



Tool ONTAP per la documentazione di VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
March 09, 2026

Sommario

Tool ONTAP per la documentazione di VMware vSphere	1
Note di rilascio	2
Note di rilascio per ONTAP tools	2
Novità negli ONTAP tools for VMware vSphere 10.5	2
Piattaforme ONTAP supportate e versioni di vCenter Server	3
Confronto delle funzionalità 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 basato sui ruoli (RBAC)	8
Scopri RBAC degli strumenti ONTAP	8
RBAC con VMware vSphere	10
RBAC con ONTAP	17
Implementa i tool ONTAP per VMware vSphere	21
Avvio rapido dei tool ONTAP per VMware vSphere	21
Flusso di lavoro di distribuzione ad alta disponibilità per ONTAP tools	23
Strumenti ONTAP per requisiti e limiti di configurazione VMware vSphere	23
Requisiti di sistema	23
Requisiti minimi di archiviazione e applicazione	24
Requisiti delle porte	24
Limiti di configurazione per distribuire ONTAP tools for VMware vSphere per vVols datastores	27
Limiti di configurazione per distribuire ONTAP tools for VMware vSphere per datastore VMFS e NFS	28
Tool ONTAP per VMware vSphere - Storage Replication Adapter (SRA)	28
Requisiti di pre-distribuzione per ONTAP tools	29
Foglio di lavoro distribuzione	29
Configurazione del firewall di rete	31
Impostazioni di archiviazione di ONTAP	31
Distribuisci ONTAP tools	31
Risolvi gli errori di distribuzione degli ONTAP tools	36
Raccogliere i file di log	36
Codici di errore di distribuzione	37
Configurare i tool ONTAP per VMware vSphere	40
Aggiungere istanze di vCenter Server agli strumenti ONTAP	40
Registrare il provider VASA con un'istanza del server vCenter negli ONTAP tools	41
Installare il plug-in NFS VAAI utilizzando gli strumenti ONTAP	42
Configurare le impostazioni dell'host ESXi negli ONTAP tools	43
Configurare le impostazioni di multipath e timeout del server ESXi	43
Impostare i valori dell'host ESXi	43
Configurare i ruoli e i privilegi utente ONTAP per ONTAP tools	44
Requisiti di mappatura degli aggregati delle SVM	45
Creare manualmente un utente e un ruolo ONTAP	46
Aggiorna i tool ONTAP per VMware vSphere 10,1 a un utente 10,3	54
Aggiorna i tool ONTAP per VMware vSphere 10,3 a un utente 10,4	56

Aggiungi un backend di storage a ONTAP tools	56
Associare un backend di storage a un'istanza del vCenter Server negli ONTAP tools	59
Configurare l'accesso alla rete negli ONTAP tools	59
Creare un datastore in ONTAP tools	60
Protezione di datastore e macchine virtuali	65
Proteggere un cluster host negli ONTAP tools	65
Proteggere utilizzando la protezione SRA	66
Configurare SRA negli ONTAP tools per proteggere i datastore	66
Configurare SRA in ONTAP tools for VMware vSphere per ambienti SAN e NAS	67
Configurare SRA in ONTAP tools per ambienti altamente scalabili	68
Configurare SRA sull'appliance VMware Live Site Recovery utilizzando ONTAP tools	69
Aggiorna le credenziali SRA negli strumenti ONTAP	70
Configura i siti protetti e di ripristino negli ONTAP tools	70
Configurare le risorse protette e del sito di ripristino	72
Verificare i sistemi di archiviazione replicati negli ONTAP tools	75
Protezione fan-out negli ONTAP tools	76
Gestisci i tool ONTAP per VMware vSphere	79
Scopri la dashboard degli strumenti ONTAP	79
Come ONTAP tools gestisce gli igroup e le policy di esportazione	80
Policy di esportazione	84
Come ONTAP tools gestisce gli igroup	85
Scopri l'interfaccia utente di ONTAP tools Manager	88
Gestisci le impostazioni del gestore degli strumenti ONTAP	90
Modifica le impostazioni di AutoSupport degli strumenti ONTAP	90
Aggiungi server NTP agli strumenti ONTAP	91
Reimposta le credenziali del provider VASA e SRA negli strumenti ONTAP	91
Modifica le impostazioni di backup di ONTAP tools	92
Abilita i servizi di ONTAP tools	92
Modificare le impostazioni dell'appliance ONTAP tools	93
Aggiungere host VMware vSphere a ONTAP tools	94
Gestire i datastore	94
Montare i datastore NFS e VMFS negli ONTAP tools	94
Smonta i datastore NFS e VMFS negli ONTAP tools	95
Montare un datastore vVols negli ONTAP tools	96
Ridimensiona i datastore NFS e VMFS negli ONTAP tools	96
Espandi gli datastore vVols negli ONTAP tools	97
Ridurre un datastore vVols negli ONTAP tools	97
Elimina i datastore in ONTAP tools	98
Visualizzazioni dello storage ONTAP per i datastore negli ONTAP tools	99
Visualizzazione dell'archiviazione della macchina virtuale in ONTAP tools	99
Gestire le soglie di archiviazione negli ONTAP tools	99
Gestire i backend di storage in ONTAP tools	100
Rileva lo storage	100
Modificare i backend di archiviazione	100
Rimuovere i backend di stoccaggio	101

Drill-down del backend dello storage	101
Gestire le istanze di vCenter Server negli strumenti ONTAP	102
Dissociare i backend di storage con l'istanza di vCenter Server	102
Modificare un'istanza di vCenter Server	102
Rimuovere un'istanza di vCenter Server	103
Rinnova il certificato di vCenter Server	103
Gestisci i certificati degli strumenti ONTAP	105
Accedi ai tool ONTAP per la console di manutenzione di VMware vSphere	107
Scopri la console di manutenzione di ONTAP tools	107
Configurare l'accesso diagnostico remoto per ONTAP tools	108
Avvia SSH sugli altri nodi di ONTAP tools	109
Aggiorna le credenziali del server vCenter negli ONTAP tools	109
Modificare il flag di convalida del certificato negli ONTAP tools	109
Report sui tool ONTAP	110
Gestire le macchine virtuali	111
Considerazioni sulla migrazione e la clonazione di macchine virtuali per ONTAP tools	111
Migrare le macchine virtuali negli archivi dati vVols in ONTAP tools	112
Pulisci le configurazioni VASA negli ONTAP tools	112
Collegare o scollegare un disco dati da una VM in ONTAP tools	112
Scopri i sistemi di archiviazione e gli host negli ONTAP tools	113
Modificare le impostazioni degli host ESXi utilizzando gli strumenti ONTAP	114
Gestire le password	115
Modificare la password del gestore strumenti ONTAP	115
Reimpostare la password di gestione degli strumenti ONTAP	115
Reimposta la password utente dell'applicazione in ONTAP tools	116
Reimposta la password della console di manutenzione di ONTAP tools	116
Gestire la protezione dei cluster di host	117
Modificare un cluster host protetto in ONTAP tools	117
Rimuovere la protezione del cluster host negli ONTAP tools	120
Ripristina la configurazione degli strumenti ONTAP	121
Disinstallare ONTAP tools	122
Rimuovere i volumi FlexVol dopo aver disinstallato ONTAP tools	122
Aggiorna i tool ONTAP per VMware vSphere	124
Aggiornamento dagli ONTAP tools for VMware vSphere 10.x alla versione 10.5	124
Codici di errore di aggiornamento di ONTAP tools	126
Migrare gli ONTAP tools for VMware vSphere 9.xx a 10.5	130
Migrazione dagli ONTAP tools for VMware vSphere 9.xx a 10.5	130
Migrare il VASA Provider e aggiornare l'SRA negli ONTAP tools	130
Passaggi per migrare il provider VASA	130
Passaggi per aggiornare l'adattatore di replicazione dello storage (SRA)	135
Automatizza utilizzando l'API REST	137
Scopri di più sull'API REST di ONTAP tools	137
Base REST per i web Services	137
Ambiente di gestione degli strumenti ONTAP	137
Dettagli di implementazione delle API REST di ONTAP tools	138

Come accedere all'API REST	138
Dettagli HTTP	139
Autenticazione	140
Richieste sincrone e asincrone	140
Effettua la tua prima chiamata API REST degli ONTAP tools	140
Prima di iniziare	141
Fase 1: Acquisire un token di accesso	141
Passaggio 2: Eseguire la chiamata API REST	141
Riferimento API REST di ONTAP tools	142
Note legali	143
Copyright	143
Marchi	143
Brevetti	143
Direttiva sulla privacy	143
Open source	143

Tool ONTAP per la documentazione di VMware vSphere

Note di rilascio

Note di rilascio per ONTAP tools

Scopri le nuove e migliorate funzionalità disponibili negli ONTAP tools for VMware vSphere 10.5.

Per un elenco completo delle nuove funzionalità e dei miglioramenti, fare riferimento [Novità negli ONTAP tools for VMware vSphere 10.5](#).

Per le informazioni più aggiornate sulla compatibilità, fare riferimento "[Tool di matrice di interoperabilità NetApp](#)".

È supportata la migrazione dagli ONTAP tools for VMware vSphere 9.12D1, 9.13D2 e 9.13P2 agli ONTAP tools for VMware vSphere 10.5.

Per maggiori informazioni, fare riferimento al "[Note sulla versione ONTAP tools for VMware vSphere 10.5](#)". Per accedere alle Note sulla versione è necessario effettuare l'accesso con il proprio account NetApp o creare un account.

Novità negli ONTAP tools for VMware vSphere 10.5

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

- **Qualifica della piattaforma**

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

- **Qualificazioni e certificazioni VMware**

Gli ONTAP tools for VMware vSphere 10.5 sono conformi agli attuali standard di certificazione di interoperabilità VMware, supportando sia l'host ESXi che vCenter Server.

- * Supporto MetroCluster *

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

- **Gestione della sicurezza e dei certificati**

Questa versione introduce una gestione semplificata dei certificati autofirmati, migliorando sia l'esperienza utente sia l'aderenza agli standard di sicurezza. Fornisce flussi di lavoro di convalida dei certificati migliorati per proteggere ONTAP e gli ONTAP tools for VMware vSphere.

- **Miglioramenti della replicazione**

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

• Aggiornamento e migrazione

Il processo di aggiornamento e migrazione dalle versioni precedenti degli ONTAP tools for VMware vSphere agli ONTAP tools for VMware vSphere 10.5 è progettato per essere fluido ed efficiente, riducendo al minimo i tempi di inattività e garantendo una transizione fluida.

Piattaforme ONTAP supportate e versioni di vCenter Server

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, fare riferimento a ["Tool di matrice di interoperabilità NetApp"](#).

Confronto delle funzionalità ONTAP tools for VMware vSphere 9 e 10

Scopri se la migrazione dagli ONTAP tools for VMware vSphere 9 agli ONTAP tools for VMware vSphere 10.2 o versioni successive è adatta alle tue esigenze.



Per le informazioni più aggiornate sulla compatibilità, fare riferimento ["Tool di matrice di interoperabilità NetApp"](#).

Caratteristica	Strumenti ONTAP 9.13	Strumenti ONTAP 10.2 e successivi
Proposta di valore chiave	Semplifica e ottimizza 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 cluster di storage metro vSphere e supporto VMware Live Site Recovery a tre siti
Qualifica di rilascio 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 si utilizzano sistemi ASA r2. ONTAP 9.15.1, 9.16.1 e 9.17.0 per ONTAP tools 10.5

Caratteristica	Strumenti ONTAP 9.13	Strumenti ONTAP 10.2 e successivi
Supporto per le versioni 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 siti condivisi, consentendo una scalabilità migliorata e prestazioni migliorate.
Supporto del protocollo	Datastore NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI e FCP)	Datastore NFS e VMFS: NFS (v3 e v4.1), VMFS (iSCSI/FCP/NVMe-oF)
Scalabilità	Host e VM: 300 host, fino a 10.000 VM Datastore: 600 NFS, fino a 50 VMFS	Host e VM: 600 host
Osservabilità	Dashboard di prestazioni, capacità e conformità dell'host Report dinamici su VM e datastore	Dashboard aggiornate su 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 il backup.	Replica SRA per datastore iSCSI VMFS e NFS v3, protezione a tre siti che combina SMAS e VMware Live Site Recovery. Supporto SRA per FCP con VMFS.
Supporto del fornitore VASA	VASA 4.0	VASA 3.0

Concetti

Scopri gli strumenti ONTAP

ONTAP tools for VMware vSphere è un set di strumenti per la gestione del ciclo di vita delle macchine virtuali. Si integra con l'ecosistema VMware per semplificare il provisioning del datastore e fornire una protezione di base per le macchine virtuali. Si tratta di una raccolta di microservizi scalabili orizzontalmente e basati su eventi, distribuiti come Open Virtual Appliance (OVA).

Gli ONTAP tools for VMware vSphere supportano:

- Funzionalità principali della macchina virtuale (VM) come protezione e ripristino di emergenza
- Fornitore VASA per la gestione basata su policy di archiviazione
- Gestione basata su criteri dello storage
- Storage Replication Adapter (SRA)

Alta disponibilità per gli strumenti ONTAP per VMware

Gli ONTAP tools for VMware vSphere offrono supporto ad alta disponibilità (HA) per contribuire a mantenere un funzionamento ininterrotto in caso di guasti.

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

- Errore host: è supportato solo l'errore di un singolo nodo.
- Errore di rete
- Errore della macchina virtuale (sistema operativo guest)
- Errore dell'applicazione (strumenti ONTAP)

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



Gli ONTAP tools for VMware vSphere non supportano vCenter HA.

Per utilizzare la funzionalità HA, assicurarsi che l'aggiunta a caldo della CPU e il collegamento a caldo della memoria siano abilitati durante la distribuzione o in un secondo momento nelle impostazioni della VM.

Concetti e termini chiave negli ONTAP tools

Nella sezione seguente vengono descritti i concetti e i termini principali utilizzati nel documento.

Autorità di certificazione (CA)

CA è un'entità attendibile che emette certificati SSL (Secure Sockets Layer).

Gruppo di coerenza

Un gruppo di coerenza è una raccolta di volumi gestiti come un'unica unità. I gruppi di coerenza vengono sincronizzati per garantire la coerenza dei dati tra unità di archiviazione e volumi. In ONTAP, forniscono una gestione semplice e una garanzia di protezione per un carico di lavoro applicativo che si estende su più volumi. Scopri di più su ["gruppi di coerenza"](#).

Stack doppio

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.

LUN (Logical Unit Number)

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

Namespace e sottosistema NVMe

Uno spazio dei nomi NVMe è una quantità di memoria non volatile che può essere formattata in blocchi logici. Gli spazi dei nomi sono l'equivalente dei LUN per i protocolli FC e iSCSI e un sottosistema NVMe è analogo a un igroup. Un sottosistema NVMe può essere associato agli iniziatori, in modo che gli iniziatori associati possano accedere agli spazi dei nomi all'interno del sottosistema.

Gestione strumenti ONTAP

ONTAP Tools Manager offre un maggiore controllo sui tool ONTAP per gli amministratori di VMware vSphere sulle istanze di vCenter Server gestite e sui backend storage integrati. Aiuta a gestire istanze di vCenter Server, backend di storage, certificati, password e download dei bundle di log.

Open Virtual Appliance (OVA)

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

Obiettivo RPO (Recovery Point Objective)

L'RPO misura la frequenza con cui si esegue il backup o la replica dei dati. Specifica il momento esatto in cui è necessario ripristinare i dati dopo un'interruzione per riprendere le operazioni aziendali. 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.

Sincronizzazione attiva di SnapMirror

La sincronizzazione attiva di SnapMirror consente ai servizi di business di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Non sono necessari interventi manuali o script personalizzati per attivare un failover con la sincronizzazione attiva di SnapMirror. Ulteriori informazioni su ["Sincronizzazione attiva di SnapMirror"](#).

Back-end dello storage

I backend dello storage sono l'infrastruttura storage sottostante che l'host ESXi utilizza per memorizzare file, dati e altre risorse della macchina virtuale. Consentono all'host ESXi di accedere e gestire i dati persistenti, fornendo le performance e le funzionalità dello storage necessarie per un ambiente virtualizzato.

Cluster globale (backend storage)

I backend di storage globale, disponibili solo con le credenziali del cluster ONTAP, sono inseriti nell'interfaccia di ONTAP tools Manager. Possono essere aggiunti con minimal Privileges per consentire il rilevamento delle risorse cluster essenziali necessarie per la gestione dei vVol. I cluster globali sono ideali per gli scenari multi-tenancy, in cui un utente SVM viene aggiunto localmente per la gestione dei vVol.

Backend dello storage locale

I backend di storage locale con credenziali cluster o SVM vengono aggiunti tramite l'interfaccia utente dei tool ONTAP e sono limitati a un vCenter. Quando si utilizzano le credenziali del cluster a livello locale, le SVM associate vengono automaticamente mappate con vCenter per gestire vVol o VMFS. Per la gestione di VMFS, incluso SRA, i tool ONTAP supportano le credenziali SVM senza richiedere un cluster globale.

Storage Replication Adapter (SRA)

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

Storage Virtual Machine (SVM)

SVM è l'unità di multi-tenancy in ONTAP. Come una macchina virtuale in esecuzione su un hypervisor, la SVM è un'entità logica che astrae le risorse fisiche. SVM contiene volumi di dati e una o più LIF attraverso i quali distribuiscono dati ai client.

Configurazione uniforme e non uniforme

- **Uniform host access** significa che gli host da due siti sono connessi a tutti i percorsi ai cluster di storage su entrambi i siti. I percorsi tra siti sono estesi su diverse distanze.
- **Accesso host non uniforme** significa che gli host in ogni sito sono connessi solo al cluster nello stesso sito. I percorsi tra siti e quelli estesi non sono connessi.



È supportato un accesso host uniforme per qualsiasi implementazione SnapMirror Active Sync; l'accesso host non uniforme è supportato solo per le implementazioni Active/Active simmetriche. Ulteriori informazioni su "[Panoramica della sincronizzazione attiva di SnapMirror in ONTAP](#)".

File system della macchina virtuale (VMFS)

VMFS è un file system in cluster progettato per la memorizzazione dei file delle macchine virtuali negli ambienti VMware vSphere.

Volumi virtuali (vVol)

I vVols forniscono un'astrazione a livello di volume per l'archiviazione utilizzata da una macchina virtuale. Offre numerosi vantaggi e rappresenta un'alternativa all'utilizzo di una LUN tradizionale. Un datastore vVol è in genere associato a un singolo LUN che funge da contenitore per i vVols.

Policy per lo storage delle VM

Le policy di storage delle macchine virtuali vengono create in vCenter Server in Policy e profili. Per vVol, creare un set di regole utilizzando le regole del provider di tipi di storage NetApp vVol.

Ripristino sito live di VMware

VMware Live Site Recovery, precedentemente noto come Site Recovery Manager (SRM), fornisce funzionalità di business continuity, disaster recovery, migrazione dei siti e test senza interruzioni per gli ambienti virtuali VMware.

API VMware vSphere per Storage Awareness (VASA)

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

API storage di VMware vSphere: Integrazione degli array (VAAI)

VAAI è un set di API che consente la comunicazione tra gli host di VMware vSphere ESXi e i dispositivi storage. Le API comprendono un set di operazioni primitive utilizzate dagli host per scaricare operazioni di storage sull'array. VAAI può offrire miglioramenti significativi delle performance per i task a uso intensivo di storage.

vSphere Metro Storage Cluster

vSphere Metro Storage Cluster (vMSC) è un'architettura che consente e supporta vSphere in un'implementazione cluster estesa. Le soluzioni vMSC sono supportate con la sincronizzazione attiva di NetApp MetroCluster e SnapMirror (in precedenza SMBC). Queste soluzioni forniscono una migliore business continuity in caso di errore del dominio. Il modello di resilienza si basa sulle tue scelte specifiche di configurazione. Ulteriori informazioni su ["Cluster di storage VMware vSphere Metro"](#).

Datastore vVol

Il datastore vVol è una rappresentazione del datastore logico di un contenitore vVol creato e gestito da un provider VASA.

RPO zero

RPO è l'acronimo di Recovery Point Objective, ovvero la quantità di perdita di dati ritenuta accettabile in un determinato periodo di tempo. Zero RPO indica che non è accettabile alcuna perdita di dati.

Controllo degli accessi basato sui ruoli (RBAC)

Scopri RBAC degli strumenti ONTAP

RBAC (role-based access control) è un framework di sicurezza per controllare l'accesso alle risorse all'interno di un'organizzazione. RBAC semplifica l'amministrazione definendo ruoli con specifici livelli di autorizzazione per eseguire azioni, invece di assegnare autorizzazioni a singoli utenti. I ruoli definiti vengono assegnati agli utenti, riducendo così il rischio di errori e semplificando la gestione del controllo degli accessi all'interno dell'organizzazione.

Il modello standard RBAC è composto da diverse tecnologie di implementazione o fasi di crescente complessità. Il risultato è che le effettive implementazioni RBAC, basate sulle esigenze dei fornitori di software e dei loro clienti, possono differire e variare da relativamente semplice a molto complesso.

Componenti RBAC

Ad un livello elevato, ci sono diversi componenti che sono generalmente inclusi in ogni implementazione RBAC. Questi componenti sono associati in modi diversi come parte della definizione dei processi di autorizzazione.

Privilegi

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

Ruoli

Un *ruolo* è un contenitore che include uno o più Privileges. I ruoli vengono generalmente definiti in base a attività o funzioni lavorative particolari. Quando un ruolo viene assegnato a un utente, all'utente viene concesso tutto il Privileges contenuto nel ruolo. Come per Privileges, le implementazioni includono ruoli predefiniti e in genere consentono la creazione di ruoli personalizzati.

Oggetti

Un *object* rappresenta una risorsa reale o astratta identificata nell'ambiente RBAC. Le azioni definite tramite Privileges vengono eseguite su o con gli oggetti associati. A seconda dell'implementazione, Privileges può essere concesso a un tipo di oggetto o a una specifica istanza di oggetto.

Utenti e gruppi

Users sono assegnati o associati a 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 a *gruppi* può semplificare ulteriormente l'amministrazione della protezione.

Permessi

Un *permesso* è una definizione che associa un utente o un gruppo insieme a un ruolo a un oggetto. Le autorizzazioni possono essere utili con un modello a oggetti gerarchico in cui possono essere eventualmente ereditate dai figli nella gerarchia.

Due ambienti RBAC

Quando si lavora con gli ONTAP tools for VMware vSphere 10, è necessario prendere in considerazione due distinti ambienti RBAC. Per eseguire le operazioni, gli ONTAP tools for VMware vSphere 10 richiedono privilegi specifici sia in vCenter che in ONTAP. Sebbene gli strumenti ONTAP automatizzino le attività di gestione dello storage, non creano account utente né in vCenter né in ONTAP. Gli account di servizio devono essere creati da un amministratore vSphere in base alle necessità. Questa documentazione fornisce agli amministratori una guida per assegnare i ruoli e le autorizzazioni necessari per una gestione efficace degli strumenti ONTAP.

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 dei tool ONTAP per VMware vSphere 10, l'ambiente RBAC viene esteso per includere oggetti aggiuntivi che rappresentano le funzionalità dei tool ONTAP. L'accesso a questi oggetti viene fornito tramite il plug-in remoto. Per ulteriori informazioni,

vedere ["Ambiente RBAC vCenter Server"](#)

Cluster ONTAP

I tool ONTAP per VMware vSphere 10 si collegano a un cluster ONTAP attraverso l'API REST ONTAP per eseguire operazioni relative allo storage. L'accesso alle risorse di storage viene controllato tramite un ruolo ONTAP associato all'utente ONTAP fornito durante l'autenticazione. Per ulteriori informazioni, vedere ["Ambiente RBAC ONTAP"](#).

