invio `1` per selezionare il menu **Configurazione applicazione**.
    d. Premi `5` per interrompere i servizi VASA Provider e SRA.
    e. Nel vSphere Client, vai al vCenter Server e seleziona **Configura** > **Provider di archiviazione**.
    f. Selezionare il VASA Provider offline per ONTAP tools 9.x e selezionare **Rimuovi**.

       Dopo l'arresto del vecchio VASA Provider, il vCenter Server esegue il failover su ONTAP tools for VMware vSphere. Tutti i datastore e le VM diventano accessibili e sono serviti da ONTAP tools for VMware vSphere.

12. I datastore NFS e VMFS migrati vengono visualizzati in ONTAP tools for VMware vSphere 10.5 dopo il processo di rilevamento dei datastore, che può richiedere fino a 30 minuti. Verifica la loro visibilità nella pagina di panoramica.
13. Esegui la migrazione della patch usando la seguente API in Swagger o in Postman:

**Metodo ed endpoint HTTP**

Questa chiamata API REST utilizza il seguente metodo e endpoint.

| Metodo HTTP | Percorso |
|---|---|
| PATCH | /api/v1 |

**Tipo di elaborazione**

Asincrono

Usa il seguente URI in Swagger:

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_i
d>/migration-jobs/<migration_id>`
```

**Metodo ed endpoint HTTP**

Questa chiamata API REST utilizza il seguente metodo e endpoint.

| Metodo HTTP | Percorso |
|---|---|
| PATCH | /api/v1 |

**Tipo di elaborazione**

Asincrono

Usa il seguente URI in Swagger:

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_i
d>/migration-jobs/<migration_id>`
```