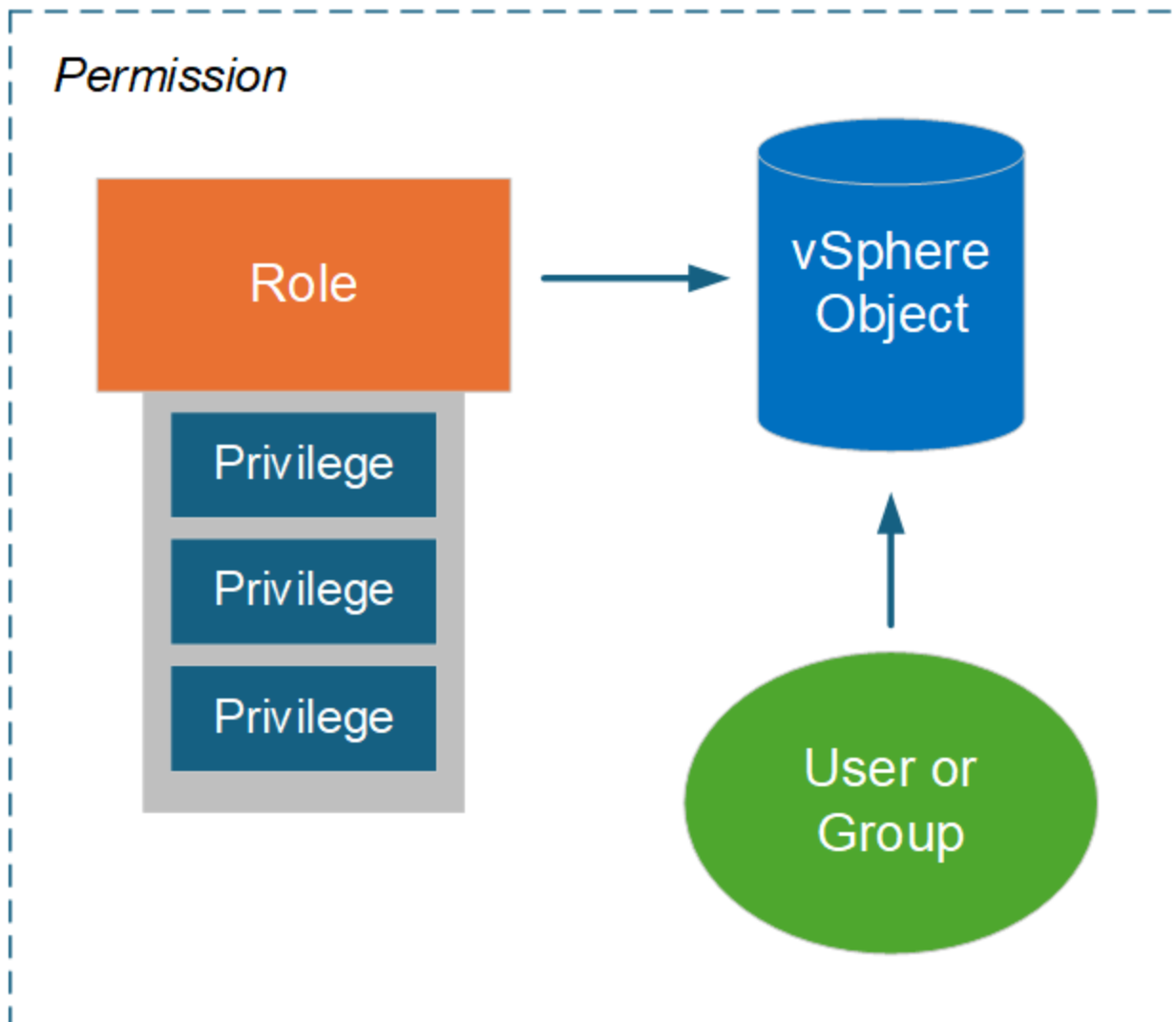
RBAC con VMware vSphere

Come funziona RBAC di vCenter Server con ONTAP tools

VMware vCenter Server offre una funzionalità RBAC che consente di controllare l'accesso agli oggetti vSphere. Si tratta di una parte importante dei servizi di sicurezza per l'autenticazione e l'autorizzazione centralizzati di vCenter.

Immagine di un'autorizzazione vCenter Server

Un'autorizzazione è la base per applicare il controllo degli accessi nell'ambiente vCenter Server. Viene applicato a un oggetto vSphere con un utente o un gruppo incluso nella definizione dell'autorizzazione. Un'illustrazione di alto livello di un'autorizzazione vCenter è riportata nella figura seguente.



Componenti di un'autorizzazione vCenter Server

Un'autorizzazione vCenter Server è un pacchetto di diversi componenti che sono associati insieme quando viene creata l'autorizzazione.

Oggetti vSphere

Le autorizzazioni sono associate agli oggetti vSphere, come vCenter Server, host ESXi, macchine virtuali, datastore, data center e cartelle. In base alle autorizzazioni assegnate all'oggetto, vCenter Server determina quali azioni o attività possono essere eseguite sull'oggetto da ciascun utente o gruppo. Per le attività specifiche degli strumenti ONTAP per VMware vSphere, tutte le autorizzazioni vengono assegnate e convalidate a livello di cartella principale o principale di vCenter Server. Per ulteriori informazioni, vedere ["USA RBAC con server vCenter"](#).

Privileges e ruoli

Esistono due tipi di vSphere Privileges utilizzati con i tool ONTAP per VMware vSphere 10. Per semplificare le operazioni con RBAC in questo ambiente, gli strumenti ONTAP forniscono ruoli che contengono la Privileges nativa e personalizzata richiesta. Il Privileges include:

- Privilegi vCenter Server nativi

Si tratta del Privileges fornito da vCenter Server.

- Privilegi specifici per i tool ONTAP

Si tratta di un'esclusiva di Privileges personalizzata per i tool ONTAP per VMware vSphere.

Utenti e gruppi

È possibile definire utenti e gruppi utilizzando Active Directory o l'istanza locale di vCenter Server. In combinazione con un ruolo, è possibile creare un'autorizzazione su un oggetto nella gerarchia degli oggetti vSphere. L'autorizzazione concede l'accesso in base ai privilegi del ruolo associato. Si noti 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 del ruolo, come parte dell'autorizzazione più ampia di vCenter Server.

vCenter Server: considerazioni RBAC per ONTAP tools

Ci sono diversi aspetti dei tool ONTAP per l'implementazione RBAC di VMware vSphere 10 con vCenter Server che è necessario considerare prima di utilizzarlo in un ambiente di produzione.

Ruoli vCenter e account amministratore

È necessario definire e utilizzare i ruoli vCenter Server personalizzati solo se si desidera limitare l'accesso agli oggetti vSphere e alle attività amministrative associate. Se non è necessario limitare l'accesso, è possibile utilizzare un account amministratore. Ogni account amministratore viene definito con il ruolo Amministratore al livello superiore della gerarchia degli oggetti. In questo modo, si ottiene l'accesso completo agli oggetti vSphere, inclusi quelli aggiunti dai tool ONTAP per VMware vSphere 10.

Gerarchia di oggetti vSphere

L'inventario degli oggetti vSphere è organizzato in una gerarchia. Ad esempio, è possibile spostare la gerarchia in basso come segue:

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

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

Ruoli inclusi nei tool ONTAP per VMware vSphere 10

Per semplificare le operazioni con vCenter Server RBAC, gli strumenti ONTAP per VMware vSphere offrono ruoli predefiniti personalizzati in base a diverse attività amministrative.



Se necessario, è possibile creare nuovi ruoli personalizzati. In questo caso, è necessario clonare uno dei ruoli degli strumenti ONTAP esistenti e modificarlo secondo necessità. Dopo aver apportato le modifiche alla configurazione, gli utenti del client vSphere interessato devono disconnettersi e riconnettersi per attivare le modifiche.

Per visualizzare gli ONTAP tools for VMware vSphere , selezionare **Menu** nella parte superiore di vSphere Client e fare clic su **Amministrazione** e quindi su **Ruoli** a sinistra. I seguenti privilegi devono essere inclusi nel ruolo assegnato all'utente vCenter responsabile della distribuzione o dell'onboarding di vCenter. Assicurarsi

che questi privilegi siano configurati come prerequisito per il processo di distribuzione o onboarding.

- Allarmi
 - Riconosci allarme
- Libreria di contenuti
 - Aggiungi elemento alla libreria
 - Effettua il check-in in un modello
 - Dai un'occhiata a un modello
 - Scarica i file
 - Importazione di spazio di archiviazione
 - Leggi l'archiviazione
 - Sincronizza elemento libreria
 - Sincronizza la libreria sottoscritta
 - Visualizza le impostazioni di configurazione
- Datastore
 - Assegnare spazio
 - Esplora il datastore
 - Operazioni sui file di basso livello
 - Rimuovi file
 - Aggiorna i file della macchina virtuale
 - Aggiorna i metadati della macchina virtuale
- Gestore agente ESX
 - Visualizzazione
- Cartella
 - Crea cartella
- Ospite
 - Configurazione
 - Impostazioni avanzate
 - Cambia impostazioni
 - Configurazione di rete
 - Risorse di sistema
 - Configurazione di avvio automatico della macchina virtuale
 - Operazioni locali
 - Crea macchina virtuale
 - Elimina macchina virtuale
 - Riconfigurare la macchina virtuale
- Rete
 - Assegna rete

- Configurare
- OvfManager
 - Accesso OvfConsumer
- Profilo host
 - Visualizzazione
- Risorsa
 - Assegna la macchina virtuale al pool di risorse
- Attività pianificata
 - Crea attività
 - Modifica attività
 - Esegui attività
- Compiti
 - Crea attività
 - Aggiorna attività
- vApp
 - Aggiungi macchina virtuale
 - Assegna pool di risorse
 - Assegna vApp
 - Creare
 - Importare
 - Mossa
 - Spegnimento
 - Accendi
 - Estrai dall'URL
 - Visualizza l'ambiente OVF
- Macchina virtuale
 - Cambia configurazione
 - Aggiungi disco esistente
 - Aggiungi nuovo disco
 - Aggiungi o rimuovi dispositivo
 - Configurazione avanzata
 - Cambia il conteggio della CPU
 - Cambia memoria
 - Cambia impostazioni
 - Cambia risorsa
 - Estendi disco virtuale
 - Modificare le impostazioni del dispositivo

- Rimuovi disco
- Reimposta le informazioni degli ospiti
- Aggiorna la compatibilità della macchina virtuale
- Modifica inventario
 - Crea da esistente
 - Crea nuovo
 - Mossa
 - Registro
 - Rimuovere
 - Annulla registrazione
- Interazione
 - Operazione di backup su macchina virtuale
 - Configurare il supporto CD
 - Configurare il supporto floppy
 - Connetti i dispositivi
 - Interazione con la console
 - Gestione del sistema operativo guest tramite API VIX
 - Spegnimento
 - Accendi
 - Reset
 - Sospendere
- Approvvigionamento
 - Consenti l'accesso al disco
 - Modello clone
 - Personalizza ospite
 - Distribuisci modello
 - Modificare le specifiche di personalizzazione
 - Leggi le specifiche di personalizzazione
- Gestione degli snapshot
 - Crea snapshot
 - Rimuovi snapshot
 - Rinomina snapshot
 - Ripristina snapshot

Sono disponibili tre ruoli predefiniti, come descritto di seguito.

Strumenti NetApp ONTAP per l'amministratore di VMware vSphere

Fornisce tutti gli strumenti vCenter Server Privileges e ONTAP nativi, specifici per Privileges, necessari per eseguire i principali strumenti ONTAP per i task di amministrazione di VMware vSphere.

Tool NetApp ONTAP per VMware vSphere in sola lettura

Fornisce accesso in sola lettura agli strumenti ONTAP. Questi utenti non possono eseguire strumenti ONTAP per le azioni VMware vSphere controllate dall'accesso.

Tool NetApp ONTAP per il provisioning di VMware vSphere

Fornisce alcuni dei privilegi nativi di vCenter Server e dei privilegi specifici degli strumenti ONTAP necessari per il provisioning dello storage. È possibile eseguire le seguenti operazioni:

- Creare nuovi datastore
- Gestire i datastore

Oggetti vSphere e backend dello storage ONTAP

I due ambienti RBAC lavorano insieme. Quando si esegue un'operazione nell'interfaccia client vSphere, vengono controllati per primi i ruoli degli strumenti ONTAP definiti in vCenter Server. Se l'operazione è consentita da vSphere, viene esaminata la Privileges ruolo ONTAP. Questa seconda fase viene eseguita in base al ruolo ONTAP assegnato all'utente al momento della creazione e della configurazione del backend di storage.

Utilizzo di vCenter Server RBAC

Quando si lavora con vCenter Server Privileges e con le autorizzazioni, è necessario prendere in considerazione alcuni aspetti.

Privilegi richiesti

Per accedere agli strumenti ONTAP per l'interfaccia utente di VMware vSphere 10, è necessario disporre del privilegio *View* specifico di ONTAP tools. Se si accede a vSphere senza questo privilegio e si fa clic sull'icona NetApp, gli strumenti di ONTAP per VMware vSphere visualizzano un messaggio di errore e impediscono l'accesso all'interfaccia utente.

Il livello di assegnazione nella gerarchia degli oggetti vSphere determina le parti dell'interfaccia utente a cui è possibile accedere. L'assegnazione del privilegio *View* all'oggetto root consente di accedere agli strumenti ONTAP per VMware vSphere facendo clic sull'icona NetApp.

È invece possibile assegnare il privilegio *View* a un altro livello di oggetto vSphere inferiore. Tuttavia, ciò limiterà gli strumenti ONTAP per i menu VMware vSphere a cui è possibile accedere e utilizzare.

Assegnazione delle autorizzazioni

Se si desidera limitare l'accesso agli oggetti e ai task vSphere, è necessario utilizzare le autorizzazioni di vCenter Server. Quando si assegna l'autorizzazione nella gerarchia degli oggetti vSphere, gli strumenti ONTAP per le attività di VMware vSphere 10 che gli utenti possono eseguire.



A meno che non sia necessario definire un accesso più restrittivo, in genere è buona norma assegnare autorizzazioni a livello dell'oggetto principale o della cartella principale.

Le autorizzazioni disponibili con i tool ONTAP per VMware vSphere 10 si applicano a oggetti non vSphere personalizzati, come i sistemi storage. Se possibile, è necessario assegnare queste autorizzazioni agli strumenti ONTAP per l'oggetto root VMware vSphere poiché non è possibile assegnarlo a un oggetto vSphere. Ad esempio, qualsiasi autorizzazione che includa un privilegio "Aggiungi/Modifica/Rimuovi sistemi di archiviazione" degli strumenti ONTAP per VMware vSphere deve essere assegnata a livello di oggetto root.

Quando si definisce un'autorizzazione a un livello superiore nella gerarchia degli oggetti, è possibile configurarla in modo che venga trasferita e ereditata dagli oggetti figlio. Se necessario, è possibile assegnare autorizzazioni aggiuntive agli oggetti figlio che sovrascrivono le autorizzazioni ereditate dal padre.

È possibile modificare un'autorizzazione in qualsiasi momento. Se si modifica uno dei Privileges all'interno di un'autorizzazione, gli utenti associati all'autorizzazione devono disconnettersi da vSphere e riconnettersi per abilitare la modifica.

RBAC con ONTAP

Come funziona ONTAP RBAC con ONTAP tools

ONTAP fornisce un ambiente RBAC solido ed estensibile. Puoi utilizzare la funzionalità RBAC per controllare l'accesso alle operazioni di storage e sistema così come esposte attraverso l'API REST e la CLI. È utile acquisire familiarità con l'ambiente prima di utilizzarlo con gli strumenti ONTAP per la distribuzione di VMware vSphere 10.

Panoramica delle opzioni amministrative

Ci sono diverse opzioni disponibili quando si utilizza RBAC ONTAP in base al tuo ambiente e agli obiettivi. Di seguito viene presentata una panoramica delle principali decisioni amministrative. Per ulteriori informazioni, vedere anche ["Automazione ONTAP: Panoramica della sicurezza RBAC"](#).



ONTAP RBAC è progettato su misura per un ambiente di archiviazione ed è più semplice dell'implementazione RBAC fornita con vCenter Server. Con ONTAP, assegna un ruolo direttamente all'utente. Con ONTAP RBAC non è necessario configurare autorizzazioni esplicite, come quelle utilizzate con vCenter Server.

Tipi di ruoli e Privileges

Quando si definisce un utente ONTAP, è necessario un ruolo ONTAP. Esistono due tipi di ruoli ONTAP:

- RIPOSO

I ruoli REST sono stati introdotti con ONTAP 9.6 e vengono generalmente applicati agli utenti che accedono a ONTAP tramite l'API REST. Le Privileges incluse in questi ruoli sono definite in termini di accesso agli endpoint delle API REST ONTAP e alle azioni associate.

- Tradizionale

Questi sono i ruoli legacy inclusi prima di ONTAP 9.6. Essi continuano a essere un aspetto fondamentale del RBAC. Le Privileges sono definite in termini di accesso ai comandi della CLI di ONTAP.

Mentre i ruoli RESTANTI sono stati introdotti più recentemente, i ruoli tradizionali hanno alcuni vantaggi. Ad esempio, è possibile includere facoltativamente parametri di query aggiuntivi in modo che Privileges definisca in modo più preciso gli oggetti a cui vengono applicati.

Scopo

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

Definizioni dei ruoli

ONTAP offre un set di ruoli predefiniti a livello di cluster e SVM. È inoltre possibile definire ruoli personalizzati.

Utilizzo dei ruoli REST ONTAP

Quando si utilizzano i ruoli REST ONTAP inclusi negli strumenti ONTAP per VMware vSphere 10, è necessario prendere in considerazione diverse considerazioni.

Mappatura dei ruoli

Indipendentemente dall'utilizzo di un ruolo tradizionale o REST, tutte le decisioni relative all'accesso a ONTAP vengono prese in base al comando CLI sottostante. Tuttavia, poiché Privileges in un ruolo REST è definito in termini di endpoint API REST, ONTAP deve creare un ruolo tradizionale *mapped* per ciascuno dei ruoli REST. Pertanto, ogni ruolo REST viene associato a un ruolo tradizionale sottostante. In questo modo, ONTAP può prendere decisioni sul controllo degli accessi in modo coerente, indipendentemente dal tipo di ruolo. Non è possibile modificare i ruoli mappati paralleli.

Definizione di un ruolo REST tramite CLI Privileges

Poiché ONTAP utilizza sempre i comandi CLI per determinare l'accesso a livello base, è possibile esprimere un ruolo REST utilizzando il comando CLI Privileges invece degli endpoint REST. Uno dei vantaggi di questo approccio è la granularità aggiuntiva disponibile con i ruoli tradizionali.

Interfaccia amministrativa per la definizione dei ruoli ONTAP

Puoi creare utenti e ruoli con l'interfaccia a riga di comando e l'API REST di ONTAP. Tuttavia, è più conveniente utilizzare l'interfaccia di Gestione sistema insieme al file JSON disponibile tramite il Gestore strumenti ONTAP. Per ulteriori informazioni, vedere ["USA RBAC ONTAP con tool ONTAP per VMware vSphere 10"](#).

Considerazioni RBAC di ONTAP per ONTAP tools

Esistono diversi aspetti dei tool ONTAP per l'implementazione RBAC di VMware vSphere 10 con ONTAP che è necessario prendere in considerazione prima di utilizzarlo in un ambiente di produzione.

Panoramica del processo di configurazione

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

Le fasi principali della configurazione sono descritte in alto di seguito. Per ["Configurare i ruoli e i privilegi degli utenti ONTAP"](#) ulteriori dettagli, fare riferimento a.

1. Preparatevi

È necessario disporre delle credenziali di amministratore per ONTAP Tools Manager e per il cluster ONTAP.

2. Scaricare il file di definizione JSON

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

3. Creare un utente ONTAP con un ruolo

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

1. Selezionare **Cluster** sulla sinistra, quindi **Settings**.
2. Scorrere fino a **utenti e ruoli** e fare clic su **→**.
3. Selezionare **Aggiungi** in **utenti** e selezionare **prodotti di virtualizzazione**.

4. Selezionare il file JSON sulla workstation locale e caricarlo.

4. Configurare il ruolo

Come parte della definizione del ruolo, è necessario prendere diverse decisioni amministrative. Per ulteriori informazioni, vedere [Configurare il ruolo utilizzando System Manager](#).

Configurare il ruolo utilizzando System Manager

Dopo aver iniziato a creare un nuovo utente e ruolo con System Manager e aver caricato il file JSON, è possibile personalizzare il ruolo in base all'ambiente e alle esigenze.

Configurazione principale di utenti e ruoli

Le definizioni dei RBAC sono composte da diverse funzionalità dei prodotti, tra cui combinazioni di VSC, VASA Provider e SRA. Devi selezionare l'ambiente o gli ambienti in cui hai bisogno di supporto RBAC. Ad esempio, se si desidera che i ruoli supportino la funzionalità plug-in remoto, selezionare VSC. È inoltre necessario scegliere il nome utente e la password associata.

Privilegi

Le Privileges del ruolo sono organizzate in quattro serie in base al livello di accesso necessario allo storage ONTAP. Le Privileges su cui si basano i ruoli includono:

- Discovery (rilevamento)

Questo ruolo consente di aggiungere sistemi storage.

- Creare storage

Questo ruolo consente di creare storage. Include inoltre tutte le Privileges associate al ruolo di rilevamento.

- Modificare l'archiviazione

Questo ruolo consente di modificare lo storage. Include inoltre tutta la Privileges associata al rilevamento e alla creazione dei ruoli storage.

- Distruzione dello storage

Questo ruolo consente di distruggere lo storage. Include inoltre tutta la Privileges associata al rilevamento, la creazione di storage e la modifica dei ruoli storage.

Generare l'utente con un ruolo

Dopo aver selezionato le opzioni di configurazione per il proprio ambiente, fare 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")
- Capacità 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.

Implementa i tool ONTAP per VMware vSphere

Avvio rapido dei tool ONTAP per VMware vSphere

Con questa sezione di avvio rapido puoi configurare gli ONTAP tools for VMware vSphere .

Inizialmente, distribuirai gli ONTAP tools for VMware vSphere come una configurazione a nodo singolo di piccole dimensioni che fornisce servizi principali per supportare i datastore NFS e VMFS. Per espandere la configurazione con contenitori aggiuntivi per servizio, maggiore resilienza o per utilizzare datastore vVols e alta disponibilità (HA), completare prima questo flusso di lavoro e poi procedere con i passaggi di espansione. Per ulteriori informazioni, fare riferimento al ["Workflow di implementazione HA"](#) .

1

Pianificare la distribuzione

Verifica che le versioni degli host vSphere, ONTAP ed ESXi siano compatibili con la versione degli strumenti ONTAP . Alloca CPU, memoria e spazio su disco sufficienti. In base alle tue regole di sicurezza, potrebbe essere necessario configurare firewall o altri strumenti di sicurezza per consentire il traffico di rete.

Assicurarsi che vCenter Server sia installato e accessibile.

- ["Tool di matrice di interoperabilità"](#)
- ["Strumenti ONTAP per requisiti e limiti di configurazione VMware vSphere"](#)
- ["Prima di iniziare"](#)

2

Implementa i tool ONTAP per VMware vSphere

Inizialmente, implementerai gli ONTAP tools for VMware vSphere come una configurazione a singolo nodo di piccole dimensioni che fornisce servizi core per supportare datastore NFS e VMFS. Se prevedi di espandere la configurazione per utilizzare datastore vVols e alta disponibilità (HA), lo farai al termine di questo flusso di lavoro. Per espandere la configurazione ad alta disponibilità (HA), assicurati che le opzioni CPU hot-add e memory hot-plug siano abilitate.

- ["Implementa i tool ONTAP per VMware vSphere"](#)

3

Aggiungere istanze di vCenter Server

Aggiungere istanze di vCenter Server agli ONTAP tools for VMware vSphere per configurare, gestire e proteggere i datastore virtuali nell'ambiente vCenter Server.

- ["Aggiungere istanze di vCenter Server"](#)

4

Configurare i ruoli utente ONTAP e Privileges

Configurare nuovi ruoli utente e Privileges per la gestione dei backend di storage utilizzando il file JSON fornito con gli strumenti ONTAP per VMware vSphere.

- ["Configurare i ruoli e i privilegi degli utenti ONTAP"](#)

5

Configurare i backend di archiviazione

Aggiunta di un backend dello storage a un cluster ONTAP. Per le configurazioni multi-tenancy in cui vCenter agisce come tenant con una SVM associata, utilizza ONTAP Tools Manager per aggiungere il cluster. Associare il backend dello storage con vCenter Server per associarlo globalmente all'istanza di vCenter Server integrata.

Aggiungi i backend dello storage locale con credenziali cluster o SVM utilizzando l'interfaccia utente dei tool ONTAP. Questi backend di storage sono limitati a un singolo vCenter. Quando si utilizzano le credenziali del cluster a livello locale, le SVM associate vengono associate automaticamente mappate in vCenter per gestire vVol o VMFS. Per la gestione di VMFS, incluso SRA, i tool ONTAP supportano le credenziali SVM senza richiedere un cluster globale.

- ["Aggiungere un backend di storage"](#)
- ["Associare il backend dello storage a un'istanza di vCenter Server"](#)

6

Aggiorna i certificati se stai lavorando con più istanze di vCenter Server

Quando si lavora con più istanze di vCenter Server, aggiornare il certificato autofirmato a un certificato firmato da un'autorità di certificazione (CA).

- ["Gestire i certificati"](#)

7

(Facoltativo) Configurare la protezione SRA

Abilitare la funzionalità SRA per configurare il disaster recovery e proteggere datastore NFS o VMFS.

- ["Abilita i tool ONTAP per i servizi VMware vSphere"](#)
- ["Configurare SRA sull'appliance VMware Live Site Recovery"](#)

8

(Opzionale) attivare la protezione di sincronizzazione attiva SnapMirror

Configura i tool ONTAP per VMware vSphere per gestire la protezione dei cluster host per la sincronizzazione attiva di SnapMirror. Eseguire il cluster ONTAP e il peering SVM nei sistemi ONTAP per utilizzare SnapMirror ActiveSync. Questo vale solo per gli archivi dati VMFS.

- ["Proteggere utilizzando la protezione del cluster host"](#)

9

Configurare backup e recovery per i tool ONTAP per l'implementazione di VMware vSphere

Il backup è abilitato per impostazione predefinita negli ONTAP tools for VMware vSphere 10.5 e viene eseguito ogni 10 minuti. Pianifica i backup degli 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 strumenti ONTAP"](#)

Flusso di lavoro di distribuzione ad alta disponibilità per ONTAP tools

Per aumentare la resilienza e supportare più container per servizio, espandi la distribuzione iniziale degli strumenti ONTAP a una configurazione ad alta disponibilità (HA). L'abilitazione del servizio VASA Provider è obbligatoria per i datastore vVols in una configurazione HA.

1

Scala in verticale l'implementazione

Puoi scalare in verticale i tool di ONTAP per la configurazione di VMware vSphere per aumentare il numero di nodi nell'implementazione e modificare la configurazione in un setup ha.

- ["Modifica i tool di ONTAP per la configurazione di VMware vSphere"](#)

2

Attivare i servizi

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

Abilitare i servizi SRA a utilizzare gli strumenti ONTAP Storage Replication Adapter (SRA) per VMware Site Recovery Manager (SRM) o VMware Live Site Recovery (VLSR).

- ["Abilitare i servizi VASA e SRA"](#)

3

Aggiornare i certificati

Se si utilizzano datastore vVol con più istanze di vCenter Server, aggiornare il certificato autofirmato a un certificato firmato dall'autorità di certificazione (CA).

- ["Gestire i certificati"](#)

Strumenti ONTAP per requisiti e limiti di configurazione VMware vSphere

Prima di implementare gli strumenti ONTAP per VMware vSphere, è necessario conoscere i requisiti di spazio per il pacchetto di implementazione e alcuni requisiti di base del sistema host.

Puoi utilizzare tool ONTAP per VMware vSphere con VMware vCenter Server Virtual Appliance (vCSA). È necessario implementare i tool ONTAP per VMware vSphere su un client vSphere supportato che include il sistema ESXi.

Requisiti di sistema

- **Requisiti di spazio per il pacchetto di installazione per nodo**

- 15 GB per le installazioni con thin provisioning
- 348 GB per installazioni con thick provisioning
- **Requisiti di dimensionamento del sistema host** La tabella seguente mostra la memoria consigliata per ogni dimensione di distribuzione. Per le distribuzioni ad alta disponibilità (HA), è necessaria una dimensione dell'appliance tre volte superiore a quella indicata.

Tipo di distribuzione	CPU per nodo	Memoria (GB) per nodo	Spazio su disco (GB) con thick provisioning per nodo
Piccolo	9	18	350
Medio	13	26	350
NOTA BENE: L'implementazione estesa è solo per la configurazione ha.	17	34	350



Una volta abilitato il backup, ogni cluster di tool ONTAP necessita di altri 50GB di spazio nel datastore in cui vengono implementate le macchine virtuali. Pertanto, una piattaforma non ha richiede 400 GB e ha richiede 1100 GB di spazio in totale.

Requisiti minimi di archiviazione e applicazione

Storage, host e applicazioni	Requisiti di versione
ONTAP	9.15.1, 9.16.1, e 9.17.0
Gli strumenti ONTAP supportavano gli host ESXi	da 7.0.3 in poi
Gli strumenti ONTAP supportavano vCenter Server	Da 7.0U3
Provider VASA	3,0
Applicazione OVA	10,5
Host ESXi per implementare la macchina virtuale degli strumenti ONTAP	7.0U3 e 8.0U3
vCenter Server per implementare la macchina virtuale degli strumenti ONTAP	7.0 e 8.0



A partire dai tool ONTAP per VMware vSphere 10,4, l'hardware della macchina virtuale viene modificato dalla versione 10 alla 17.

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

["Tool di matrice di interoperabilità"](#)

Requisiti delle porte

La tabella seguente illustra le porte di rete utilizzate da NetApp e le relative funzioni. 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, consentendo l'integrazione con sistemi esterni all'ambiente cluster.
- **Porte inter-nodo:** queste porte consentono la comunicazione tra i nodi all'interno del cluster Kubernetes. Sono necessari per attività di clustering come la condivisione di dati e la collaborazione. Per le distribuzioni a nodo singolo, le porte tra nodi vengono utilizzate solo all'interno del nodo e non necessitano di accesso esterno. Le porte internodo possono accettare traffico dall'esterno del cluster. Bloccare l'accesso a Internet alle porte tra nodi tramite regole firewall.
- **Porte interne:** queste porte comunicano all'interno del cluster Kubernetes utilizzando indirizzi ClusterIP. Non sono esposti esternamente e non devono essere aggiunti alle regole del firewall.



Assicurarsi che tutti i nodi degli strumenti ONTAP risiedano nella stessa subnet per mantenere una comunicazione ininterrotta tra loro.

Fare clic per espandere o comprimere la tabella dei requisiti delle porte.

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

Nome del servizio/componente	Porta	Protocollo	Tipo di porta	Descrizione
kubelet	10248, 10250	TCP	Inter-nodo	Componente Kubernetes
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
nodo calico	9091, 9099	TCP	Inter-nodo	Componente di rete Calico.
contenitore	10010	TCP	Inter-nodo	Servizio demone del contenitore.
VXLAN (flanella)	8472	UDP	Inter-nodo	Rete di sovrapposizione per la comunicazione tra pod.



Per le distribuzioni HA, assicurarsi che la porta UDP 8472 sia aperta tra tutti i nodi. Questa porta consente la comunicazione pod-to-pod tra i nodi; bloccandola si interromperà la rete tra nodi.

Limiti di configurazione per distribuire ONTAP tools for VMware vSphere per vVols datastore

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

Implementazione	Tipo	Numero di vVol	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 Small	200	80	32
Terreno non ha	250	100	32
HA piccolo	350	200	64
HA Media	600	200	128
HA grande	1024	250	256

Tool ONTAP per VMware vSphere - Storage Replication Adapter (SRA)

La tabella seguente mostra i numeri supportati per istanza di VMware Live Site Recovery utilizzando gli strumenti ONTAP per VMware vSphere.

Dimensione della distribuzione vCenter	Piccolo	Medio
Numero totale di macchine virtuali configurate per la protezione mediante replica basata su array	2000	5000
Numero totale di gruppi di protezione da replica basati su array	250	250
Numero totale di gruppi di protezione per piano di ripristino	50	50
Numero di datastore replicati	255	255
Numero di macchine virtuali	4000	7000

La tabella seguente mostra il numero di VMware Live Site Recovery e i corrispondenti strumenti ONTAP per le

dimensioni della distribuzione di VMware vSphere.

Numero di istanze di VMware Live Site Recovery	Dimensioni di distribuzione degli strumenti ONTAP
Fino a 4	Piccolo
da 4 a 8	Medio
Più di 8	Grande

Per ulteriori informazioni, fare riferimento a "[Limiti operativi di VMware Live Site Recovery](#)".

Requisiti di pre-distribuzione per ONTAP tools

Prima di procedere con la distribuzione, assicurarsi che siano soddisfatti i seguenti requisiti:

Requisiti	Il tuo stato
La versione vSphere, la versione ONTAP e la versione host ESXi sono compatibili con la versione dei tool ONTP.	<input type="checkbox"/> Sì <input type="checkbox"/> No
L'ambiente vCenter Server è configurato e configurato	<input type="checkbox"/> Sì <input type="checkbox"/> No
La cache del browser è stata eliminata	<input type="checkbox"/> Sì <input type="checkbox"/> No
Si dispone delle credenziali vCenter Server padre	<input type="checkbox"/> Sì <input type="checkbox"/> No
Si dispone delle credenziali di accesso per l'istanza di vCenter Server, a cui gli strumenti ONTAP per VMware vSphere si collegheranno dopo la distribuzione per la registrazione	<input type="checkbox"/> Sì <input type="checkbox"/> No
Il nome di dominio su cui viene emesso il certificato viene mappato all'indirizzo IP virtuale in una distribuzione multi-vCenter in cui i certificati CA personalizzati sono obbligatori.	<input type="checkbox"/> Sì <input type="checkbox"/> No
È stato eseguito il controllo nslookup sul nome di dominio per verificare se il dominio viene risolto all'indirizzo IP desiderato.	<input type="checkbox"/> Sì <input type="checkbox"/> No
Il certificato viene creato con il nome di dominio e l'indirizzo IP degli strumenti ONTAP.	<input type="checkbox"/> Sì <input type="checkbox"/> No
L'applicazione degli strumenti ONTAP e i servizi interni sono raggiungibili da vCenter Server.	<input type="checkbox"/> Sì <input type="checkbox"/> No
Utilizzando SVM multi-tenant, disponi di un LIF di gestione SVM su ciascuna SVM.	<input type="checkbox"/> Sì <input type="checkbox"/> No

Foglio di lavoro distribuzione

Per implementazione a nodo singolo

Utilizzare il seguente foglio di lavoro per raccogliere le informazioni richieste per gli strumenti ONTAP per la distribuzione iniziale di 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 <code>https://<ip>:8443/virtualization/ui/</code>	
Gli strumenti ONTAP forniscono un indirizzo IP virtuale per la comunicazione interna. Questo indirizzo IP viene utilizzato per la comunicazione interna in una configurazione con più istanze di strumenti ONTAP . Questo indirizzo IP non deve essere uguale all'indirizzo IP dell'applicazione degli strumenti ONTAP (piano di controllo Kubernetes).	
Nome host DNS per il nodo di gestione degli strumenti ONTAP	
Server DNS primario	
Server DNS secondario	
Dominio di ricerca DNS	
Indirizzo IPv4 per il nodo di gestione degli strumenti ONTAP. 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.	
Subnet mask dell'indirizzo IPv4	
Gateway predefinito per l'indirizzo IPv4	
Indirizzo IPv6 (opzionale)	
Lunghezza prefisso IPv6 (opzionale)	
Gateway per l'indirizzo IPv6 (opzionale)	



Creare record DNS per tutti gli indirizzi IP indicati sopra. Prima di assegnare i nomi host, eseguire il mapping agli indirizzi IP liberi sul DNS. Tutti gli indirizzi IP devono trovarsi sulla stessa VLAN selezionata per la distribuzione.

Per l'implementazione ha (High Availability, alta disponibilità)

Oltre ai requisiti di implementazione a nodo singolo, per l'implementazione ha sono necessarie le seguenti informazioni:

Requisito	Il tuo valore
Server DNS primario	

Server DNS secondario	
Dominio di ricerca DNS	
Nome host DNS per il secondo nodo	
Indirizzo IP per il secondo nodo	
Nome host DNS per il terzo nodo	
Indirizzo IP per il terzo nodo	

Configurazione del firewall di rete

Assicurarsi che le porte firewall necessarie siano aperte per tutti gli indirizzi IP rilevanti. Gli strumenti ONTAP richiedono l'accesso al LIF tramite la porta 443. Per un elenco completo delle porte richieste, vedere la sezione requisiti delle porte all'indirizzo "[Strumenti ONTAP per requisiti e limiti di configurazione VMware vSphere](#)".

Impostazioni di archiviazione di ONTAP

Per garantire un'integrazione perfetta dello storage ONTAP con i tool ONTAP per VMware vSphere, prendi in considerazione le seguenti impostazioni:

- Se si utilizza Fibre Channel (FC) per la connettività di storage, configurare la suddivisione in zone sugli switch FC per connettere gli host ESXi con i LIF FC dell'SVM. "[Scoprite lo zoning FC e FCoE con i sistemi ONTAP](#)"
- Per utilizzare la replica SnapMirror gestita dagli strumenti ONTAP, l'amministratore dello storage ONTAP deve creare "[Relazioni di peer dei cluster ONTAP](#)" e "[Relazioni peer SVM ONTAP intercluster](#)" in ONTAP prima di utilizzare SnapMirror.

Distribuisci ONTAP tools

Gli ONTAP tools for VMware vSphere vengono distribuiti come un singolo nodo di piccole dimensioni con servizi principali per supportare i datastore NFS e VMFS. Il processo di distribuzione degli strumenti ONTAP potrebbe richiedere fino a 45 minuti.

Prima di iniziare

Se si distribuisce un singolo nodo di piccole dimensioni, la libreria di contenuti è facoltativa. Per le distribuzioni multi-nodo o HA è necessaria una libreria di contenuti. In VMware, una libreria di contenuti archivia modelli di VM, modelli di vApp e altri file. L'implementazione con una libreria di contenuti garantisce un'esperienza fluida perché non dipende dalla connettività di rete.

Prima di creare una libreria di contenuti, tieni presente quanto segue:

- Creare la libreria dei contenuti su un datastore condiviso in modo che tutti gli host del cluster possano accedervi.
- Configurare la libreria dei contenuti prima di distribuire gli ONTAP tools for VMware vSphere OVA.
- Assicurarsi che la libreria dei contenuti sia stata creata prima di configurare l'appliance per HA.



Non eliminare il modello OVA nella libreria dei contenuti dopo la distribuzione.



Per abilitare la distribuzione HA in futuro, evitare di distribuire la macchina virtuale degli strumenti ONTAP direttamente su un host ESXi. In alternativa, distribuiscilo all'interno di un cluster host ESXi o di un pool di risorse.

Per creare una libreria di contenuti, segui questi passaggi:

1. Scarica il file contenente i file binari (.ova) e i certificati firmati per gli ONTAP tools for VMware vSphere da ["Sito di supporto NetApp"](#).
2. Accedere al client vSphere
3. Selezionare il menu del client vSphere e selezionare **Libreria di contenuti**.
4. Selezionare **Crea** a destra della pagina.
5. Fornire un nome per la libreria e creare la libreria di contenuti.
6. Vai alla libreria dei contenuti che hai creato.
7. Selezionare **azioni** nella parte destra della pagina e selezionare **Importa elemento** e importare il file OVA.



Per ulteriori informazioni, consulta il ["Creazione e utilizzo della libreria di contenuti"](#) blog.



Prima di procedere con la distribuzione, impostare il Distributed Resource Scheduler (DRS) del cluster nell'inventario su "Conservativo". In questo modo si garantisce che le VM non vengano migrate durante l'installazione.

Inizialmente, gli ONTAP tools for VMware vSphere vengono distribuiti come configurazione non HA. Per scalare verso un'implementazione HA, è necessario abilitare il plug-in a caldo della CPU e il plug-in a caldo della memoria. È possibile eseguire questo passaggio come parte del processo di implementazione o modificare le impostazioni della VM dopo l'implementazione.

Fasi

1. Scaricare il file che contiene i file binari (.ova) e i certificati firmati per il ONTAP tools for VMware vSphere dal. Se hai importato l'OVA nella libreria dei contenuti, puoi saltare questo passaggio e procedere con quello successivo
2. Accedere al server vSphere.
3. Accedere al pool di risorse, al cluster o all'host in cui si intende distribuire l'OVA.



Non memorizzare mai i tool ONTAP per la macchina virtuale VMware vSphere nei datastore vVol gestiti.

4. È possibile distribuire l'OVA dalla libreria di contenuti o dal sistema locale.

Dal sistema locale	Dalla libreria di contenuti
a. fare clic con il pulsante destro del mouse e selezionare Deploy OVF template... b. scegliere il file OVA dall'URL o navigare fino alla posizione desiderata, quindi selezionare Next .	a. accedere alla libreria di contenuti e selezionare l'elemento della libreria che si desidera distribuire. b. selezionare azioni > Nuova VM da questo modello

5. Nel campo **Select a name and folder** (Seleziona un nome e una cartella*), immettere il nome della macchina virtuale e sceglierne la posizione.

- Se si utilizza la versione vCenter Server 8.0.3, selezionare l'opzione **Personalizza l'hardware di**

questa macchina virtuale, che attiverà un'ulteriore fase chiamata **Personalizza hardware** prima di passare alla finestra **Pronto per il completamento**.

- Se si utilizza la versione vCenter Server 7.0.3, seguire i passaggi nella sezione **cosa succede dopo?** alla fine della distribuzione.

netapp-ontap-tools-for-vmware-vsphere-10.4-1740090540 - New Virtual Machine from Content Library

- 1 Select a creation type
- 2 Select a template
- 3 Select a name and folder**
- 4 Select a compute resource
- 5 Review details
- 6 Select storage
- 7 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: demootv

Select a location for the virtual machine.

vcf-vc01.ontappmtme.openenglab.netapp.com
> Raleigh

- Customize the operating system
 Customize this virtual machine's hardware

CANCEL

BACK

NEXT

6. Selezionare una risorsa di computer e selezionare **Avanti**. Se lo si desidera, selezionare la casella **Accendi automaticamente VM distribuita**.
7. Esaminare i dettagli del modello e selezionare **Avanti**.
8. Leggere e accettare il contratto di licenza e selezionare **Avanti**.
9. Selezionare lo spazio di archiviazione per la configurazione e il formato del disco, quindi selezionare **Avanti**.
10. Selezionare la rete di destinazione per ciascuna rete di origine e selezionare **Avanti**.
11. Nella finestra **Personalizza modello**, compila i campi richiesti.

netapp-ontap-tools-for-vmware-vmphere-10.5-1758196320 - New Virtual Machine from Content Library

- 1 Select a name and folder
- 2 Select a compute resource
- 3 Review details
- 4 License agreements
- 5 Select storage
- 6 Select networks
- 7 Customize template**
- 8 Customize hardware
- 9 Ready to complete

Customize template ✕

NTP Servers	A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware tools based time synchronization will be used
▼ Deployment Configuration	2 settings
ONTAP tools IP address*	This will be the primary interface for communication with ONTAP tools
ONTAP tools virtual IP address*	ONTAP tools uses this IP address for internal communication
▼ vCenter Configuration	3 settings
vCenter hostname*	Provide the hostname of the vCenter Server.
vCenter username*	Provide the username of the vCenter Server. <u>administrator@vsphere.</u>
vCenter password*	To authenticate your login, provide the vCenter Server password.

CANCEL
BACK
NEXT



Il nome host vCenter è il nome dell'istanza di vCenter Server in cui è distribuito l'appliance degli strumenti ONTAP .

Se si distribuiscono strumenti ONTAP in una topologia a due vCenter Server, in cui l'appliance è ospitata in un'istanza di vCenter e ne gestisce un'altra, è possibile assegnare un ruolo limitato all'istanza di vCenter che ospita gli strumenti ONTAP . È possibile creare un utente e un ruolo vCenter dedicati con solo le autorizzazioni richieste per la distribuzione del modello OVF. Per i dettagli, vedere i ruoli elencati in "[Ruoli inclusi nei tool ONTAP per VMware vSphere 10](#)".

Per l'istanza vCenter che verrà gestita dagli strumenti ONTAP , assicurarsi che l'account utente vCenter disponga dei privilegi di amministratore.

- I nomi host devono includere lettere (A-Z, a-z), cifre (0-9) e trattini (-). Per configurare lo stack doppio, specificare il nome host mappato all'indirizzo IPv6.



Pure IPv6 non è supportato. La modalità mista è supportata con VLAN contenente indirizzi IPv6 e IPv4.

- L'indirizzo IP degli strumenti ONTAP è l'interfaccia principale per la comunicazione con gli strumenti ONTAP.
- IPv4 è il componente dell'indirizzo IP della configurazione del nodo, che può essere utilizzato per abilitare la shell diagnostica e l'accesso SSH sul nodo ai fini del debug e della manutenzione.

12. Quando si utilizza la versione vCenter Server 8.0.3, nella finestra **Personalizza hardware**, abilitare le opzioni **Aggiunta a caldo CPU** e **Collegamento a caldo della memoria** per consentire la funzionalità HA.

netapp-ontap-tools-for-vmware-vsphere-10.5-1740090540 - New Virtual Machine from Content Library

- 1 Select a creation type
- 2 Select a template
- 3 Select a name and folder
- 4 Select a compute resource
- 5 Review details
- 6 License agreements
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Customize hardware**
- 11 Ready to complete

Customize hardware

Virtual Hardware VM Options Advanced Parameters

ADD NEW DEVICE

CPU * 9 Sockets: 9

Cores per Socket 1

CPU Hot Plug Enable CPU Hot Add

Reservation 0 MHz

Limit Unlimited MHz

Shares Normal 1000

Hardware virtualization Expose hardware assisted virtualization to the guest OS

Performance Counters Enable virtualized CPU performance counters

Scheduling Affinity

Memory * 18 GB

Reservation 0 MB

Reserve all guest memory (All locked)

Limit Unlimited MB

Shares Normal 368640

Memory Hot Plug Enable

CANCEL BACK NEXT

13. Rivedere i dettagli nella finestra **Pronto per il completamento**, selezionare **fine**.

Quando viene creata l'attività di distribuzione, l'avanzamento viene visualizzato nella barra delle applicazioni di vSphere.

14. Accendere la macchina virtuale dopo aver completato l'attività se non è stata selezionata l'opzione di accensione automatica della macchina virtuale.

È possibile tenere traccia dell'avanzamento dell'installazione nella console Web della VM.

In caso di discrepanze nel modulo OVF, una finestra di dialogo richiederà un'azione correttiva. Utilizzare il pulsante Tab per navigare, apportare le modifiche necessarie e selezionare **OK**. Hai tre tentativi per risolvere eventuali problemi. Se i problemi persistono dopo tre tentativi, il processo di installazione si interromperà e si consiglia di riprovare l'installazione su una nuova macchina virtuale.

Cosa succederà?

Se disponi di strumenti ONTAP per VMware vSphere con vCenter Server 7,0.3, segui questi passaggi dopo l'implementazione.