**Esempio di Curl**

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-
4163-44f9-a872-9adabb008ca9/migration-jobs/d50073ce-35b4-4c51-9d2e-
4ce66f802c35`
```

**Esempio di output JSON**

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

Utilizzare il valore 'migration_id' restituito nel passaggio 7 come <migration_id> nella chiamata API PATCH. Il corpo della richiesta è vuoto per l'operazione di patch.

UUID è l'UUID della migrazione restituito in risposta all'API post-migrate.

Dopo aver eseguito l'API di migrazione delle patch, tutte le VM sono conformi alla storage policy.

**Cosa c'è dopo**

Dopo aver completato la migrazione e registrato ONTAP tools 10.5 sul vCenter Server, segui questi passaggi:

- Attendi il completamento della fase di **Rilevamento** e il sistema aggiorna automaticamente i certificati su tutti gli host.
- Attendi prima di avviare le operazioni su datastore e macchine virtuali. Il tempo di attesa dipende dal numero di host, datastore e macchine virtuali. Se non attendi, potresti vedere errori occasionali.

Dopo l'aggiornamento, se lo stato di conformità della macchina virtuale non è aggiornato, riapplica il criterio di storage seguendo questi passaggi:

1. Vai al datastore e seleziona **Riepilogo** > **Criteri di archiviazione VM**.
2. Il sistema mostra lo stato di conformità sotto **VM storage policy compliance** come **Out-of-date**.
3. Seleziona il criterio Storage VM e la VM corrispondente.
4. Seleziona **Applica**.
5. Lo stato di conformità in **Conformità ai criteri di storage delle VM** risulta conforme.

**Informazioni correlate**

- "Scopri gli strumenti ONTAP per VMware vSphere 10 RBAC"
- "Aggiorna da ONTAP tools for VMware vSphere 10.x a 10.5"

## Procedura per aggiornare l'adattatore di replica dello storage (SRA)

**Prima di iniziare**

Nel piano di recovery, il sito protetto si riferisce alla posizione in cui le VM sono attualmente in esecuzione, mentre il sito di recovery è la posizione in cui le VM verranno recuperate. L'interfaccia dell'appliance VMware Live Site Recovery visualizza lo stato del piano di recovery con dettagli sui siti protetto e di recovery. Nel piano di recovery, i pulsanti CLEANUP e REPROTECT sono disabilitati, mentre i pulsanti TEST e RUN restano abilitati. Questo indica che il sito è pronto per recovery di dati. Prima di migrare l'SRA, verifica che un sito sia nello stato protetto e l'altro nello stato di recovery.

Non avviare la migrazione se il failover è stato completato ma la riprotezione è in sospeso. Assicurarsi che il processo di riprotezione sia completato prima di procedere con la migrazione. Se è in corso un failover di prova, terminarlo e avviare la migrazione.

1. Segui questi passaggi per eliminare l'adattatore ONTAP tools SRA per VMware vSphere 9.xx in VMware Site Recovery:
2. Accedere alla pagina di gestione della configurazione di VMware Live Site Recovery.
   a. Vai alla sezione **Storage Replication Adapter**.
   b. Dal menu con i tre puntini seleziona **Ripristina configurazione**.
   c. Dal menu con i puntini di sospensione seleziona **Cancella**.
3. Esegui questi passaggi sia sul sito di protezione che su quello di recovery.
   a. "Abilita i servizi di ONTAP tools per VMware vSphere"
   b. Configura ONTAP tools for VMware vSphere 10.5 SRA adapter seguendo i passaggi in "Configura SRA sull'appliance VMware Live Site Recovery".
   c. Nell'interfaccia di VMware Live Site Recovery, esegui **Rileva array** e **Rileva dispositivi**. Conferma che i dispositivi vengano visualizzati come prima della migrazione.

# Automatizza utilizzando l'API REST

## Scopri di più sull'API REST di ONTAP tools

ONTAP tools for VMware vSphere 10 è un set di strumenti per la gestione del ciclo di vita delle macchine virtuali. Include una solida API REST che puoi usare come parte dei tuoi processi di automazione.

### Fondamenti dei servizi web REST

Representational State Transfer (REST) è uno stile per la creazione di applicazioni web distribuite, inclusa la progettazione di API di servizi web. Stabilisce un insieme di tecnologie per esporre risorse basate su server e gestirne gli stati.

#### Risorse e rappresentazione dello stato

Le risorse sono i componenti fondamentali di un'applicazione di servizi web REST. Ci sono due compiti iniziali importanti quando progetti un'API REST:

- Identifica le risorse di sistema o basate su server
- Definisci gli stati delle risorse e le relative operazioni di transizione di stato

Le applicazioni client possono visualizzare e modificare lo stato delle risorse tramite flussi di messaggi ben definiti.

#### messaggi HTTP

L'Hypertext Transfer Protocol (HTTP) è il protocollo utilizzato dal client e dal server dei servizi web per scambiarsi messaggi relativi alle risorse. Segue il modello CRUD basato sulle operazioni generiche di creazione, lettura, aggiornamento ed eliminazione. Il protocollo HTTP include intestazioni di richiesta e risposta, nonché codici di stato della risposta.

#### Formattazione dei dati JSON

Sebbene siano disponibili diversi formati di messaggio, l'opzione più diffusa è JavaScript Object Notation (JSON). JSON è uno standard di settore per la rappresentazione di semplici strutture dati in testo semplice e viene utilizzato per trasferire informazioni sullo stato che descrivono le risorse e le azioni desiderate.

#### Sicurezza

La sicurezza è un aspetto importante di un'API REST. Oltre al protocollo Transport Layer Security (TLS) utilizzato per proteggere il traffico HTTP sulla rete, gli ONTAP tools for VMware vSphere 10 REST API utilizzano anche i token di accesso per l'autenticazione. Devi ottenere un token di accesso e usarlo nelle chiamate API successive.

#### Supporto per richieste asincrone

Gli ONTAP tools for VMware vSphere 10 REST API eseguono la maggior parte delle richieste in modo sincrono, restituendo un codice di stato quando l'operazione è completata. Supportano anche l'elaborazione asincrona per le attività che richiedono più tempo per essere completate.

### Ambiente di gestione di ONTAP tools

Ci sono diversi aspetti dell'ambiente ONTAP tools Manager che dovresti considerare.

#### Macchina virtuale

ONTAP tools for VMware vSphere 10 viene distribuito utilizzando l'architettura plug-in remota di vSphere. Il software, incluso il supporto per la REST API, viene eseguito in una macchina virtuale separata.

**Indirizzo IP degli strumenti ONTAP**

ONTAP tools for VMware vSphere 10 espone un singolo indirizzo IP che funge da gateway per le funzionalità della macchina virtuale. Devi fornire l'indirizzo durante la configurazione iniziale e viene assegnato a un componente interno del bilanciatore di carico. L'indirizzo viene utilizzato sia dall'interfaccia utente di ONTAP tools Manager sia per accedere direttamente alla pagina della documentazione Swagger e alla REST API.

**Due API REST**

Oltre all'API REST di ONTAP tools per VMware vSphere 10, il cluster ONTAP ha una propria API REST. ONTAP tools Manager utilizza l'API REST di ONTAP come client per eseguire attività relative allo storage. È importante tenere presente che queste due API sono separate e distinte. Per ulteriori informazioni, consulta "Automazione ONTAP".

# Dettagli di implementazione delle API REST di ONTAP tools

Sebbene REST definisca un insieme comune di tecnologie e best practice, l'implementazione esatta di ciascuna API può variare in base alle scelte di progettazione. Dovresti conoscere come è progettata l'API REST di ONTAP tools for VMware vSphere 10 prima di utilizzarla.

L'API REST include diverse categorie di risorse, come vCenters e Aggregati. Consulta la "Riferimento API" per maggiori informazioni.

## Come accedere all'API REST

Puoi accedere agli ONTAP tools for VMware vSphere 10 REST API tramite l'indirizzo IP degli ONTAP tools insieme alla porta. Ci sono diverse parti che compongono l'URL completo, tra cui:

- Indirizzo IP e porta di ONTAP tools
- Versione API
- Categoria di risorse
- Risorsa specifica

Devi configurare l'indirizzo IP durante la configurazione iniziale, mentre la porta rimane fissa a 8443. La prima parte dell'URL è la stessa per ogni istanza di ONTAP tools for VMware vSphere 10; solo la categoria di risorsa e la risorsa specifica cambiano tra gli endpoint.

Gli indirizzi IP e i valori delle porte negli esempi seguenti sono solo a scopo illustrativo. Devi modificare questi valori per il tuo ambiente.

**Esempio di accesso ai servizi di autenticazione**

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Questo URL può essere utilizzato per richiedere un token di accesso utilizzando il metodo POST.

**Esempio per elencare i server vCenter**