1. Accedere al client vCenter
2. Spegnere il nodo ONTAP Tools.

3. Accedere agli ONTAP tools for VMware vSphere in **Inventari** e selezionare l'opzione **Modifica impostazioni**.
4. Nelle opzioni **CPU**, selezionare la casella di controllo **Abilita aggiunta a caldo CPU**
5. Nelle opzioni **memoria**, selezionare la casella di controllo **Abilita in Memory hot plug**.

Risolvi gli errori di distribuzione degli ONTAP tools

Se riscontri problemi durante la distribuzione, esamina i registri e i codici di errore per diagnosticare e risolvere i problemi. A partire dagli ONTAP tools for VMware vSphere 10.5, i bundle 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 registri di servizio degli strumenti ONTAP esistenti, migliorando il supporto e la risoluzione dei problemi.

Raccogliere i file di log

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



La generazione di log da ONTAP Tools Manager include tutti i log per tutte le istanze di vCenter Server. La generazione di log dall'interfaccia utente del client vCenter è prevista per vCenter Server selezionato.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **Log Bundle** dalla barra laterale.

Questa operazione può richiedere alcuni minuti.

4. Selezionare **generate** per generare i file di registro.
5. Immettere l'etichetta per il pacchetto di log e selezionare **genera**.

Scaricare il file tar.gz e inviarlo all'assistenza tecnica.

Per generare il bundle di log utilizzando l'interfaccia utente del client vCenter, procedere come segue:

Fasi

1. Accedere al client vSphere.
2. Dalla home page di vSphere Client, andare a **supporto** > **pacchetto di registrazione** > **genera**.
3. Specifica l'etichetta del bundle di log e generalo. L'opzione di download verrà visualizzata durante la generazione dei file. Il download potrebbe richiedere del tempo.



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

Codici di errore di distribuzione

Potrebbero verificarsi codici di errore durante gli strumenti ONTAP per le operazioni di distribuzione, riavvio e ripristino di VMware vSphere.

I codici di errore sono composti da cinque cifre, in cui le prime due rappresentano lo script che ha riscontrato il problema e le ultime tre cifre rappresentano il flusso di lavoro specifico all'interno dello script.

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



I codici di errore forniti in questa pagina sono solo a scopo di riferimento. Se l'errore persiste o se non è stata menzionata alcuna soluzione, contattare il team di supporto.

Nella tabella seguente sono elencati i codici di errore e i nomi dei file corrispondenti.

Codice errore	Nome script
00	firstboot-network-config.pl, distribuzione in modalità
01	firstboot-network-config.pl, aggiornamento della modalità
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, implementazione, ha
04	firstboot-deploy-otv-ng.pl, implementazione, non ha
05	firstboot-deploy-otv-ng.pl, riavviare
06	firstboot-deploy-otv-ng.pl, upgrade, ha
07	firstboot-deploy-otv-ng.pl, upgrade, non ha
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Le ultime tre cifre del codice di errore indicano l'errore specifico del flusso di lavoro nello script:

Codice errore di distribuzione	Flusso di lavoro	Risoluzione
049	Per la rete e la convalida, lo script perl li assegnerà a breve	-
050	Generazione chiave SSH non riuscita	Riavviare la macchina virtuale primaria (VM).
053	Installazione RKE2 non riuscita	Eseguire quanto segue e riavviare la macchina virtuale primaria o ridistribuire: Sudo rke2-killall.sh (tutte le VM) Sudo rke2-uninstall.sh (tutte le VM).
054	Impostazione kubeconfig non riuscita	Ridistribuzione

055	Distribuzione del registro non riuscita	Se il pod del Registro di sistema è presente, attendere che il pod sia pronto, quindi riavviare la macchina virtuale primaria oppure ridistribuirla.
059	La distribuzione di KubeVip non è riuscita	Assicurati che l'indirizzo IP virtuale per il piano di controllo di Kubernetes e l'indirizzo IP degli strumenti ONTAP forniti durante l'implementazione appartengano alla stessa VLAN e siano indirizzi IP gratuiti. Riavviare se tutti i punti precedenti sono corretti. Altrimenti, ridistribuzione.
060	L'implementazione dell'operatore non è riuscita	Riavviare
061	Distribuzione dei servizi non riuscita	Esegui il debug di base di Kubernetes come Get pods, Get rs, Get svc e così via nello spazio dei nomi del sistema ntv per maggiori dettagli e log degli errori su /var/log/ansible-perl-errors.log e /var/log/ansible-run.log e ridistribuisce.
062	La distribuzione dei servizi strumenti ONTAP non è riuscita	Fare riferimento ai log degli errori in /var/log/ansible-perl-errors.log per ulteriori dettagli e ridistribuire.
065	L'URL della pagina Swagger non è raggiungibile	Ridistribuzione
066	I passaggi di post-implementazione per il certificato del gateway non sono riusciti	Effettuare le seguenti operazioni per recuperare/completare l'aggiornamento: * Attiva shell diagnostica. * Eseguire il comando 'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'. * Controllare i log in /var/log/post-deploy-upgrade.log.
088	La configurazione della rotazione del registro per il giornale non è riuscita	Verificare le impostazioni di rete della VM compatibili con l'host su cui è ospitata la VM. È possibile provare a eseguire la migrazione a un altro host e riavviare la macchina virtuale.
089	La modifica della proprietà del file di configurazione rotazione del registro di riepilogo non è riuscita	Riavviare la macchina virtuale principale.
096	Installa il provisioner di storage dinamico	-

108	Seeding script non riuscito	-
Riavviare il codice di errore	Flusso di lavoro	Risoluzione
067	Attesa per rke2-server scaduta.	-
101	Impossibile reimpostare la password utente Maint/Console.	-
102	Impossibile eliminare il file della password durante la reimpostazione della password utente Maint/Console.	-
103	Impossibile aggiornare la nuova password utente Maint/Console nel vault.	-
088	La configurazione della rotazione del registro per il giornale non è riuscita.	Verificare le impostazioni di rete della VM compatibili con l'host su cui è ospitata la VM. È possibile provare a eseguire la migrazione a un altro host e riavviare la macchina virtuale.
089	La modifica della proprietà del file di configurazione rotazione del registro di riepilogo non è riuscita.	Riavviare l'VM.

Configurare i tool ONTAP per VMware vSphere

Aggiungere istanze di vCenter Server agli strumenti ONTAP

Aggiungi le istanze di vCenter Server ai tool ONTAP per VMware vSphere per configurare, gestire e proteggere i datastore virtuali nel tuo ambiente vCenter Server. Quando si aggiungono più istanze di vCenter Server, sono richiesti certificati CA personalizzati per la comunicazione sicura tra gli strumenti ONTAP e ciascun vCenter Server.

A proposito di questa attività

Gli strumenti ONTAP si integrano con vCenter Server per eseguire attività di archiviazione come provisioning, snapshot e protezione dei dati direttamente dal client 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. Ad 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 consiglia di distribuire vCenter Server utilizzando il suo fully qualified domain name (FQDN) e di assicurarsi 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.

Fasi

1. Apri un browser web e vai all'URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **vCenters > Add** per integrare le istanze di vCenter Server. Fornisci l'indirizzo IP vCenter o il

nome host, il nome utente, la password e i dettagli della porta.

4. Nelle opzioni avanzate, è possibile recuperare automaticamente il certificato di vCenter Server (autorizzarlo) oppure caricarlo manualmente.



Non occorre un account di amministratore per aggiungere istanze vCenter agli strumenti ONTAP. È possibile creare un ruolo personalizzato senza l'account admin con autorizzazioni limitate. Per ulteriori informazioni, fare riferimento alla ["USA vCenter Server RBAC con i tool ONTAP per VMware vSphere 10"](#) sezione.

L'aggiunta di un'istanza di vCenter Server agli strumenti ONTAP attiva automaticamente le seguenti azioni:

- Gli strumenti ONTAP registrano il plug-in del client vCenter come plug-in remoto.
- All'istanza di vCenter Server vengono applicate le Privileges personalizzate per i plug-in e le API.
- Per gestire gli utenti vengono creati ruoli personalizzati.
- Il plug-in viene visualizzato come collegamento nell'interfaccia utente di vSphere.

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

Utilizzare gli ONTAP tools for VMware vSphere per registrare il provider VASA con un'istanza di vCenter Server. Ciò consente la gestione basata su policy di storage, il supporto vVols e l'integrazione con appliance VMware Live Site Recovery su sistemi ONTAP .

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

Fasi

1. Accedere al client vSphere.
2. Selezionare **tasti di scelta rapida > NetApp ONTAP tools** nella sezione dei plug-in.
3. Selezionare **Impostazioni > Impostazioni provider VASA**. Gli strumenti ONTAP visualizzano lo stato di registrazione del fornitore VASA come non registrato.
4. Selezionare il pulsante **Registra** per registrare il provider VASA.
5. Inserisci un nome e le credenziali per il fornitore VASA. Il nome utente può contenere solo lettere, numeri e caratteri di sottolineatura. Impostare la lunghezza della password tra 8 e 256 caratteri.
6. Selezionare **Registra**.
7. Dopo una registrazione riuscita e l'aggiornamento della pagina, gli strumenti ONTAP visualizzano lo stato, il nome e la versione del provider VASA registrato.

Cosa succederà

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

Fasi

1. Accedere all'istanza di vCenter Server.
2. Accedere con le credenziali di amministratore.
3. Selezionare **Storage Providers > Configure**. Verificare che il provider VASA incorporato sia elencato

correttamente.

Installare il plug-in NFS VAAI utilizzando gli strumenti ONTAP

Il plug-in NFS vStorage API for Array Integration (NFS VAAI) collega VMware vSphere agli array di archiviazione NFS. Utilizzare gli ONTAP tools for VMware vSphere per installare il plug-in VAAI. Ciò consente all'array di storage NFS di gestire determinate operazioni di storage al posto degli host ESXi.

Prima di iniziare

- Scaricare il "[Plug-in NetApp NFS per VMware VAAI](#)" pacchetto di installazione.
- Assicurarsi di disporre dell'host ESXi e della patch più recente di vSphere 7.0U3 o versioni successive e di ONTAP 9.14.1 o versioni successive.
- Montare un datastore NFS.

Fasi

1. Accedere al client vSphere.
2. Selezionare **tasti di scelta rapida > NetApp ONTAP tools** nella sezione dei plug-in.
3. Selezionare **Impostazioni > NFS VAAI Tools**.
4. Se hai già caricato il plug-in VAAI su vCenter Server, seleziona **Modifica in Versione esistente**. In caso contrario, seleziona **Carica**.
5. Sfogliare e selezionare il `.vib` file e selezionare **carica** per caricare il file negli strumenti ONTAP.
6. Selezionare **Installa su host ESXi**, selezionare l'host ESXi su cui si desidera installare il plug-in NFS VAAI, quindi selezionare **Installa**.

vSphere Web Client mostra solo gli host ESXi che possono installare il plug-in. È possibile monitorare l'avanzamento dell'installazione nella sezione Attività recenti.

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

Dopo aver riavviato l'host ESXi, gli ONTAP tools for VMware vSphere rilevano e abilitano automaticamente il plug-in NFS VAAI.

Quali sono le prossime novità?

Dopo aver installato il plug-in NFS VAAI e riavviato l'host ESXi, configurare i criteri di esportazione NFS per l'offload della copia VAAI. Assicurarsi che le norme sulla politica di esportazione soddisfino questi requisiti:

- Il volume ONTAP pertinente consente 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 maggiori informazioni, fare riferimento a "[Configura le policy di esportazione NFS corrette per l'offload delle copie VAAI](#)" Articolo della Knowledge Base.

Informazioni correlate

["Supporto per VMware vStorage su NFS"](#)

"Attivare o disattivare NFSv4.0"

"Supporto ONTAP per NFSv4.2"

Configurare le impostazioni dell'host ESXi negli ONTAP tools

La configurazione delle impostazioni multipath e timeout del server ESXi aiuta a mantenere la disponibilità e l'integrità dei dati. Abilita il failover automatico su un percorso di archiviazione di backup se il percorso primario non è più disponibile.

Configurare le impostazioni di multipath e timeout del server ESXi

I tool ONTAP per VMware vSphere controllano e impostano le impostazioni di multipath host ESXi e le impostazioni di timeout HBA che funzionano meglio con i sistemi storage NetApp.

A proposito di questa attività

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

Fasi

1. Dalla home page del client Web VMware vSphere, selezionare **host e cluster**.
2. Nella pagina dei collegamenti del client Web VMware vSphere, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Andare alla scheda **ESXi host compliance** nella panoramica (dashboard) degli strumenti ONTAP per il plug-in VMware vSphere.
4. Selezionare il collegamento **Applica impostazioni consigliate**.
5. Nella finestra **Applica impostazioni host consigliate**, seleziona gli host che desideri aggiornare per utilizzare le impostazioni consigliate NetApp e seleziona **Avanti**.



È possibile espandere l'host ESXi per visualizzare i valori correnti.

6. Nella pagina delle impostazioni, selezionare i valori consigliati secondo necessità.
7. Nel pannello di riepilogo, controllare i valori e selezionare **fine**. È possibile tenere traccia dell'avanzamento nel riquadro attività recenti.

Impostare i valori dell'host ESXi

Utilizzare gli 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 .

È possibile impostare i seguenti valori su un host ESXi:

Impostazioni adattatore HBA/CNA

Imposta i seguenti parametri sui valori predefiniti:

- Disk.QFullSampleSize

- Disk.QFullThreshold
- Timeout HBA FC Emulex
- Timeout HBA FC QLogic

Impostazioni MPIO

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

Per ambienti ad alte prestazioni o quando si esegue il test con un singolo datastore LUN, regolare l'impostazione del bilanciamento del carico del criterio di selezione del percorso (PSP) round-robin (VMW_PSP_RR) 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	Impostare 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

Utilizzare questa sezione per configurare i ruoli utente e i privilegi ONTAP per i backend di archiviazione con gli ONTAP tools for VMware vSphere e ONTAP System Manager. È possibile assegnare ruoli utilizzando i file JSON forniti, creare manualmente utenti e ruoli e applicare i privilegi minimi richiesti per gli account non amministratori.

Prima di iniziare

- Scaricare il file ONTAP Privileges dagli ONTAP tools for VMware vSphere utilizzando https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip. Dopo aver scaricato il file zip, troverai due file JSON. Utilizzare il file JSON specifico di ASA r2 durante la configurazione di un sistema ASA r2.



È possibile creare utenti a livello di cluster o direttamente a livello di macchine virtuali di archiviazione (SVM). Se non si utilizza il file user_roles.json, assicurarsi che l'utente disponga delle autorizzazioni SVM minime richieste.

- Accedi con privilegi di amministratore per il backend di archiviazione.

Fasi

1. Estrarre il file `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip` scaricato.
2. Accedere a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster del cluster.
3. Accedi al cluster con privilegi di amministratore. Per configurare un utente:
 - a. Per configurare un utente degli strumenti ONTAP del cluster, selezionare il riquadro **Cluster > Impostazioni > Utenti e ruoli**.
 - b. Per configurare un utente degli strumenti SVM ONTAP , selezionare il riquadro **Storage SVM > Impostazioni > Utenti e ruoli**.
 - c. Selezionare **Aggiungi** in utenti.
 - d. Nella finestra di dialogo **Aggiungi utente**, selezionare **prodotti di virtualizzazione**.
 - e. **Sfoggia** per selezionare e caricare il file JSON Privileges ONTAP . Per i sistemi non ASA r2, selezionare il file `users_roles.json` e per i sistemi ASA r2, selezionare il file `users_roles_ASAr2.json`.

Gli strumenti ONTAP popolano automaticamente il campo Prodotto.

- f. Selezionare la funzionalità del prodotto come **VSC, VASA Provider e SRA** dal menu a discesa.

Gli strumenti ONTAP popolano automaticamente il campo **Ruolo** in base alla funzionalità del prodotto selezionata.

- g. Immettere il nome utente e la password richiesti.
- h. Selezionare i privilegi (Discovery, Create Storage, Edit Storage, Destroy Storage, NAS/SAN Role) di cui l'utente ha bisogno, quindi selezionare **Aggiungi**.

Gli strumenti ONTAP aggiungono il nuovo ruolo e utente. Puoi visualizzare i privilegi relativi al ruolo configurato.

Requisiti di mappatura degli aggregati delle SVM

Durante il provisioning degli archivi dati utilizzando le credenziali utente SVM, gli ONTAP tools for VMware vSphere creano volumi sull'aggregato specificato nell'API POST degli archivi dati. ONTAP impedisce agli utenti SVM di creare volumi su aggregati non mappati sull'SVM. Prima di creare i volumi, mappare l'SVM sugli aggregati richiesti utilizzando l'API REST o la CLI ONTAP .

API REST:

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

CLI ONTAP:

```

still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver          Aggregate          State          Size Type          SnapLock
Type-----
-----svm_test          still15_vsim_ucs630f_aggr1
online          10.11GB vmdisk  non-snaplock

```

Creare manualmente un utente e un ruolo ONTAP

Creare manualmente utenti e ruoli senza il file JSON.

1. Accedere a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster del cluster.
2. Accedere al cluster con admin Privileges.
 - a. Per configurare i ruoli degli strumenti ONTAP del cluster, selezionare **Cluster > Impostazioni > Utenti e ruoli**.
 - b. Per configurare i ruoli degli strumenti SVM ONTAP del cluster, selezionare **Storage SVM > Impostazioni > Utenti e ruoli**.
3. Crea ruoli:
 - a. Selezionare **Aggiungi** nella tabella **ruoli**.
 - b. Immettere i dettagli **nome ruolo** e **attributi ruolo**.

Aggiungere il **Percorso API REST** e scegliere l'accesso dall'elenco a discesa.
 - c. Aggiungere tutte le API necessarie e salvare le modifiche.
4. Crea utenti:
 - a. Selezionare **Aggiungi** nella tabella **utenti**.
 - b. Nella finestra di dialogo **Aggiungi utente**, selezionare **System Manager**.
 - c. Immettere il **Nome utente**.
 - d. Selezionare **ruolo** dalle opzioni create nel passaggio **Crea ruoli** riportato sopra.
 - e. Immettere le applicazioni a cui assegnare l'accesso e il metodo di autenticazione. ONTAPI e HTTP sono le applicazioni richieste e il tipo di autenticazione è **Password**.
 - f. Impostare **Password per l'utente** e **Salva** l'utente.

Elenco dei privilegi minimi richiesti per gli utenti cluster con ambito globale non amministratori

Questa pagina elenca i privilegi minimi richiesti per un utente del cluster con ambito globale non amministratore senza un file JSON. Se un cluster si trova nell'ambito locale, utilizzare il file JSON per creare gli utenti, poiché gli ONTAP tools for VMware vSphere necessitano di più dei semplici privilegi di lettura per il provisioning su ONTAP.

È possibile accedere alle funzionalità tramite API:

API	Livello di accesso	Utilizzato per
/api/cluster	Sola lettura	Rilevamento della configurazione del cluster

/api/cluster/licenze/licenze	Sola lettura	Controllo della licenza per licenze specifiche del protocollo
/api/cluster/nodi	Sola lettura	Rilevamento del tipo di piattaforma
/api/security/accounts	Sola lettura	Scoperta dei privilegi
/api/security/ruoli	Sola lettura	Scoperta dei privilegi
/api/storage/aggregati	Sola lettura	Controllo dello spazio aggregato durante il provisioning del datastore/volume
/api/storage/cluster	Sola lettura	Per ottenere i dati sullo spazio e sull'efficienza a livello di cluster
/api/storage/dischi	Sola lettura	Per ottenere i dischi associati in un aggregato
/api/storage/qos/policy	Lettura/creazione/Modifica	Gestione delle policy QoS e VM
/api/svm/svm	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 di gestione LIF è cluster/SVM
/api/storage/availability-zones	Sola lettura	Scoperta SAZ. Applicabile alla versione ONTAP 9.16.1 e successive e ai sistemi ASA r2.
/api/cluster/metrocluster	Sola lettura	Ottiene lo stato e i dettagli di configurazione MetroCluster .

Crea tool ONTAP per l'utente con ambito cluster basato su API VMware vSphere ONTAP



Per le operazioni PATCH e il rollback automatico sui datastore sono richiesti privilegi di individuazione, creazione, modifica ed eliminazione. La mancanza di autorizzazioni potrebbe causare problemi di flusso di lavoro e di pulizia.

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

Per creare un utente soggetto all'ambito del cluster con tutti gli Privileges 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 ONTAP versione 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 su ONTAP versione 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 tool ONTAP per l'utente con ambito SVM basato su API di VMware vSphere ONTAP

Eeguire i seguenti comandi per creare un utente con ambito SVM dotato di 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 ONTAP versione 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 comando seguente:

```

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_stil60-cluster_
```

Eeguire 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_stil60-cluster
```

Aggiorna i tool ONTAP per VMware vSphere 10,1 a un utente 10,3

Per i tool ONTAP per gli utenti di VMware vSphere 10,1 con un utente impostato su cluster creato utilizzando il file JSON, utilizzare i seguenti comandi dell'interfaccia della riga di comando di ONTAP con l'Privileges dell'amministratore utente per eseguire l'aggiornamento alla release 10,3.

Per le funzionalità del prodotto:

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

Privileges 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 i tool ONTAP per l'utente di VMware vSphere 10,1 con un utente con ambito SVM creato utilizzando il file json, utilizza i comandi dell'interfaccia della riga di comando di ONTAP con l'utente admin Privileges per eseguire l'upgrade alla release 10,3.

Privileges 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, aggiungere 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 i tool ONTAP per VMware vSphere 10,3 a un utente 10,4

A partire da ONTAP 9.16.1, aggiornare gli ONTAP tools for VMware vSphere 10.3 alla versione 10.4.

Per i tool ONTAP per l'utente VMware vSphere 10,3 con un utente sottoposto a cluster creato utilizzando il file JSON e ONTAP versione 9.16.1 o successiva, utilizza il comando CLI ONTAP con admin user Privileges per eseguire l'upgrade alla release 10,4.

Per le funzionalità del prodotto:

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

Privileges cluster:

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

Aggiungi un backend di storage a ONTAP tools

Utilizza gli ONTAP tools for VMware vSphere per aggiungere e gestire i backend di storage per i tuoi host ESXi. È possibile integrare cluster o SVM, abilitare il supporto MetroCluster e convalidare i certificati per una connettività sicura. È possibile configurare i backend di archiviazione utilizzando 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 archiviazione in locale, utilizzare le credenziali del cluster o SVM nell'interfaccia degli strumenti ONTAP . I backend di archiviazione locale sono disponibili solo per il vCenter Server selezionato. Gli strumenti ONTAP mappano le SVM sul vCenter Server per la gestione dei datastore vVols o VMFS. Per i datastore VMFS e i flussi di lavoro SRA, è possibile utilizzare le credenziali SVM senza mappare un cluster a livello globale.

Per aggiungere un backend di archiviazione globale, utilizzare le credenziali del cluster ONTAP in ONTAP Tools Manager. I backend di archiviazione globali consentono ai flussi di lavoro di individuare e identificare le risorse del cluster necessarie per la gestione vVol. Negli ambienti multitenant, è possibile aggiungere un

utente SVM localmente per gestire i datastore vVols .

Se il supporto MetroCluster è abilitato in ONTAP, integrare sia i cluster di origine che quelli di destinazione come backend di archiviazione locali o globali.

Prima di iniziare

Verificare che il certificato includa un campo Subject Alternative Name (SAN) valido. I sistemi ONTAP utilizzano il campo SAN per identificare i LIF di gestione del cluster e dell'SVM.

Utilizzo di ONTAP Tools Manager



In un setup multi-tenant, puoi aggiungere un cluster backend storage a livello globale e una SVM locale per utilizzare le credenziali utente della SVM.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **backend di archiviazione** dalla barra laterale.
4. Aggiungere il backend di archiviazione e fornire l'indirizzo IP del server o i dettagli FQDN, nome utente e password.



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

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



Se necessario, è possibile disabilitare la convalida del nome alternativo del soggetto (SAN) dalla console di manutenzione. Per le istruzioni, vedere ["Cambia il flag di convalida del certificato"](#).

6. Se il backend di archiviazione aggiunto fa parte di una configurazione MetroCluster, ONTAP Tools Manager mostra un messaggio pop-up per aggiungere il cluster peered. Selezionare **Aggiungi** e fornire i dettagli per il backend di archiviazione peer MetroCluster.



Dopo che il sistema ONTAP ha eseguito uno switchover e uno switchback, eseguire manualmente la scoperta degli strumenti ONTAP.

Utilizzo dell'interfaccia utente del client vSphere



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

1. Accedere al client vSphere.
2. Nella pagina Collegamenti, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Selezionare **backend di archiviazione** dalla barra laterale.
4. Aggiungere il backend di archiviazione e fornire l'indirizzo IP del server, il nome utente, la password e i dettagli della porta.



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

5. Recupera automaticamente i certificati del cluster ONTAP e autorizza il certificato oppure caricalo

manualmente navigando fino alla sua posizione.

6. Se il backend di archiviazione aggiunto fa parte della configurazione MetroCluster , gli strumenti ONTAP visualizzano la schermata **Aggiungi peer MetroCluster ***. **Selezionare *Aggiungi peer** per aggiungere il backend di archiviazione peer.



Dopo che il sistema ONTAP ha eseguito uno switchover e uno switchback, eseguire manualmente la scoperta degli strumenti ONTAP .

Cosa succederà?

Gli strumenti ONTAP aggiornano l'elenco per mostrare il nuovo backend di archiviazione.

Gli strumenti ONTAP elencano il backend di archiviazione appena aggiunto nella pagina **Backend di archiviazione**. Se un certificato scade entro 30 giorni o meno, gli strumenti ONTAP mostrano un avviso nella colonna della data di scadenza del certificato. Dopo la scadenza, gli strumenti ONTAP contrassegnano il backend di archiviazione come sconosciuto perché non riesce a connettersi al sistema di archiviazione.

Informazioni correlate

["Configurazione dei cluster in una configurazione MetroCluster"](#)

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

Associare un backend di archiviazione a un'istanza di vCenter Server per consentire l'accesso a tutte le istanze di vCenter Server. Per la configurazione MetroCluster , quando si associa un cluster backend di archiviazione, assicurarsi di associare anche il suo cluster peer al vCenter Server.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Seleziona vCenter dalla barra laterale.
4. Selezionare le ellissi verticali accanto all'istanza di vCenter Server che si desidera connettere ai backend di storage.
5. Dal menu a discesa, seleziona il backend di archiviazione che desideri 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 al criterio di esportazione, a meno che non si configuri l'accesso alla rete. È possibile modificare i criteri di esportazione per consentire l'accesso solo da indirizzi IP specifici. Se un host ESXi escluso tenta un'operazione di montaggio, l'operazione fallisce.

Fasi

1. Accedere al client vSphere.
2. Selezionare **NetApp ONTAP tools** nella pagina dei collegamenti nella sezione dei plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Impostazioni > Gestisci accesso alla rete > Modifica**.

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

4. Selezionare **Salva**.

Creare un datastore in ONTAP tools

Quando si crea un datastore a livello di cluster host, gli strumenti ONTAP lo montano su tutti gli host di destinazione e abilitano l'azione solo se si dispone dei privilegi richiesti.

Interoperabilità tra datastore nativi con vCenter Server e datastore gestiti da strumenti ONTAP

A partire dagli ONTAP tools for VMware vSphere 10.4, gli strumenti ONTAP creano igroup annidati per gli archivi dati, con igroup padre specifici per gli archivi dati e igroup figlio mappati agli host. È possibile creare igroup piatti da ONTAP System Manager e utilizzarli per creare datastore VMFS senza ricorrere agli strumenti ONTAP . Fare riferimento a "[Gestire gli iniziatori SAN e gli igroup](#)" per maggiori informazioni.

Dopo aver integrato l'archiviazione ed eseguito la scoperta del datastore, gli strumenti ONTAP trasformano gli igroup piatti nei datastore VMFS in igroup annidati. Non è possibile utilizzare igroup piatti precedenti per creare nuovi datastore. Utilizzare l'interfaccia degli strumenti ONTAP o l'API REST per riutilizzare gli igroup annidati.

Creare un datastore vVol

A partire dagli ONTAP tools for VMware vSphere 10.3, è possibile creare un datastore vVols su sistemi ASA r2 con efficienza di spazio come thin.vVol. Il provider VASA crea un contenitore e gli endpoint del protocollo desiderati durante la creazione del datastore vVol. Il provider VASA non assegna alcun volume di supporto a questo contenitore.

Prima di iniziare

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

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP * > *Crea datastore**.
3. Selezionare vVol **tipo di datastore**.
4. Immettere le informazioni **Nome datastore** e **protocollo**.



Il sistema ASA R2 supporta i protocolli iSCSI e FC per i vVol.

5. Seleziona la macchina virtuale storage in cui desideri creare il datastore.
6. In Opzioni avanzate:
 - Se selezioni **Criterio di esportazione personalizzato**, assicurati di eseguire l'individuazione in vCenter per tutti gli oggetti. Si consiglia di non utilizzare questa opzione.
 - È possibile selezionare il nome **Custom Initiator group** per i protocolli iSCSI e FC.



Nel sistema di archiviazione ASA r2 di tipo SVM, le unità di archiviazione (LUN/namespace) non vengono create perché l'archivio dati è solo un contenitore logico.

7. Nel riquadro **attributi archiviazione** è possibile creare nuovi volumi o utilizzare i volumi esistenti. Tuttavia, non è possibile combinare questi due tipi di volumi per creare un datastore vVol.

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

8. Controllare la selezione nel riquadro **Riepilogo** e selezionare **fine**.

Creare 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.

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP * > *Crea datastore**.

3. Selezionare NFS nel campo **tipo datastore**.
4. Immettere il nome del datastore, le dimensioni e le informazioni sul protocollo nel riquadro **Nome e protocollo**. Selezionare **Datastore cluster** e **autenticazione Kerberos** nelle opzioni avanzate.



L'autenticazione Kerberos è disponibile solo quando è selezionato il protocollo NFS 4,1.

5. Selezionare **piattaforma** e **Storage VM** nel riquadro **Storage**.
6. Se si seleziona **Criterio di esportazione personalizzato** nelle opzioni avanzate, eseguire l'individuazione in vCenter per tutti gli oggetti. Si consiglia di non utilizzare questa opzione.



Non è possibile creare un datastore NFS utilizzando il criterio del volume predefinito o root dell'SVM.

- Nelle opzioni avanzate, il pulsante di commutazione **asimmetrico** è visibile solo se nel menu a discesa della piattaforma sono selezionate prestazioni o capacità.
 - Selezionando l'opzione **Qualsiasi** nel menu a discesa della piattaforma, è possibile visualizzare tutte le SVM in vCenter. La piattaforma e la bandiera asimmetrica non influiscono sulla visibilità.
7. Selezionare l'aggregato per la creazione del volume nel riquadro **attributi archiviazione**. Nelle opzioni avanzate, scegliere **Riserva spazio** e **attiva QoS** come richiesto.
 8. Controllare le selezioni nel riquadro **Riepilogo** e selezionare **fine**.

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

Creare un datastore VMFS

VMFS è un file system clusterizzato 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.

In un cluster protetto:

- È possibile creare solo datastore VMFS. L'aggiunta di un datastore VMFS a un cluster protetto ne determina automaticamente la protezione.
- Non è possibile creare un datastore in un data center con uno o più cluster host protetti.
- Non è possibile creare un datastore su un host ESXi se il cluster host padre è protetto da una "policy di failover duplex automatizzato" (configurazione uniforme o non uniforme).
- È possibile creare un datastore VMFS solo su un host ESXi protetto da una relazione asincrona. Non è possibile creare e montare un datastore su un host ESXi che fa parte di un cluster host protetto dal criterio "Automated failover Duplex".

Prima di iniziare

- Abilitare servizi e LIF per ogni protocollo da parte dello storage ONTAP.
- Mappare la SVM per l'aggregato dell'utente SVM nel sistema storage ASA R2.
- Configurare l'host ESXi se si utilizza il protocollo NVMe/TCP:
 - a. Esaminare ["Guida alla compatibilità VMware"](#)



VMware vSphere 7,0 U3 e le versioni successive supportano il protocollo NVMe/TCP. Tuttavia, si consiglia VMware vSphere 8,0 e versioni successive.

- b. Verificare se il fornitore della scheda di interfaccia di rete (NIC) supporta la NIC ESXi con il protocollo NVMe/TCP.
 - c. Configurare la scheda di rete ESXi per NVMe/TCP in base alle specifiche del fornitore della scheda di rete.
 - d. Quando si utilizza VMware vSphere 7 release, seguire le istruzioni sul sito VMware "[Configurare il binding VMkernel per NVMe over TCP Adapter](#)" per configurare il binding della porta NVMe/TCP. Quando si utilizza VMware vSphere 8 release, seguire "[Configurazione di NVMe su TCP su ESXi](#)", per configurare il binding della porta NVMe/TCP.
 - e. Per VMware vSphere 7 release, seguire le istruzioni a pagina "[Abilita gli adattatori software NVMe su RDMA o NVMe su TCP](#)" per configurare gli adattatori software NVMe/TCP. Per la release VMware vSphere 8, seguire "[Aggiunta di adattatori software NVMe su RDMA o NVMe su TCP](#)" questa procedura per configurare gli adattatori software NVMe/TCP.
 - f. Eseguire "[Rilevamento di host e sistemi storage](#)" l'azione sull'host ESXi. Per ulteriori informazioni, fare riferimento a "[Come configurare NVMe/TCP con vSphere 8,0 Update 1 e ONTAP 9.13,1 per datastore VMFS](#)".
- Se si utilizza il protocollo NVMe/FC, procedere come segue per configurare l'host ESXi:
 - a. Se non è già abilitato, abilitare NVMe over Fabrics (NVMe-of) sugli host ESXi.
 - b. Zoning SCSI completo.
 - c. Verificare che gli host ESXi e il sistema ONTAP siano connessi a un livello fisico e logico.

Per configurare una SVM ONTAP per il protocollo FC, fare riferimento alla "[Configurare una SVM per FC](#)".

Per ulteriori informazioni sull'utilizzo del protocollo NVMe/FC con VMware vSphere 8,0, consultare "[Configurazione host NVMe-of per ESXi 8.x con ONTAP](#)".

Per ulteriori informazioni sull'utilizzo di NVMe/FC con VMware vSphere 7,0, consultare "[Guida alla configurazione degli host NVMe/FC di ONTAP](#)" e "[TR-4684](#)".

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP** * > ***Crea datastore**.
3. Selezionare il tipo di datastore VMFS.
4. Immettere il nome del datastore, le dimensioni e le informazioni sul protocollo nel riquadro **Nome e protocollo**. Per aggiungere il nuovo datastore a un cluster VMFS esistente, selezionare il cluster del datastore in Opzioni avanzate.
5. Selezionare Storage VM nel riquadro **Storage**. Specificare il **nome gruppo iniziatore personalizzato** nella sezione **Opzioni avanzate** secondo necessità. È possibile scegliere un igroup esistente per il datastore o creare un nuovo igroup con un nome personalizzato.

Quando si seleziona il protocollo NVMe/FC o NVMe/TCP, viene creato un nuovo sottosistema di namespace che viene utilizzato per la mappatura degli spazi dei nomi. Gli strumenti ONTAP creano il sottosistema dello spazio dei nomi utilizzando il nome generato automaticamente che include il nome del datastore. È possibile rinominare il sottosistema dello spazio dei nomi nel campo **nome del sottosistema dello spazio dei nomi personalizzato** nelle opzioni avanzate del riquadro **Archiviazione**.

6. Dal riquadro **attributi di archiviazione**:

a. Selezionare **aggregate** dalle opzioni a discesa.



Per i sistemi di archiviazione ASA r2, l'opzione **Aggregate** non viene visualizzata perché l'archiviazione è disaggregata. Quando si sceglie un sistema di storage ASA r2 di tipo SVM, la pagina degli attributi di storage mostra le opzioni per abilitare la 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 * di performance per i sistemi storage ASA R2 con SVM a 12 nodi, che è un cluster eterogeneo. Questa opzione non è disponibile se la SVM selezionata è un cluster omogeneo o utilizza un utente SVM.

'Qualsiasi' è il valore predefinito del livello di servizio delle prestazioni (PSL). Questa impostazione crea l'unità di memorizzazione utilizzando l'algoritmo di posizionamento bilanciato ONTAP. Tuttavia, è possibile selezionare l'opzione prestazioni o estreme in base alle esigenze.

d. Selezionare **Usa volume esistente, attiva QoS** come richiesto e fornire i dettagli.



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



Non è possibile utilizzare il volume esistente per creare un datastore VMFS con protocollo NVMe/FC o NVMe/TCP. Creare un nuovo volume per il datastore VMFS.

7. Rivedere i dettagli del datastore nel riquadro **Riepilogo** e selezionare **fine**.



Se si crea il datastore su un cluster protetto, viene visualizzato un messaggio di sola lettura: "Il datastore viene montato su un cluster protetto".

Risultato

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

Protezione di datastore e macchine virtuali

Proteggere un cluster host negli ONTAP tools

I tool ONTAP per VMware vSphere gestiscono la protezione dei cluster di host. Tutti i datastore appartenenti alla SVM selezionata e montati su uno o più host del cluster sono protetti in un cluster di host.

Prima di iniziare

Prima di proteggere un cluster host, assicurati di soddisfare questi requisiti:

- Il cluster host contiene solo datastore provenienti da una singola SVM.
- Gli archivi dati sul cluster host non vengono montati su host esterni al cluster.
- I datastore montati sul cluster host sono datastore VMFS con protocollo iSCSI o FC. Non è possibile utilizzare datastore vVols, NFS o VMFS con i 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.

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Nella finestra di protezione del cluster, il sistema compila automaticamente i dettagli relativi al tipo di datastore e alla macchina virtuale (VM) di archiviazione di origine. Selezionare il collegamento datastore per visualizzare i datastore protetti.
4. Selezionare **Aggiungi relazione**.
5. Nella finestra **Aggiungi relazione SnapMirror**, selezionare la VM di archiviazione di destinazione* e il tipo **criterio**.

Il tipo di criterio può essere asincrono o AutomatedFailOverDuplex.

Quando Aggiungi la relazione SnapMirror come policy di tipo AutomatedFailOverDuplex, devi aggiungere la VM storage di destinazione come backend dello storage al medesimo vCenter in cui vengono implementati i tool ONTAP per VMware vSphere.

Nel tipo di policy AutomatedFailOverDuplex sono presenti configurazioni host uniformi e non uniformi. Quando si seleziona il pulsante di attivazione/disattivazione **configurazione host uniforme**, la configurazione del gruppo di iniziatori host viene replicata implicitamente sul sito di destinazione. Per ulteriori informazioni, fare riferimento a "[Concetti e termini chiave](#)".

6. Se si sceglie di avere una configurazione host non uniforme, selezionare l'accesso host (origine/destinazione) per ogni host all'interno di quel cluster.
7. Selezionare **Aggiungi**.
8. È possibile modificare la protezione del cluster host utilizzando l'operazione **Modifica protezione del cluster host**. È possibile modificare o eliminare le relazioni utilizzando le opzioni del menu con i puntini di

sospensione.

9. Selezionare il pulsante **Proteggi**.

Il sistema crea un'attività vCenter con i dettagli dell'ID processo e ne mostra l'avanzamento nel pannello delle attività recenti. Si tratta di 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, andare su **Strumenti NetApp ONTAP * > *Protezione > Relazioni tra cluster host**. Selezionare un gruppo di coerenza per visualizzarne la capacità, i datastore associati e i gruppi di coerenza figlio.



Se è necessario rimuovere la protezione entro un'ora dalla creazione, eseguire prima l'individuazione dello storage.

Informazioni correlate

["Cluster di archiviazione metro VMware vSphere \(vMSC\)"](#)

Proteggere utilizzando la protezione SRA

Configurare SRA negli ONTAP tools per proteggere i datastore