```
https://10.61.25.34:8443/virtualization/api/v1/vcenters
```

Questo URL può essere utilizzato per richiedere un elenco delle istanze del server vCenter definite tramite il metodo GET.

## Dettagli HTTP

Gli ONTAP tools for VMware vSphere 10 REST API utilizzano HTTP e i relativi parametri per agire sulle istanze e sulle raccolte di risorse. I dettagli dell'implementazione HTTP sono presentati di seguito.

### Metodi HTTP

I metodi o verbi HTTP supportati dall'API REST sono presentati nella tabella seguente.

| Metodo | CRUD | Descrizione |
|---|---|---|
| GET | Leggi | Recupera le proprietà di un oggetto per un'istanza di risorsa o una raccolta. Questa è considerata un'operazione di elenco quando viene utilizzata con una raccolta. |
| POST | Crea | Crea una nuova istanza della risorsa in base ai parametri di input. |
| PUT | Aggiorna | Aggiorna un'intera istanza di risorsa con il corpo della richiesta JSON fornito. I valori chiave che non possono essere modificati dall'utente vengono mantenuti. |
| PATCH | Aggiorna | Richiedi che una serie di modifiche selezionate nella richiesta siano applicate all'istanza della risorsa. |
| ELIMINA | Elimina | Elimina un'istanza di risorsa esistente. |

### Intestazioni di richiesta e risposta

La tabella seguente riassume le intestazioni HTTP più importanti utilizzate con l'API REST.

| Intestazione | Tipo | Note sull'utilizzo |
|---|---|---|
| Accetta | Richiesta | Questo è il tipo di contenuto che l'applicazione client può accettare. I valori validi includono '*/*` o `application/json`. |
| x-auth | Richiesta | Contiene un token di accesso che identifica l'utente che effettua la richiesta tramite l'applicazione client. |
| Tipo di contenuto | Risposta | Restituito dal server in base all'intestazione della richiesta `Accept`. |

### codici di stato HTTP

Di seguito sono descritti i codici di stato HTTP utilizzati dall'API REST.

| Codice | Significato | Descrizione |
|---|---|---|
| 200 | OK | Indica il successo delle chiamate che non creano una nuova istanza di risorsa. |
| 201 | Creato | È stato creato correttamente un oggetto con un identificatore univoco per l'istanza della risorsa. |

| Codice | Significato | Descrizione |
|---|---|---|
| 202 | Accettato | La richiesta è stata accettata ed è stato creato un processo in background per eseguire la richiesta. |
| 204 | Nessun contenuto | La richiesta è andata a buon fine anche se non è stato restituito alcun contenuto. |
| 400 | Richiesta non valida | L'input della richiesta non è riconosciuto o non è appropriato. |
| 401 | Non autorizzato | L'utente non è autorizzato e deve autenticarsi. |
| 403 | Vietato | L'accesso è negato a causa di un errore di autorizzazione. |
| 404 | Non trovato | La risorsa a cui si fa riferimento nella richiesta non esiste. |
| 409 | Conflitto | Il tentativo di creare un oggetto non è riuscito perché l'oggetto esiste già. |
| 500 | errore interno | Si è verificato un errore interno generico sul server. |

### Autenticazione

L'autenticazione di un client all'API REST viene eseguita tramite un token di accesso. Le caratteristiche rilevanti del token e del processo di autenticazione includono:

- Il client deve richiedere un token utilizzando le credenziali di amministratore (nome utente e password) di ONTAP tools Manager.
- I token sono formattati come JSON Web Token (JWT).
- Ogni token scade dopo 60 minuti.
- Le richieste API provenienti da un client devono includere il token nell' `x-auth`intestazione della richiesta.

Consulta "La tua prima chiamata API REST" per un esempio di richiesta e utilizzo di un token di accesso.

### Richieste sincrone e asincrone

La maggior parte delle chiamate API REST si completa rapidamente e quindi viene eseguita in modo sincrono. Cioè, restituiscono un codice di stato (come 200) dopo che una richiesta è stata completata. Le richieste che richiedono più tempo per essere completate vengono eseguite in modo asincrono usando un processo in background.

Dopo aver effettuato una chiamata API che viene eseguita in modo asincrono, il server restituisce un codice di stato HTTP 202. Questo indica che la richiesta è stata accettata ma non ancora completata. Puoi interrogare il processo in background per determinarne lo stato, incluso se ha avuto successo o meno.

L'elaborazione asincrona viene utilizzata per diversi tipi di operazioni di lunga durata, incluse le operazioni di datastore e vVol. Per ulteriori informazioni, consulta la categoria job manager dell'API REST nella pagina Swagger.

# Effettua la tua prima chiamata API REST degli ONTAP tools

Puoi effettuare una chiamata API tramite curl per iniziare a utilizzare le ONTAP tools for VMware vSphere 10 REST API.

## Prima di iniziare

Dovresti esaminare le informazioni e i parametri richiesti negli esempi di curl.

**Informazioni richieste**

Ti serviranno i seguenti elementi:

- ONTAP tools for VMware vSphere 10 indirizzo IP o FQDN così come la porta
- Credenziali per l'amministratore di ONTAP tools Manager (nome utente e password)

**Parametri e variabili**

Gli esempi di curl presentati di seguito includono variabili in stile Bash. Puoi impostare queste variabili nell'ambiente Bash o aggiornarle manualmente prima di eseguire i comandi. Se imposti le variabili, la shell sostituirà i valori in ogni comando prima che venga eseguito. Le variabili sono descritte nella tabella seguente.

| Variabile | Descrizione |
|---|---|
| $FQDN_IP_PORT | Il fully qualified domain name o l'indirizzo IP di ONTAP tools Manager insieme al numero di porta. |
| $MYUSER | Nome utente per l'account Manager degli ONTAP tools. |
| $MYPASSWORD | Password associata al nome utente di ONTAP tools Manager. |
| $ACCESS_TOKEN | Il token di accesso rilasciato da ONTAP tools Manager. |

I seguenti comandi e l'output nella riga di comando di Linux illustrano come impostare e visualizzare una variabile:

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

## Passaggio 1: Acquisisci un token di accesso

Per utilizzare l'API REST devi ottenere un token di accesso. Di seguito trovi un esempio di come richiedere un token di accesso. Devi sostituire i valori con quelli appropriati per il tuo ambiente.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login” \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

Copia e salva il token di accesso fornito nella risposta.

## Passaggio 2: Effettua la chiamata REST API

Dopo che hai ottenuto un token di accesso, puoi usare curl per effettuare una chiamata API REST. Includi il token di accesso ottenuto nel primo passaggio.

**Esempio di curl**

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

La risposta JSON include un elenco delle istanze vCenter VMware configurate per ONTAP tools Manager.

# Riferimento API REST di ONTAP tools

La documentazione di riferimento delle API REST di ONTAP tools for VMware vSphere 10 contiene i dettagli relativi a tutte le chiamate API. Questa documentazione è utile quando sviluppi applicazioni di automazione.

Puoi accedere alla documentazione dell'API REST di ONTAP tools for VMware vSphere 10 online tramite l'interfaccia utente Swagger. Ti serve l'indirizzo IP o il fully qualified domain name (FQDN) del servizio gateway di ONTAP tools for VMware vSphere 10, oltre alla porta.

**Passaggi**

1. Digita il seguente URL nel tuo browser, sostituendo l'indirizzo IP e la porta appropriati con la variabile, e premi **Enter**.

   `https://$FQDN_IP_PORT/`

   **Esempio**

   `https://10.61.25.33:8443/`

2. Come esempio di una singola chiamata API, scorri verso il basso fino alla categoria **vCenters** e seleziona **GET** accanto all'endpoint `/virtualization/api/v1/vcenters`

# Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi, brevetti e altro.

## Copyright

"https://www.netapp.com/company/legal/copyright/"

## Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi di NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

"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

## Informativa sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

## Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp.

"Avviso per ONTAP tools for VMware vSphere 10.5"

## Informazioni sul copyright

Copyright © 2026 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.