I tool ONTAP per VMware vSphere offrono la possibilità di abilitare la funzionalità SRA per la configurazione del disaster recovery.

Prima di iniziare

- È necessario aver configurato l'istanza di vCenter Server e l'host ESXi configurato.
- Devi aver implementato tool ONTAP per VMware vSphere.
- Il `.tar.gz` file dell'adattatore SRA dovrebbe essere stato scaricato dal ["Sito di supporto NetApp"](#).
- Prima di eseguire i flussi di lavoro SRA, è necessario disporre delle stesse pianificazioni SnapMirror personalizzate sui cluster ONTAP di origine e di destinazione.
- ["Abilita i tool ONTAP per i servizi VMware vSphere"](#) per abilitare la funzionalità SRA.

Fasi

1. Accedere all'interfaccia di gestione dell'appliance VMware Live Site Recovery utilizzando l'URL: `https://:<srm_ip>:5480`, Quindi accedere a Storage Replication Adapter nell'interfaccia di gestione dell'appliance VMware Live Site Recovery.
2. Selezionare **Nuova scheda**.
3. Caricare il programma di installazione `.tar.gz` per il plug-in SRA in VMware Live Site Recovery.
4. Eseguire nuovamente la scansione delle schede di rete per verificare che i dettagli siano aggiornati nella pagina VMware Live Site Recovery Storage Replication Adapters (schede di replica storage di VMware Live Site Recovery).



Dopo un failover, azioni quali espansione, montaggio ed eliminazione potrebbero non essere disponibili per i datastore. Eseguire la scoperta del datastore per aggiornare e visualizzare le azioni appropriate del menu contestuale.



Dopo ogni operazione di riprotezione, è necessario eseguire l'individuazione dello storage su entrambi i siti.

In una nuova configurazione con protezione SRA, eseguire 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 SnapMirror Active Sync in cui la sorgente SnapMirror cambia nel sito B per Automated Failover Duplex e Asynchronous SnapMirror, eseguire un failover di prova tra i siti B e C. Saltare questo passaggio potrebbe comportare il fallimento dell'operazione di riprotezione.

Informazioni correlate

["Configurare il disaster recovery per i datastore NFS utilizzando VMware Site Recovery Manager"](#)

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

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

Configurare SRA per gli ambienti SAN

Prima di iniziare

Nel sito protetto e nel sito di ripristino devono essere installati i seguenti programmi:

- VMware Live Site Recovery: il sito VMware fornisce la documentazione di installazione per VMware Live Site Recovery.

["Informazioni su VMware Live Site Recovery"](#)

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

Fasi

1. Verificare che gli host ESXi primari siano connessi alle LUN nel sistema di storage primario sul sito protetto.
2. Verificare che i LUN si trovino in igroups che dispongono di `ostype` Opzione impostata su *VMware* sul sistema di storage primario.
3. Verificare che gli host ESXi nel sito di ripristino dispongano di una connettività iSCSI e Fibre Channel appropriata alla macchina virtuale di archiviazione (SVM). Gli host ESXi del sito secondario devono avere accesso allo storage del sito secondario, mentre gli host ESXi del sito primario devono avere accesso allo storage del sito primario.

Per farlo, verificare che gli host ESXi abbiano LUN locali connessi alla SVM o al `iscsi show initiators` Sulle SVM.

Controllare l'accesso LUN per i LUN mappati nell'host ESXi per verificare la connettività iSCSI.

Configurare SRA per gli ambienti NAS

Prima di iniziare

Nel sito protetto e nel sito di ripristino devono essere installati i seguenti programmi:

- VMware Live Site Recovery: la documentazione sull'installazione di VMware Live Site Recovery è disponibile sul sito VMware - ["Informazioni su VMware Live Site Recovery"](#)

- SRA: installare l'adattatore su VMware Live Site Recovery e sul server SRA.

Fasi

1. Verificare che gli archivi dati 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 macchina virtuale di storage (SVM).
3. Verificare che nel campo **Indirizzi NFS** siano specificati indirizzi validi, come l'indirizzo IP o il nome di dominio completo (FQDN) 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 nel campo **Indirizzi NFS**.
4. Utilizzare `ping` Su ciascun host ESXi nel sito di ripristino per verificare che l'host disponga di una porta VMkernel in grado di accedere agli indirizzi IP utilizzati per le esportazioni NFS dalla SVM.

Configurare SRA in ONTAP tools per ambienti altamente scalabili

È necessario configurare gli intervalli di timeout dello storage in base alle impostazioni consigliate per Storage Replication Adapter (SRA) in modo da garantire prestazioni ottimali in ambienti altamente scalabili.

Impostazioni del provider di storage

È necessario impostare i seguenti valori di timeout su VMware Live Site Recovery per l'ambiente scalato:

Impostazioni avanzate	Valori di timeout
<code>StorageProvider.resignatureTimeout</code>	Aumentare il valore dell'impostazione da 900 secondi a 12000 secondi.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Impostare un valore alto (ad esempio: 99999)

Attivare anche il `StorageProvider.autoResignatureMode` opzione.

Per ulteriori informazioni sulla modifica delle impostazioni del provider di archiviazione, fare riferimento alla ["Modificare le impostazioni del provider di storage"](#).

Impostazioni di storage

Quando si preme un timeout, aumentare i valori di `storage.commandTimeout` e `storage.maxConcurrentCommandCnt` ad 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.

Per modificare le impostazioni dei provider SAN, consultare la sezione ["Modificare le impostazioni di archiviazione"](#).

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

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

La configurazione di SRA sull'appliance VMware Live Site Recovery salva le credenziali ONTAP tools for VMware vSphere all'interno dell'appliance, consentendo la comunicazione tra VMware Live Site Recovery e SRA.

Prima di iniziare

- Scarica il file `.tar.gz` dal ["Sito di supporto NetApp"](#).
- Abilitare i servizi SRA in ONTAP Tools Manager. Per ulteriori informazioni, consulta ["Abilita i servizi"](#) sezione.
- Aggiungere vCenter Server agli strumenti ONTAP per l'appliance VMware vSphere. Per ulteriori informazioni, consulta ["Aggiungi server vCenter"](#) sezione.
- Aggiungere backend di storage agli ONTAP tools for VMware vSphere. Per ulteriori informazioni, consulta ["Aggiungere backend di archiviazione"](#) sezione.



Se è stata applicata la patch del certificato vCenter dagli strumenti ONTAP, aggiornare la configurazione vCenter nell'appliance VMware Live Site Recovery utilizzando la porta (:5480). Per le istruzioni, fare riferimento a ["Riconfigurare l'appliance Site Recovery Manager"](#).

Fasi

1. Nella schermata dell'appliance VMware Live Site Recovery, selezionare **Storage Replication Adapter > New Adapter**.
2. Caricare il file `.tar.gz` su VMware Live Site Recovery.
3. Accedere al dispositivo VMware Live Site Recovery utilizzando un account amministratore tramite un client SSH come PuTTY.
4. Passare all'utente root utilizzando il comando: `su root`
5. Esegui il comando `cd /var/log/vmware/srm` per andare alla directory del registro.
6. Nella posizione del registro, immettere il comando per ottenere l'ID Docker utilizzato da SRA: `docker ps -l`
7. Per accedere all'ID contenitore, immettere il comando: `docker exec -it -u srm <container id> sh`
8. Configurare VMware Live Site Recovery con gli ONTAP tools for VMware vSphere utilizzando il comando:
`perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Fornire la password tra virgolette singole in modo che lo script Perl tratti i caratteri speciali come parte della password e non come delimitatori.
 - È possibile impostare il nome utente e la password dell'applicazione (VASA Provider/SRA) in ONTAP Tools Manager quando si abilitano questi servizi per la prima volta. Utilizzare queste credenziali per registrare SRA con VMware Live Site Recovery.

- Per individuare il GUID di vCenter, accedere alla pagina vCenter Server in ONTAP Tools Manager dopo aver aggiunto l'istanza di vCenter. Fare riferimento a "[Aggiungi server vCenter](#)" sezione.
9. Eseguire nuovamente la scansione degli adattatori per confermare che i dettagli aggiornati siano visualizzati nella pagina Adattatori VMware Live Site Recovery Storage Replication.

Risultati Viene visualizzato un messaggio di conferma che indica che le credenziali di archiviazione sono state salvate. Ora puoi utilizzare 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 comunichi con SRA, è necessario aggiornare le credenziali SRA sul server VMware Live Site Recovery se sono state modificate le credenziali.

Prima di iniziare

È necessario aver eseguito i passaggi descritti nell'argomento "[Configurazione di SRA sull'appliance VMware Live Site Recovery](#)".

Fasi

1. Eseguire i seguenti comandi per eliminare la cartella della macchina per il ripristino dei siti live di VMware memorizzata nella cache degli strumenti ONTAP Password del nome utente:

- a. `sudo su <enter root password>`
- b. `docker ps`
- c. `docker exec -it <container_id> sh`
- d. `cd conf/`
- e. `rm -rf *`

2. Eseguire 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>` È necessario disporre di un'unica citazione relativa al valore della password.

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

Configura i siti protetti e di ripristino negli ONTAP tools

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

Quando si aggiunge un nuovo datastore, è possibile 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 volume protetto, aggiornare SnapMirror ed eseguire il discovery dello storage sia sul sito protetto che su quello di ripristino. È possibile eseguire il discovery manualmente o in base a una pianificazione per garantire che il nuovo datastore venga rilevato e protetto.

Associare siti protetti e di ripristino

È necessario associare i siti protetti e di ripristino creati utilizzando il client vSphere per consentire l'individuazione dei sistemi di storage mediante Storage Replication Adapter (SRA).



Storage Replication Adapter (SRA) supporta il fan-out con una relazione di sincronizzazione di tipo Automated Failover Duplex e una relazione asincrona SnapMirror sul gruppo di coerenza. Tuttavia, il fan-out con due SnapMirror asincroni su un gruppo di coerenza o con due SnapMirror fan-out su un volume non è supportato. Le relazioni SnapMirror di tipo Vault non sono considerate in queste restrizioni di fan-out.

Prima di iniziare

- È necessario che VMware Live Site Recovery sia installato sui siti protetti e di ripristino.
- È necessario che SRA sia installato nei siti protetti e di ripristino.

Fasi

1. Nella home page di vSphere Client, fare doppio clic sull'icona **Site Recovery** e quindi selezionare **Siti**.
2. Selezionare **oggetti > azioni > abbina siti**.
3. Nella finestra di dialogo **Associa server di Site Recovery Manager**, immettere l'indirizzo del Platform Services Controller del sito protetto, quindi selezionare **Avanti**.
4. Nella sezione Select vCenter Server (Seleziona server vCenter), procedere come segue:
 - a. Verificare che vCenter Server del sito protetto venga visualizzato come candidato corrispondente per l'associazione.
 - b. Immettere le credenziali amministrative SSO, quindi selezionare **fine**.
5. Se richiesto, selezionare **Sì** per accettare i certificati di protezione.

Risultato

Nella finestra di dialogo **Oggetti** vengono visualizzati sia i siti protetti che quelli di ripristino.

Configurare i gruppi di protezione

Prima di iniziare

Assicurarsi che i siti di origine e di destinazione siano configurati per:

- È installata la stessa versione di VMware Live Site Recovery
- Macchine virtuali
- Siti di ripristino e protezione associati
- Gli archivi dati di origine e di destinazione devono essere montati sui rispettivi siti

Fasi

1. Accedi a vCenter Server e seleziona **Site Recovery > Gruppi di protezione**.
2. Nel riquadro **gruppi di protezione**, selezionare **nuovo**.
3. Specificare un nome e una descrizione per il gruppo protezione, direzione e selezionare **Avanti**.
4. Nel campo **Tipo**, seleziona l'opzione **Tipo...** come gruppi di datastore (replica basata su array) per datastore NFS e VMFS. Il dominio di errore è costituito esclusivamente da SVM con replica abilitata. Vengono visualizzate le SVM che hanno implementato solo il peering e non presentano problemi.

5. Nella scheda gruppi di replica, selezionare la coppia di array abilitata o i gruppi di replica che hanno configurato la macchina virtuale, quindi selezionare **Avanti**.

Tutte le macchine virtuali presenti nel gruppo di replica vengono aggiunte al gruppo di protezione.

6. È possibile selezionare il piano di ripristino esistente oppure crearne uno nuovo selezionando **Aggiungi al nuovo piano di ripristino**.
7. Nella scheda Pronto per il completamento, esaminare i dettagli del gruppo di protezione creato, quindi selezionare **fine**.

Configurare le risorse protette e del sito di ripristino

Configurare le mappature di rete negli ONTAP tools

È necessario configurare i mapping delle risorse, ad esempio reti di macchine virtuali, host ESXi e cartelle su entrambi i siti, in modo da consentire la mappatura di ciascuna risorsa dal sito protetto alla risorsa appropriata nel sito di ripristino.

È necessario completare le seguenti configurazioni delle risorse:

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

Prima di iniziare

È necessario aver collegato i siti protetti e di ripristino.

Fasi

1. Accedere a vCenter Server e selezionare **Site Recovery > Sites**.
2. Selezionare il sito protetto e selezionare **Gestisci**.
3. Selezionare **mappature di rete > nuovo** nella scheda Gestisci per creare una nuova mappatura di rete.
4. Nella procedura guidata Crea mappatura di rete, effettuare le seguenti operazioni:
 - a. Selezionare **prepara automaticamente mappature per reti con nomi corrispondenti** e selezionare **Avanti**.
 - b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e selezionare **Aggiungi mappature**.
 - c. Selezionare **Avanti** dopo aver creato correttamente le mappature.
 - d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi selezionare **fine**.

Risultato

La pagina Network Mappings (Mapping di rete) visualizza le risorse protette del sito e le risorse del sito di ripristino. È possibile seguire la stessa procedura per le altre reti del proprio ambiente.

Configurare i mapping delle cartelle negli ONTAP tools

È necessario mappare le cartelle sul sito protetto e sul sito di ripristino per consentire la

comunicazione tra di esse.

Prima di iniziare

È necessario aver collegato i siti protetti e di ripristino.

Fasi

1. Accedere a vCenter Server e selezionare **Site Recovery > Sites**.
2. Selezionare il sito protetto e selezionare **Gestisci**.
3. Selezionare **Mapping cartelle > icona cartella** nella scheda Gestisci per creare una nuova mappatura cartelle.
4. Nella procedura guidata Create Folder Mapping (Crea mappatura cartelle), eseguire le seguenti operazioni:
 - a. Selezionare **prepara automaticamente mappature per cartelle con nomi corrispondenti** e selezionare **Avanti**.
 - b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e selezionare **Aggiungi mappature**.
 - c. Selezionare **Avanti** dopo aver creato correttamente le mappature.
 - d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi selezionare **fine**.

Risultato

La pagina Folder Mappings (Mapping cartelle) visualizza le risorse del sito protetto e le risorse del sito di ripristino. È possibile seguire la stessa procedura per le altre reti del proprio ambiente.

Configurare le mappature delle risorse negli ONTAP tools

È necessario mappare le risorse sul sito protetto e sul sito di ripristino in modo che le macchine virtuali siano configurate per eseguire il failover in un gruppo di host o nell'altro.

Prima di iniziare

È necessario aver collegato i siti protetti e di ripristino.



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

Fasi

1. Accedere a vCenter Server e selezionare **Site Recovery > Sites**.
2. Selezionare il sito protetto e selezionare **Gestisci**.
3. Selezionare **mappature risorse > nuovo** nella scheda Gestisci per creare una nuova mappatura delle risorse.
4. Nella procedura guidata Create Resource Mapping (Crea mappatura risorse), eseguire le seguenti operazioni:
 - a. Selezionare **prepara automaticamente mappature per risorsa con nomi corrispondenti** e selezionare **Avanti**.
 - b. Selezionare gli oggetti del data center richiesti per i siti protetti e di ripristino e selezionare **Aggiungi mappature**.
 - c. Selezionare **Avanti** dopo aver creato correttamente le mappature.

- d. Selezionare l'oggetto utilizzato in precedenza per creare la mappatura inversa, quindi selezionare **fine**.

Risultato

La pagina Resource Mappings (Mapping delle risorse) visualizza le risorse protette del sito e le risorse del sito di ripristino. È possibile seguire la stessa procedura per le altre reti del proprio ambiente.

Configurare i datastore segnaposto negli ONTAP tools

Configurare un datastore segnaposto per riservare spazio nell'inventario vCenter nel sito di ripristino per le macchine virtuali (VM) protette. Gli archivi dati segnaposto richiedono una capacità minima, perché le VM segnaposto sono piccole e in genere utilizzano solo poche centinaia di kilobyte.

Prima di iniziare

- Assicurarsi che i siti protetti e di ripristino siano connessi.
- Verificare che le mappature delle risorse siano state configurate.

Fasi

1. Accedere a vCenter Server e selezionare **Site Recovery > Sites**.
2. Selezionare il sito protetto e selezionare **Gestisci**.
3. Selezionare **segnaposto datastore > nuovo** nella scheda Gestisci per creare un nuovo archivio dati segnaposto.
4. Selezionare l'archivio dati appropriato e selezionare **OK**.



Gli archivi dati segnaposto possono risiedere su storage locali o remoti, ma non richiedono replica.

5. Ripetere i passaggi da 3 a 5 per configurare un archivio dati segnaposto per il sito di ripristino.

Configurare SRA utilizzando il gestore array in ONTAP tools

È possibile configurare Storage Replication Adapter (SRA) utilizzando la procedura guidata Array Manager di VMware Live Site Recovery per abilitare le interazioni tra VMware Live Site Recovery e le Storage Virtual Machine (SVM).

Prima di iniziare

- È necessario aver abbinato i siti protetti e i siti di ripristino in VMware Live Site Recovery.
- Prima di configurare il gestore array, è necessario aver configurato lo spazio di archiviazione integrato.
- Dovresti aver configurato e replicato le relazioni SnapMirror tra i siti protetti e i siti di recovery.
- Dovresti aver abilitato le LIF di gestione SVM per l'abilitazione della multi-tenancy.

SRA supporta la gestione a livello di cluster e la gestione a livello di SVM. Aggiungendo lo storage a livello di cluster è possibile rilevare ed eseguire operazioni su tutte le SVM del cluster. Se si aggiunge storage a livello di SVM, è possibile gestire solo la SVM specifica.

Fasi

1. In VMware Live Site Recovery, selezionare **Array Managers > Add Array Manager**.

2. Immettere le seguenti informazioni per descrivere l'array in VMware Live Site Recovery:

- a. Immettere un nome per identificare il gestore array nel campo **Display Name**.
- b. Nel campo **tipo SRA**, selezionare **scheda di replica storage NetApp per ONTAP**.
- c. Inserire le informazioni per la connessione al cluster o alla SVM:
 - Se ci si connette a un cluster, è necessario immettere il LIF di gestione del cluster.
 - Se ci si connette direttamente a una SVM, è necessario immettere l'indirizzo IP del LIF di gestione della SVM.



Durante la configurazione dell'array manager occorre utilizzare la stessa connessione (indirizzo IP) per il sistema storage utilizzato per integrare il sistema storage nei tool ONTAP per VMware vSphere. Ad esempio, se la configurazione del gestore degli array ha un ambito SVM, occorre aggiungere lo storage nei tool ONTAP per VMware vSphere a livello di SVM.

- d. Se ci si connette a un cluster, specificare il nome SVM nel campo **Nome SVM** oppure lasciarlo vuoto per gestire tutte le SVM nel cluster.
- e. Inserire i volumi da rilevare nel campo **Volume include list** (elenco di inclusione del volume).

È possibile inserire il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di ripristino.

Ad esempio, se si desidera rilevare il volume `src_vol1` che si trova in una relazione SnapMirror con il volume `dst_vol1`, è necessario specificare `src_vol1` nel campo del sito protetto e `dst_vol1` nel campo del sito di ripristino.

- f. **(opzionale)** inserire i volumi da escludere dal rilevamento nel campo **elenco esclusioni volume**.

È possibile inserire il volume di origine nel sito protetto e il volume di destinazione replicato nel sito di ripristino.

Ad esempio, se si desidera escludere il volume `src_vol1` che si trova in una relazione SnapMirror con il volume `dst_vol1`, è necessario specificare `src_vol1` nel campo del sito protetto e `dst_vol1` nel campo del sito di ripristino.

3. Selezionare **Avanti**.

4. Verificare che l'array sia rilevato e visualizzato nella parte inferiore della finestra Add Array Manager (Aggiungi array) e selezionare **Finish** (fine).

È possibile seguire gli stessi passaggi per il sito di ripristino utilizzando gli indirizzi IP e le credenziali di gestione SVM appropriati. Nella schermata Enable Array Pairs (Abilita coppie di array) della procedura guidata Add Array Manager (Aggiungi gestore array), verificare che sia selezionata la coppia di array corretta e che sia visualizzata come pronta per essere abilitata.

Verificare i sistemi di archiviazione replicati negli ONTAP tools

È necessario verificare che il sito protetto e il sito di ripristino siano associati correttamente dopo la configurazione dell'adattatore di replica dello storage (SRA). Il sistema storage replicato deve essere raggiungibile sia dal sito protetto che dal sito di recovery.

Prima di iniziare

- È necessario aver configurato il sistema di archiviazione.
- È necessario abbinare il sito protetto e il sito di ripristino utilizzando il gestore dell'array VMware Live Site Recovery.
- Prima di eseguire l'operazione di test failover e di failover per SRA, è necessario aver attivato la licenza FlexClone e la licenza SnapMirror.
- È necessario disporre degli stessi criteri e pianificazioni SnapMirror sui siti di origine e destinazione.

Fasi

1. Accedere al server vCenter.
2. Vai a **Site Recovery > Array Based Replication**.
3. Selezionare la coppia di array richiesta e verificare i dettagli corrispondenti.

I sistemi di archiviazione devono essere rilevati nel sito protetto e nel sito di ripristino con lo stato "abilitato".

Protezione fan-out negli ONTAP tools

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



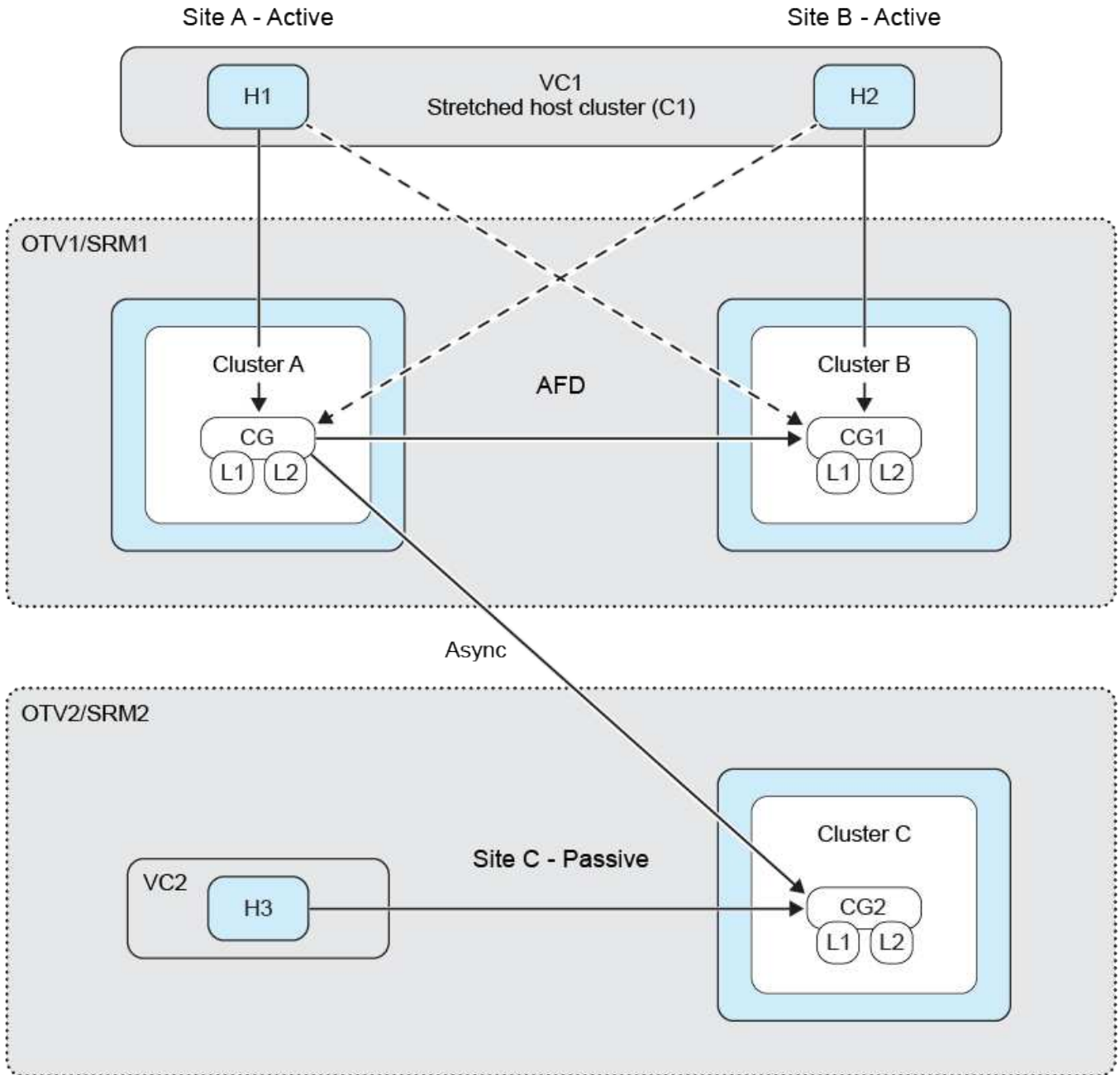
Il fan-out non è supportato per l'utente SVM.

Per impostare la protezione fan-out, collegare in peering i tre cluster di siti e le SVM.

Esempio:

Se	quindi
<ul style="list-style-type: none">• Il gruppo di coerenza di origine è nel cluster C1 e SVM svm1• Il primo gruppo di coerenza di destinazione è sul cluster C2 e SVM svm2 e.• Il secondo gruppo di coerenza di destinazione è sul cluster C3 e SVM svm3	<ul style="list-style-type: none">• Il peering dei cluster sul cluster ONTAP di origine sarà (C1, C2) e (C1, C3).• Il peering del cluster sul primo cluster ONTAP di destinazione sarà (C2, C1), (C2, C3) e.• Il peering del cluster sul secondo cluster ONTAP di destinazione sarà (C3, C1) e (C3, C2).• Il peering delle SVM sull'origine SVM sarà (svm1, svm2) e (svm1, svm3).• Il peering delle SVM sulla prima SVM di destinazione sarà (svm2, svm1) e (svm2, svm3) e.• Il peering delle SVM sulla seconda destinazione SVM sarà (svm3, svm1) e (svm3, svm2).

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

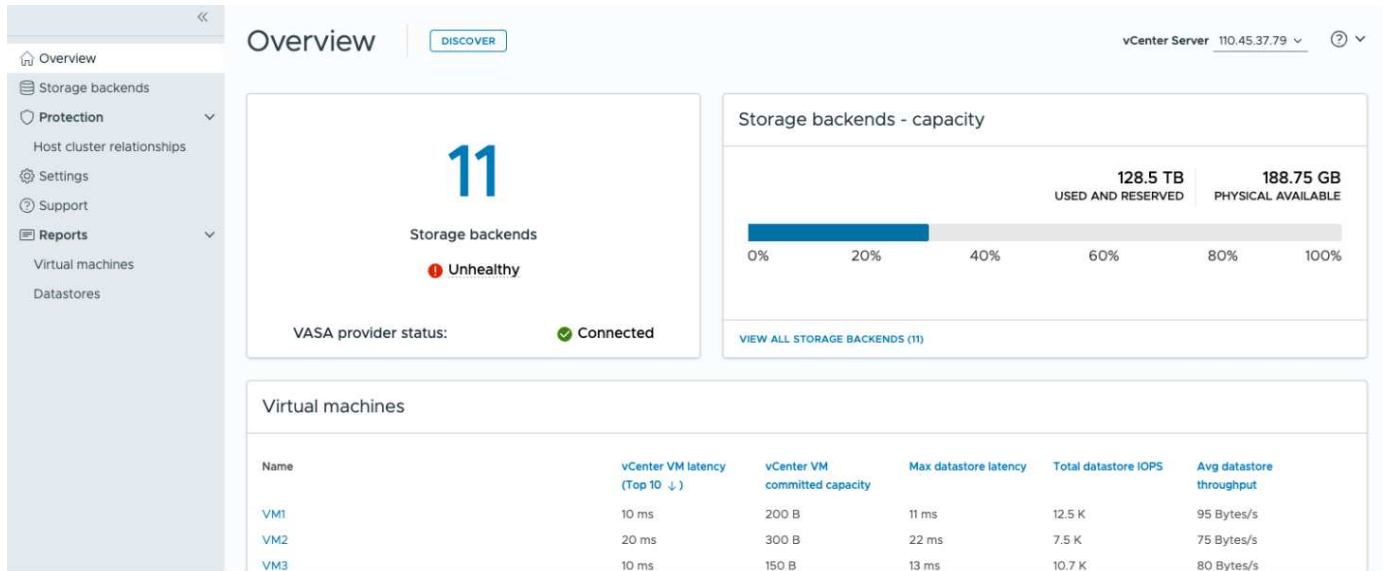


Gestisci i tool ONTAP per VMware vSphere

Scopri la dashboard degli strumenti ONTAP

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

In Enhanced Linked Mode (ELM), viene visualizzato il menu a discesa vCenter Server. Selezionare un vCenter Server per visualizzarne i dati. Il menu a discesa è disponibile in tutte le viste di elenco del plug-in. Quando si seleziona un vCenter Server in una pagina, questo rimane invariato cambiando scheda nel plug-in.



Dalla pagina di panoramica è possibile eseguire l'azione **Discovery**. L'azione di individuazione rileva i backend di storage, gli host, i datastore e lo stato o le relazioni di protezione aggiunti o aggiornati a livello di vCenter. Esegui la scoperta su richiesta senza attendere la scoperta pianificata.



Il pulsante di azione **Scoperta** è abilitato solo se si dispone dei privilegi necessari per eseguire l'azione di scoperta.

Dopo aver inviato la richiesta di individuazione, è possibile monitorare l'avanzamento dell'azione nel pannello delle attività recenti.

Il cruscotto ha diverse schede che mostrano diversi elementi del sistema. La tabella seguente mostra le diverse schede e ciò che esse rappresentano.

Carta	Descrizione
-------	-------------

Stato	La scheda Stato mostra il numero di backend di archiviazione e lo stato di integrità generale dei backend di archiviazione e del provider VASA. Lo stato dei backend di archiviazione mostra integro quando lo stato di tutti i backend di archiviazione è normale e mostra non integro se uno dei backend di archiviazione presenta un problema (stato sconosciuto/irraggiungibile/danneggiato). Selezionare la descrizione comando per aprire i dettagli di stato dei backend di archiviazione. È possibile selezionare qualsiasi backend di storage per ulteriori dettagli. Il collegamento altri stati provider VASA mostra lo stato corrente del provider VASA registrato in vCenter Server.
Backend di archiviazione - capacità	Questa scheda mostra la capacità aggregata utilizzata e disponibile di tutti i backend di storage per l'istanza di vCenter Server selezionata. Nel caso di sistemi di storage ASA r2, i dati sulla capacità non vengono visualizzati perché si tratta di un sistema disaggregato.
Macchine virtuali	Questa scheda mostra le 10 macchine virtuali principali ordinate in base alla metrica delle prestazioni. È possibile selezionare l'istogramma per ottenere le 10 macchine virtuali principali per la metrica selezionata in ordine crescente o decrescente. Le modifiche di ordinamento e filtraggio apportate alla scheda persistono fino a quando non si modifica o si cancella la cache del browser.
Datastore	Questa scheda mostra i 10 principali datastore ordinati in base a una metrica di prestazioni. È possibile selezionare l'istogramma per ottenere i primi 10 datastore per la metrica selezionata ordinati in ordine crescente o decrescente. Le modifiche di ordinamento e filtraggio apportate alla scheda persistono fino a quando non si modifica o si cancella la cache del browser. È disponibile un menu a discesa tipo datastore per selezionare il tipo di datastore: NFS, VMFS o vVol.
Scheda di conformità host ESXi	Questa scheda mostra se tutti gli host ESXi (per il vCenter selezionato) seguono le impostazioni host NetApp consigliate 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 visualizzarne l'elenco.

Come ONTAP tools gestisce gli igroup e le policy di esportazione

I gruppi iniziatori (igroup) sono tabelle di nomi di porte World Wide Port Name (WWPN)

dell'host del protocollo FC o nomi di nodi qualificati dell'host iSCSI. È possibile definire igroups e mapparli alle LUN per controllare quali iniziatori hanno accesso alle LUN.

Negli 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 su più datastore. Gli ONTAP tools for VMware vSphere introducono igroup annidati, in cui ogni datastore in vCenter è associato a un igroup padre, mentre ogni host è collegato a un igroup figlio sotto tale padre. È possibile definire igroup padre personalizzati con nomi definiti dall'utente da riutilizzare in più datastore per semplificare la gestione degli igroup. Comprendere il flusso di lavoro igroup per gestire LUN e datastore negli ONTAP tools for VMware vSphere. Flussi di lavoro diversi generano configurazioni igroup diverse, come mostrato negli esempi seguenti:



I nomi menzionati sono solo a scopo illustrativo e non si riferiscono ai nomi reali dei gruppi igroup. Gli igroup gestiti dagli strumenti ONTAP utilizzano il prefisso "otv_". È possibile assegnare qualsiasi nome agli igroup personalizzati.

Termine	Descrizione
DS<numero>	Datastore
iqn<numero>	IQN iniziatore
host<numero>	Ospita MoRef
lun<numero>	ID LUN
<DSName>Igroup<numero>	Gruppo padre predefinito (gestito dagli strumenti ONTAP)
<Host-Moref>Igroup<numero>	Gruppo infantile
CustomIgroup<numero>	Gruppo padre personalizzato definito dall'utente
ClassicIgroup<numero>	Igroup utilizzato nelle versioni 9.x degli strumenti ONTAP.

Esempio 1:

Crea un datastore su un singolo host con un iniziatore

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

Risultato:

- DS1Igroup:
 - host1Igroup → (iqn1: lun1)

ONTAP crea l'igroup padre DS1Igroup per DS1 e mappa l'igroup figlio host1Igroup su lun1. Il sistema mappa sempre i LUN sugli igroup figlio.

Esempio 2:

Montare il datastore esistente su un host aggiuntivo

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

Risultato:

- DS1lgroup:
 - host1lgroup → (iqn1: lun1)
 - host2lgroup → (iqn2: lun1)

Gli ONTAP tools for VMware vSphere creano un igroup figlio host2lgroup e lo aggiungono all'igroup padre esistente DS1lgroup.

Esempio 3:

Smontare un datastore da un host

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

Risultato:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

Gli ONTAP tools for VMware vSphere rimuovono host1lgroup dalla gerarchia. Il sistema non elimina esplicitamente gli igroup figlio. Li elimina in queste due condizioni:

- Se non viene mappato alcun LUN, il sistema ONTAP elimina l'igroup figlio.
- Un processo di pulizia pianificato rimuove gli igroup figlio sospesi senza mapping LUN. Questi scenari si applicano solo agli igroup gestiti dagli strumenti ONTAP, non a quelli creati dall'utente.

Esempio 4:

Elimina archivio dati

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

Risultato:

- DS1lgroup:
 - host2lgroup → (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:

- Customlgroup1:
 - host1lgruppo → (iqn1: lun2, lun3)
 - host2lgroup → (iqn2: lun2)

- host3lgroup → (iqn3: lun3)

Customlgroup1 viene creato per DS2 e riutilizzato per DS3. Gli igroup figlio vengono creati o aggiornati sotto il 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:

- Customlgroup1:
 - host1lgroup → (iqn1: lun3)
 - host3lgroup → (iqn3: lun3)
- Anche se Customlgroup1 non viene riutilizzato, non viene eliminato.
- Se non viene mappato alcun LUN, il sistema ONTAP elimina host2lgroup.
- host1lgroup 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 datastore vVols (Aggiungi volume)

Flusso di lavoro:

Prima dell'espansione:

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

- DS4lgroup: host4lgroup → (iqn4: lun4)

Dopo l'espansione:

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

- DS4lgroup: host4lgroup → (iqn4: lun4, lun5)

Viene creato un nuovo LUN e mappato all'igroup figlio esistente host4lgroup.

Esempio 8:

Riduci datastore vVols (rimuovi volume)

Flusso di lavoro:

Prima del restringimento:

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

- DS4lgroup: host4lgroup → (iqn4: lun4, lun5)

Dopo il restringimento:

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

- DS4lgroup: host4lgroup → (iqn4: lun4)

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

Esempio 9:

Migrazione dagli strumenti ONTAP 9 a 10 (normalizzazione igroup)

Flusso di lavoro

Gli strumenti ONTAP per le versioni VMware vSphere 9.x non supportano gli igroup gerarchici. Durante la migrazione alla versione 10.3 o successive, gli igroup devono essere normalizzati nella struttura gerarchica.

Prima della migrazione:

[Migrazione] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classiclgroup1 (iqn6 e iqn7: lun6, lun7)

La logica degli strumenti ONTAP 9.x consente più iniziatori per igroup senza imporre la mappatura host uno a uno.

Dopo la migrazione:

[Migrazione] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classiclgroup1: otv_Classiclgroup1 (iqn6 e iqn7: lun6, lun7)

Durante la migrazione:

- Viene creato un nuovo igroup padre (Classiclgroup1).
- L'igroup originale viene rinominato con il prefisso otv_ e diventa un igroup figlio.

Ciò garantisce il rispetto del modello gerarchico.

Argomenti correlati

["A proposito di igroups"](#)

Policy di esportazione

I criteri di esportazione controllano l'accesso al datastore NFS e le autorizzazioni client negli ONTAP tools for VMware vSphere. Le policy di esportazione vengono create e gestite nei sistemi ONTAP e possono essere utilizzate con gli archivi dati NFS per applicare 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 si crea un datastore NFS negli strumenti ONTAP per VMware vSphere, è possibile selezionare una policy di esportazione esistente o crearne una nuova. La policy di esportazione viene quindi applicata al datastore, garantendo che solo i client autorizzati possano accedervi.

Quando si monta un datastore NFS su un nuovo host ESXi, gli strumenti ONTAP per VMware vSphere aggiungono l'indirizzo IP dell'host alla policy di esportazione esistente associata al datastore. Ciò consente al nuovo host di accedere al datastore senza dover creare una nuova policy di esportazione.

Quando si elimina o si smonta un datastore NFS da un host ESXi, gli ONTAP tools for VMware vSphere rimuovono l'indirizzo IP dell'host dalla policy di esportazione. Se nessun altro host utilizza tale criterio di esportazione, verrà eliminato. Quando si elimina un datastore NFS, gli ONTAP tools for VMware vSphere

rimuovono la policy di esportazione associata a tale datastore se non viene riutilizzata da altri datastore. Se la policy di esportazione viene riutilizzata, l'indirizzo IP dell'host viene mantenuto e non cambia. Quando si eliminano i datastore, la policy di esportazione annulla l'assegnazione dell'indirizzo IP dell'host e assegna una policy di esportazione predefinita, in modo che i sistemi ONTAP possano accedervi se necessario.

L'assegnazione della policy di esportazione varia a seconda che venga riutilizzata su datastore diversi. Quando si riutilizza la policy di esportazione, è possibile aggiungerla con il nuovo indirizzo IP host. Quando si elimina o si smonta un datastore che utilizza una policy di esportazione condivisa, la policy non verrà eliminata. Rimane invariata e l'indirizzo IP host non viene rimosso, poiché è condivisa con gli altri datastore. Il riutilizzo delle policy di esportazione è sconsigliato, poiché può causare problemi di accesso e latenza.

Argomenti correlati

["Creare una policy di esportazione"](#)

Come ONTAP tools gestisce gli igroup

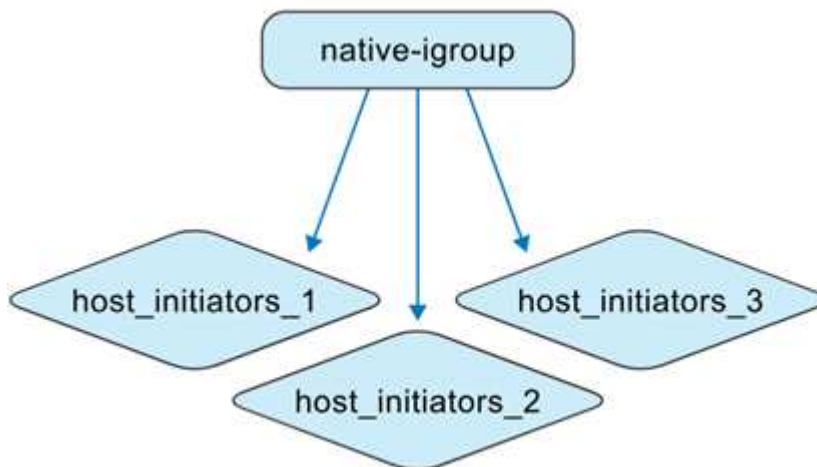
Se si gestiscono sia le VM degli strumenti ONTAP sia i sistemi di archiviazione ONTAP, è importante comprendere il comportamento degli igroup, in particolare quando si spostano gli archivi dati da ambienti non gestiti dagli strumenti ONTAP a quelli che lo sono. Questa pagina spiega come vengono aggiornati gli igroup durante questo processo.

Gli ONTAP tools for VMware vSphere 10.4 e versioni successive creano e gestiscono automaticamente oggetti ONTAP e vCenter per semplificare la gestione dei datastore negli ambienti data center VMware.

Gli ONTAP tools for VMware vSphere interpretano gli igroup in due contesti diversi:

Strumenti non ONTAP gestiti da igroup

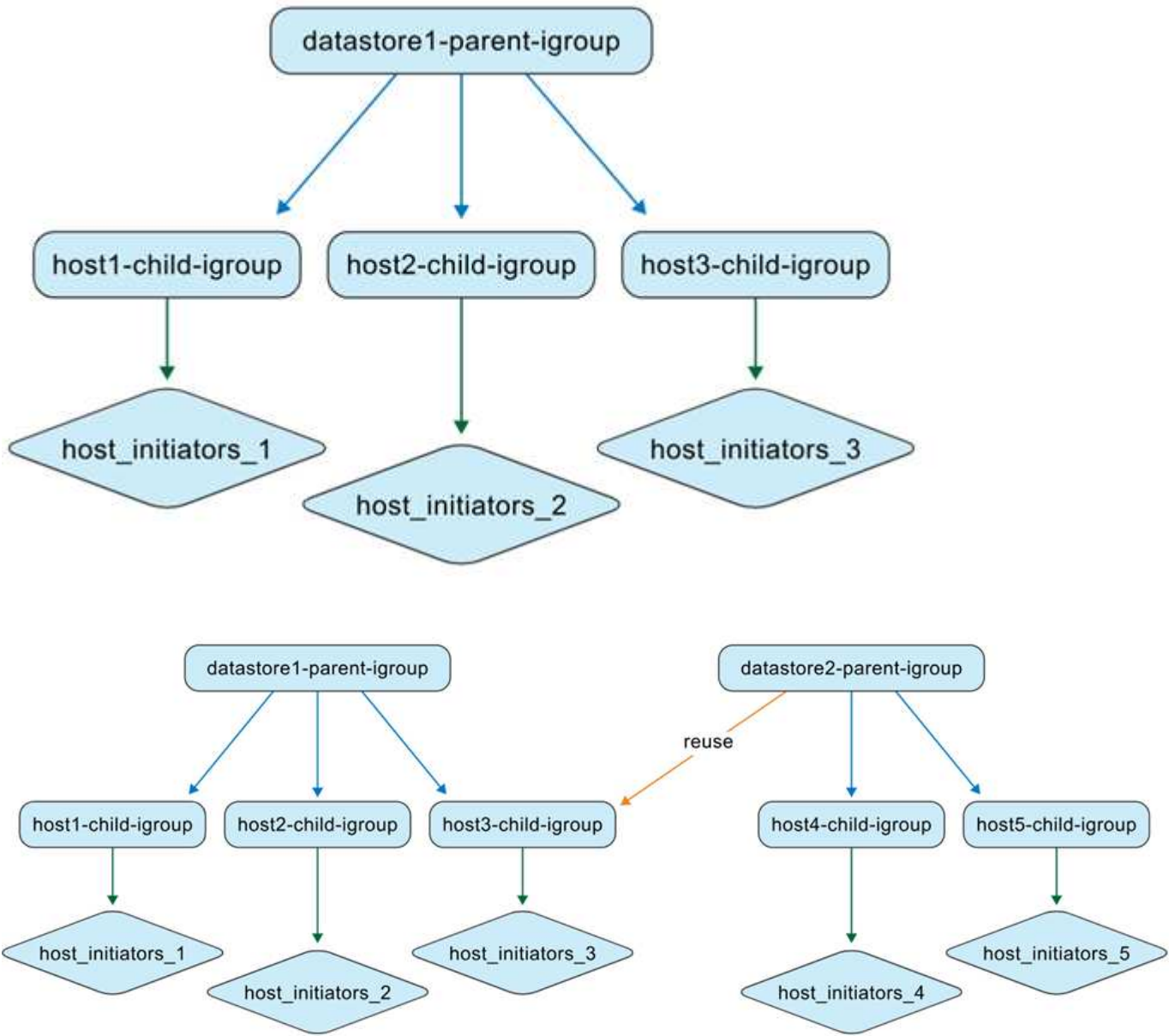
In qualità di amministratore di storage, puoi creare igroup sul sistema ONTAP come strutture semplici o nidificate. L'illustrazione mostra un igroup piatto creato nel sistema ONTAP.



Strumenti ONTAP gestiti igroup

Quando si creano datastore, gli ONTAP tools for VMware vSphere creano automaticamente igroup utilizzando una struttura annidata per semplificare la mappatura LUN.

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, gli strumenti ONTAP riutilizzano l'igroup a livello di host per una gestione efficiente.



Ecco alcuni casi di utilizzo ONTAP tools for VMware vSphere .

Quando si crea un datastore con impostazioni igroup predefinite

Quando si crea un datastore e si lascia vuoto il campo igroup (impostazione predefinita), gli strumenti ONTAP generano automaticamente una struttura igroup annidata per quel datastore. L'igroup padre a livello di datastore viene denominato utilizzando il modello:

otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>. Ogni igroup figlio a livello di host segue il modello: otv_<hostMoref>_<vcguid>. È possibile visualizzare l'associazione tra igroup padre (a livello di datastore) e figlio (a livello di host) nella sezione **Parent Initiator Group** dell'interfaccia di archiviazione ONTAP .

Con l'approccio igroup annidato, le LUN vengono mappate solo agli igroup figlio. L'inventario di vCenter Server visualizza quindi il nuovo datastore.

Quando si crea un datastore con un nome igroup personalizzato

Durante la creazione del datastore negli strumenti ONTAP , è possibile immettere un nome igroup personalizzato anziché selezionarlo dal menu a discesa. Gli strumenti ONTAP creano quindi un igroup padre a livello di datastore utilizzando il nome specificato. Se lo stesso host viene utilizzato per più datastore, viene riutilizzato l'igroup (figlio) a livello di host esistente. Di conseguenza, il LUN per il nuovo datastore viene mappato su questo igroup figlio esistente, che ora potrebbe essere associato a più igroup padre (uno per ciascun datastore). È possibile visualizzare il nuovo datastore con il nome igroup personalizzato nell'interfaccia di vCenter Server.

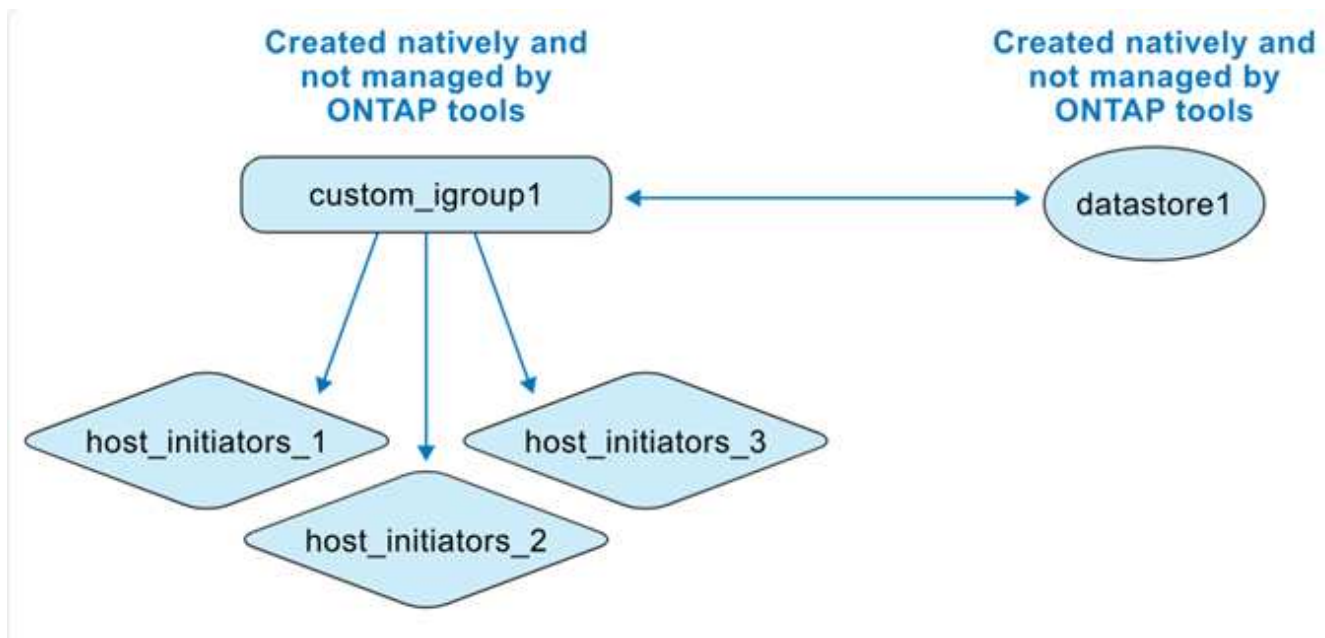
Quando si riutilizza il nome igroup durante la creazione del datastore

Quando si crea un datastore utilizzando l'interfaccia utente degli strumenti ONTAP , è possibile scegliere un igroup padre personalizzato esistente dall'elenco a discesa. Dopo aver riutilizzato l'igroup padre per creare un altro datastore, l'interfaccia utente dei sistemi ONTAP mostra questa associazione. Il nuovo datastore viene visualizzato anche nell'interfaccia utente di vCenter Server.

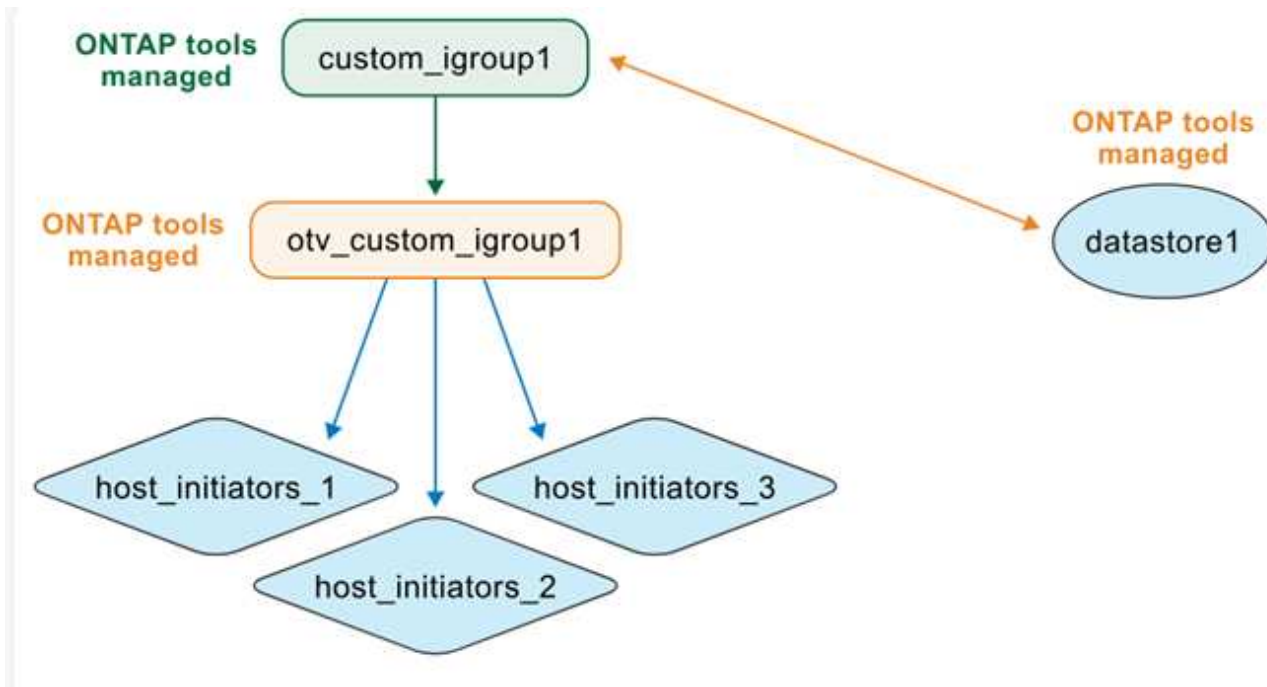
Questa operazione può essere eseguita anche tramite API. Per riutilizzare un igroup esistente durante la creazione del datastore, specificare l'UUID dell'igroup nel payload della richiesta API.

Quando si crea un datastore e un igroup in modo nativo da ONTAP e vCenter

Se si creano igroup e datastore direttamente nei sistemi ONTAP e negli ambienti VMware, gli strumenti ONTAP non gestiscono inizialmente questi oggetti. Ciò crea una struttura igroup piatta.



Per gestire un datastore e un igroup esistenti con gli strumenti ONTAP , è necessario eseguire un'individuazione del datastore. Gli strumenti ONTAP identificano e registrano il datastore e l'igroup e li convertono in una struttura annidata nel proprio database. Viene creato un nuovo igroup padre utilizzando il nome personalizzato, mentre l'igroup esistente viene rinominato con il prefisso "otv_" e diventa l'igroup figlio. Le mappature degli iniziatori rimangono invariate. Durante l'individuazione vengono convertiti solo gli igroup mappati sui datastore. Dopodiché la struttura igroup appare come nell'illustrazione sottostante.



Dopo aver eseguito la scoperta del datastore negli strumenti ONTAP , gli strumenti ONTAP convertono l'igroup piatto in una struttura annidata. Gli strumenti ONTAP gestiscono quindi l'igroup, rinominandolo con il prefisso 'otv_'. Durante tutto il processo, la LUN rimane mappata sullo stesso igroup.

Come gli strumenti ONTAP riutilizzano gli igroup creati in modo nativo

È possibile creare un datastore negli strumenti ONTAP utilizzando un igroup creato inizialmente nei sistemi ONTAP , dopo che gli strumenti ONTAP lo hanno gestito. Questi igroup vengono visualizzati nell'elenco a discesa del nome del gruppo di iniziatori personalizzato. Il nuovo LUN per il datastore viene quindi mappato al corrispondente igroup figlio normalizzato, ad esempio "otv_Nativegroup1".

Gli ONTAP tools for VMware vSphere non rilevano né utilizzano gli igroup creati nel sistema ONTAP che non sono gestiti dagli strumenti ONTAP o collegati a un datastore.

Scopri l'interfaccia utente di ONTAP tools Manager

Gli ONTAP tools for VMware vSphere supportano il multi-tenancy, consentendo la gestione di più istanze di vCenter Server.

ONTAP Tools Manager è una console basata sul Web per la gestione ONTAP tools for VMware vSphere, istanze di vCenter Server, backend di storage e configurazione di appliance quali High Availability (HA) e ridimensionamento dei nodi.

ONTAP Tools Manager offre le seguenti funzionalità:

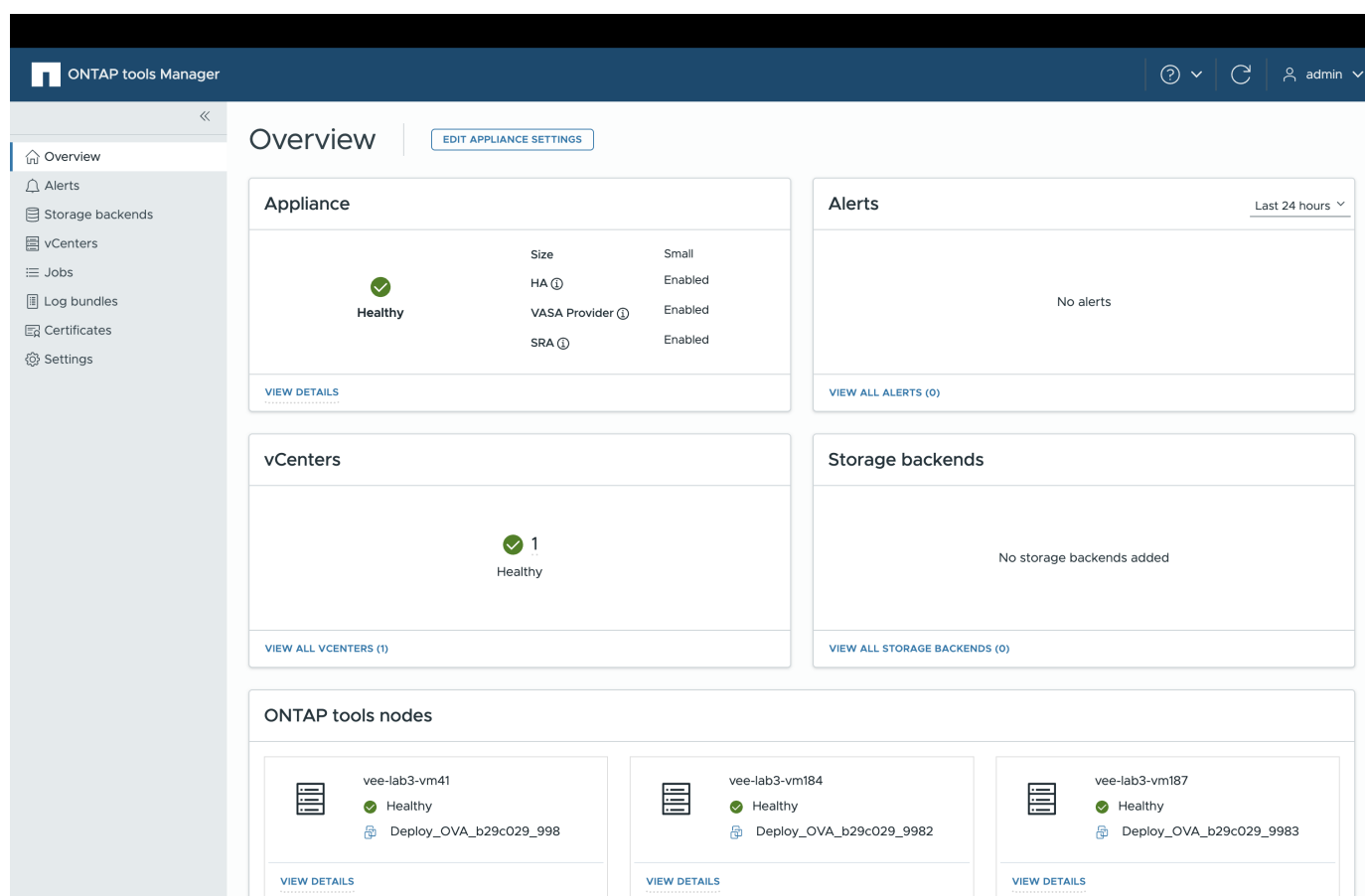
- Gestisci avvisi: visualizza e filtra gli avvisi generati dagli ONTAP tools for VMware vSphere.
- Gestisci i backend di archiviazione: aggiungi e gestisci i cluster di archiviazione ONTAP e mappali alle istanze di vCenter Server a livello globale.
- Gestisci istanze di vCenter Server: aggiungi e gestisci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

in degli strumenti ONTAP sia dall'interfaccia del gestore degli strumenti ONTAP . È possibile filtrare i lavori in base al periodo di tempo, modificare le dimensioni della pagina e visualizzare i dettagli del lavoro, inclusi errori e sottoattività. Fare clic su uno stato non riuscito per i dettagli dell'errore. Per i lavori con sottoattività, espandere la riga per visualizzare descrizioni e stati. Per i sotto-lavori, utilizzare il drill-down del lavoro per visualizzarne i dettagli.

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

Per accedere a ONTAP Tools Manager, avviare il

https://<ONTAPtoolsIP>:8443/virtualization/ui/ sistema dal browser e accedere con gli strumenti ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.



Carta	Descrizione
Scheda dell'appliance	La scheda Appliance mostra lo stato generale dell'appliance degli strumenti ONTAP , i dettagli di configurazione e lo stato dei servizi abilitati. Per visualizzare maggiori informazioni, seleziona il link Visualizza dettagli . Se si modifica un'impostazione dell'apparecchio, la scheda mostra lo stato del lavoro e i dettagli fino al completamento della modifica.

Carta	Descrizione
Scheda avvisi	La scheda Avvisi mostra gli avvisi degli strumenti ONTAP classificati per tipo, inclusi gli avvisi a livello di nodo HA. È possibile visualizzare avvisi dettagliati facendo clic sul collegamento ipertestuale del conteggio, che conduce alla pagina degli avvisi filtrati in base al tipo di avviso selezionato.
Scheda vCenters	La scheda vCenter mostra lo stato di integrità di tutte le istanze di vCenter Server gestite dagli strumenti ONTAP . È possibile visualizzare i dettagli di ciascun vCenter selezionando il collegamento corrispondente, che conduce a una pagina con maggiori informazioni sull'istanza selezionata.
Scheda backend di archiviazione	La scheda Backend di archiviazione mostra lo stato di integrità e connettività di tutti i cluster di archiviazione ONTAP configurati negli strumenti ONTAP . È possibile visualizzare i dettagli per ciascun backend di archiviazione selezionando il collegamento corrispondente, che conduce a una pagina con maggiori informazioni sul cluster selezionato.
Scheda nodi strumenti ONTAP	La scheda dei nodi degli strumenti ONTAP mostra tutti i nodi nell'appliance, inclusi il nome del nodo, il nome della VM, lo stato e le informazioni di rete. Selezionare Visualizza dettagli per visualizzare maggiori dettagli su un nodo specifico. [NOTA] In una configurazione non HA, viene visualizzato un solo nodo. In una configurazione HA vengono visualizzati tre nodi.

Gestisci le impostazioni del gestore degli strumenti ONTAP

Modifica le impostazioni di AutoSupport degli strumenti ONTAP

Quando si configurano gli ONTAP tools for VMware vSphere per la prima volta, AutoSupport è abilitato per impostazione predefinita. Invia messaggi al supporto tecnico 24 ore dopo l'attivazione.

Disattiva AutoSupport

Disattivando AutoSupport, non riceverai più supporto e monitoraggio proattivi.



Si consiglia di mantenere abilitato AutoSupport , poiché aiuta ad accelerare il rilevamento e la risoluzione dei problemi. Anche quando AutoSupport è disattivato, il sistema continua a raccogliere e memorizzare informazioni localmente, ma non invia report tramite la rete.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>

2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare l'opzione **Impostazioni > Telemetria > Modifica**.
4. Deselezionare l'opzione **AutoSupport** e salvare le modifiche.

Aggiorna URL proxy AutoSupport

Aggiornare l'URL del proxy AutoSupport in modo che la funzionalità AutoSupport instrada i dati attraverso il server proxy per una trasmissione sicura.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Seleziona **Impostazioni** dalla barra laterale.
4. Selezionare l'opzione **Impostazioni > Telemetria > Modifica**.
5. Immettere un **URL proxy** valido e salvare le modifiche.

Se si disattiva AutoSupport, anche l'URL proxy viene disattivato.

Aggiungi server NTP agli strumenti ONTAP

Immettere i dettagli del server NTP per sincronizzare gli orologi dell'appliance ONTAP Tools.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare l'opzione **Impostazioni > Server NTP > Modifica**.
4. Immettere gli indirizzi FQDN (Fully Qualified Domain Name), IPv4 o IPv6 separati da virgola.

Aggiornare alla 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 utilizzando l'interfaccia di ONTAP Tools Manager. La nuova password deve essere lunga tra 8 e 256 caratteri.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante

l'implementazione.

3. Selezionare l'opzione **Impostazioni > Credenziali fornitore VASA/SRA > Reimposta password**.
4. Inserisci la nuova password e confermala.
5. Selezionare **Salva** per applicare le modifiche.

Modifica le impostazioni di backup di ONTAP tools

A partire dagli ONTAP tools for VMware vSphere 10.5, la funzionalità di backup è abilitata per impostazione predefinita e viene creato un backup ogni 10 minuti. È possibile disattivare il backup o modificarne la frequenza.

Non disattivare il backup perché impedisce agli strumenti ONTAP di mantenere un RPO basso. La disattivazione del backup non elimina i file di backup esistenti. È possibile modificare la frequenza del backup impostando un valore compreso tra 10 e 60 minuti.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare l'opzione **Impostazioni > Backup > Modifica**.
4. Nella finestra di modifica è possibile disattivare il backup o modificarne la frequenza.

Abilita i servizi di ONTAP tools

È possibile modificare la password dell'amministratore utilizzando Gestione strumenti ONTAP per abilitare servizi come provider VASA, importazione della configurazione vVol e disaster recovery (SRA) utilizzando Gestione strumenti ONTAP.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **Modifica impostazioni appliance** nella sezione Panoramica.
4. Nella sezione **Servizi** è possibile abilitare servizi opzionali come VASA Provider, importazione della configurazione vVols e disaster recovery (SRA) in base alle esigenze.

Quando si abilitano i servizi per la prima volta, è necessario creare le credenziali del provider VASA e SRA. Vengono utilizzati per registrare o abilitare i servizi VASA Provider e SRA su vCenter Server. Il nome utente può contenere solo lettere, numeri e caratteri di sottolineatura. La lunghezza della password deve essere compresa tra 8 e 256 caratteri.



Prima di disabilitare qualsiasi servizio opzionale, assicurarsi che i vCenter Server gestiti dagli strumenti ONTAP non li utilizzino.

L'opzione *Consenti importazione della configurazione vVols* viene visualizzata solo quando è abilitato il

servizio VASA Provider. Questa opzione consente la migrazione dei dati vVols dagli strumenti ONTAP 9.xx agli strumenti ONTAP 10.5.

Modificare le impostazioni dell'appliance ONTAP tools

Utilizzare ONTAP Tools Manager per ampliare la configurazione ONTAP tools for VMware vSphere , aumentando il numero di nodi o abilitando l'alta disponibilità (HA). Per impostazione predefinita, gli ONTAP tools for VMware vSphere vengono distribuiti come configurazione a nodo singolo, non HA.

Prima di iniziare

- Assicurarsi che il modello OVA abbia la stessa versione OVA del nodo 1. Il nodo 1 è il nodo predefinito in cui vengono inizialmente implementati i tool ONTAP per VMware vSphere OVA.
- Assicurarsi che l'hot add della CPU e l'hot plug della memoria siano abilitati.
- Nel vCenter Server, imposta il livello di automazione del Disaster Recovery Service (DRS) su parzialmente automatizzato. Dopo aver implementato HA, ripristinalo su completamente automatizzato.
- I nomi host dei nodi nella configurazione HA devono essere in minuscolo.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **Modifica impostazioni appliance** nella sezione Panoramica.
4. Nella sezione **Configurazione**, aumenta le dimensioni del nodo e abilita la configurazione HA. Utilizzare le credenziali di vCenter Server per apportare modifiche.

Nella configurazione HA è possibile modificare i dettagli della libreria dei contenuti. Fornire la password per ogni modifica.



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

5. Utilizzare il pulsante di commutazione ha per abilitare la configurazione ha. Nella pagina **ha settings**, verificare che:
 - La libreria di contenuti appartiene allo stesso vCenter Server in cui vengono eseguite le macchine virtuali del nodo degli strumenti ONTAP. Le credenziali vCenter Server vengono utilizzate per convalidare e scaricare il modello OVA per le modifiche all'appliance.
 - La macchina virtuale che ospita gli strumenti ONTAP non viene implementata direttamente su un host ESXi. La VM deve essere distribuita su un cluster o su un pool di risorse.



Dopo aver abilitato la configurazione HA, non è possibile tornare a una configurazione a nodo singolo non HA.

6. Nella sezione **ha settings** della finestra **Edit Appliance Settings**, è possibile immettere i dettagli dei nodi

2 e 3. I tool ONTAP per VMware vSphere supportano tre nodi nel setup ha.



Gli strumenti ONTAP precompilano la maggior parte delle opzioni di input con i dettagli della rete Node 1 per semplificare il flusso di lavoro. È possibile modificare i dati di input prima di passare all'ultima pagina della procedura guidata. È possibile immettere i dettagli dell'indirizzo IPv6 per gli altri due nodi solo quando l'indirizzo IPv6 è abilitato sul nodo di gestione degli strumenti ONTAP .

Assicurarsi che un host ESXi contenga solo una VM di strumenti ONTAP. I dati immessi vengono convalidati ogni volta che si passa alla finestra successiva.

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

Quali sono le prossime novità?

La pagina **Panoramica** mostra lo stato della distribuzione. È anche possibile monitorare lo stato del processo di modifica delle impostazioni dell'appliance dalla vista processi utilizzando l'ID processo.

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

La scheda **Avvisi** sul pannello di sinistra elenca gli avvisi per gli strumenti ONTAP per VMware vSphere.

Aggiungere host VMware vSphere a ONTAP tools

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

Fasi

1. Aggiungi un host al tuo cluster VMware vSphere seguendo il flusso di lavoro a pagina: "[Come aggiungere un host ESX al cluster vSphere utilizzando il flusso di lavoro di avvio rapido](#)"
2. Dopo aver aggiunto l'host, vai al menu principale degli strumenti ONTAP e seleziona **Scopri** nel pannello di panoramica. Attendi il completamento del processo di scoperta. In alternativa, è possibile attendere il completamento della rilevazione dell'host pianificata.

Risultato

Il nuovo host è ora rilevato e gestito dagli ONTAP tools for VMware vSphere. È possibile procedere alla gestione del datastore sul nuovo host.

Argomenti correlati

- "[Montare un datastore vVols](#)" sui nuovi host.
- "[Montare il datastore NFS e VMFS](#)" sui nuovi host.

Gestire i datastore

Montare i datastore NFS e VMFS negli ONTAP tools

Il montaggio di un datastore fornisce l'accesso allo storage a host aggiuntivi. È possibile montare il datastore sugli host aggiuntivi dopo aver aggiunto gli host all'ambiente VMware.



Quando si aggiunge un nuovo host ESXi utilizzando ["Aggiungi un host ESX al flusso di lavoro del cluster vSphere"](#) , attendere il completamento della rilevazione host pianificata prima che venga visualizzata negli strumenti ONTAP . In alternativa, è possibile eseguire manualmente l'individuazione dalla schermata di panoramica degli strumenti NetApp ONTAP .

A proposito di questa attività

- Alcune azioni del pulsante destro del mouse sono disattivate o non disponibili a seconda della versione del client vSphere e del tipo di datastore selezionato.
 - Se si utilizza vSphere client 8,0 o versioni successive, alcune delle opzioni del pulsante destro del mouse sono nascoste.
 - Dalle versioni di vSphere 7.0U3 a vSphere 8,0, anche se vengono visualizzate le opzioni, l'azione verrà disattivata.
- vSphere disabilita l'opzione di montaggio del datastore quando il cluster host è protetto con configurazioni uniformi.

Fasi

1. Dalla home page di vSphere Client, selezionare **host e cluster**.
2. Nel riquadro di spostamento di sinistra, selezionare i data center contenenti gli host.
3. Per montare datastore NFS/VMFS su un host o un cluster di host, fare clic con il pulsante destro del mouse e selezionare **Strumenti NetApp ONTAP * > *Monta datastore**.
4. Selezionare gli archivi dati che si desidera montare e selezionare **Mount**.

Quali sono le prossime novità?

È possibile tenere traccia dell'avanzamento nel riquadro attività recenti.

Argomento correlato

["Aggiungi nuovi host VMware vSphere"](#)

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 dagli ONTAP tools for VMware vSphere.

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su un oggetto datastore NFS o VMFS e selezionare **Smonta datastore**.

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

3. Selezionare uno o più host ESXi per smontare il datastore.

Non è possibile smontare il datastore da tutti gli host. L'interfaccia utente suggerisce invece di utilizzare l'operazione di eliminazione dell'archivio dati.

4. Selezionare il pulsante **Smonta**.

Se l'archivio dati fa parte di un cluster host protetto, viene visualizzato un messaggio di avviso.



Se il datastore protetto viene smontato, l'impostazione di protezione esistente potrebbe comportare una protezione parziale. Fare riferimento a ["Modificare il cluster host protetto"](#) per consentire una protezione completa.

Quali sono le prossime novità?

È possibile tenere traccia dell'avanzamento nel pannello attività recenti.

Montare un datastore vVols negli ONTAP tools

È possibile montare un datastore di volumi virtuali VMware (vVol) su uno o più host aggiuntivi per fornire accesso allo storage a host aggiuntivi. È possibile smontare il datastore vVol solo attraverso le API.



Quando si aggiunge un nuovo host ESXi utilizzando ["Aggiungi un host ESX al flusso di lavoro del cluster vSphere"](#), attendere il completamento della rilevazione host pianificata prima che venga visualizzata negli strumenti ONTAP. In alternativa, è possibile eseguire manualmente l'individuazione dalla schermata di panoramica degli strumenti NetApp ONTAP.

Fasi

1. Dalla home page di vSphere Client, selezionare **host e cluster**.
2. Nel riquadro di navigazione, selezionare il centro dati che contiene l'archivio dati.
3. Fare clic con il pulsante destro del mouse sul datastore e selezionare **NetApp ONTAP tools > Mount datastore**.
4. Nella finestra di dialogo **Mount Datastore on hosts**, selezionare gli host su cui si desidera montare il datastore, quindi selezionare **Mount**.

Il pannello delle attività recenti mostra lo stato di avanzamento.

Argomento correlato

["Aggiungi nuovi host VMware vSphere"](#)

Ridimensiona i datastore NFS e VMFS negli ONTAP tools

Il ridimensionamento di un datastore consente di aumentare lo storage dei file delle macchine virtuali. È possibile modificare le dimensioni di un datastore in base al cambiamento dei requisiti dell'infrastruttura.

A proposito di questa attività

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

Fasi

1. Dalla home page di vSphere Client, selezionare **host e cluster**.
2. Nel riquadro di navigazione, selezionare il centro dati che contiene l'archivio dati.
3. Fare clic con il pulsante destro del mouse sul datastore NFS o VMFS e selezionare **NetApp ONTAP tools > Ridimensiona datastore**.

4. Nella finestra di dialogo Ridimensiona, immettere una nuova dimensione per l'archivio dati e selezionare **OK**.

Espandi gli datastore vVols negli ONTAP tools

Facendo clic con il pulsante destro del mouse sull'oggetto datastore nella vista oggetti vCenter, la sezione plug-in mostra le azioni supportate per gli ONTAP tools for VMware vSphere. A seconda del tipo di datastore e dei privilegi utente correnti, vengono abilitate azioni specifiche.



Il funzionamento del datastore Expand vVol non è applicabile ai datastore vVol basati sul sistema ASA R2.

Fasi

1. Dalla home page di vSphere Client, selezionare **host e cluster**.
2. Nel riquadro di navigazione, selezionare il centro dati che contiene l'archivio dati.
3. Fare clic con il pulsante destro del mouse sul datastore e selezionare **Strumenti NetApp ONTAP > Aggiungi storage al datastore**.
4. Nella finestra **Crea o Seleziona volumi**, è possibile creare nuovi volumi oppure scegliere tra quelli esistenti. Seguire le istruzioni sullo schermo per effettuare la selezione.
5. Nella finestra **Riepilogo**, rivedere le selezioni e selezionare **Espandi**. È possibile tenere traccia dell'avanzamento nel pannello attività recenti.

Ridurre un datastore vVols negli ONTAP tools

Questa pagina spiega come rimuovere volumi da un datastore vVols .

Utilizzare l'azione di rimozione dello storage dal datastore su qualsiasi datastore vVols gestito dagli strumenti ONTAP in vCenter Server.

Non è possibile rimuovere l'archiviazione da un volume se contiene vVols; l'opzione di rimozione sarà disabilitata per tali volumi. Quando si rimuovono volumi dal datastore, è anche possibile eliminare i volumi selezionati dall'archiviazione ONTAP .



L'operazione di riduzione del datastore vVols non è supportata per i datastore vVols basati sui sistemi ASA r2.

Fasi

1. Dalla home page di vSphere Client, selezionare **host e cluster**.
2. Nel riquadro di navigazione, selezionare il centro dati che contiene l'archivio dati.
3. Fare clic con il pulsante destro del mouse sul datastore vVol e selezionare **Strumenti NetApp ONTAP > Rimuovi storage dal datastore**.
4. Selezionare i volumi che non hanno vVols e selezionare **Rimuovi**.



L'opzione per selezionare il volume su cui risiede vVols è disabilitata.

5. Nella finestra pop-up **Rimuovi storage**, seleziona la casella di controllo **Elimina volumi dal cluster ONTAP** per eliminare i volumi dal datastore e dallo storage ONTAP e seleziona **Elimina**.

Elimina i datastore in ONTAP tools

Questa pagina descrive come eliminare i datastore NFS, VMFS o vVols utilizzando gli strumenti ONTAP in vCenter Server.

Quando si elimina un datastore, vengono eseguite le seguenti azioni a seconda del tipo di datastore:

- Il contenitore vVol è smontato.
- Se l'igroup non è in uso, iqn viene rimosso dall'igroup.
- Il contenitore vVol è stato eliminato.
- I volumi flessibili vengono lasciati nell'array di archiviazione.

È possibile eliminare il datastore solo se non sono presenti vVols sul datastore selezionato.

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su un sistema host, un cluster host o un data center e selezionare **Strumenti NetApp ONTAP** > ***Elimina datastore**.



Non è possibile eliminare un datastore utilizzato dalle macchine virtuali. Spostare le macchine virtuali in un altro datastore prima di eliminarle. Non è possibile 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 nessuna macchina virtuale è associata a un datastore VMFS, verrà visualizzata una finestra di dialogo di conferma. Se la protezione del cluster host è abilitata ed esiste una relazione AFD, è possibile pulire gli elementi di archiviazione secondaria.
 - c. Per i datastore VMFS protetti sui sistemi ASA r2, rimuovere la protezione prima di eliminare. A partire da ONTAP 9.17.1 e ONTAP tools for VMware vSphere 10.5, è possibile 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, è possibile eliminare il datastore solo se non sono presenti vVols. La finestra di dialogo **Elimina datastore** include un'opzione per rimuovere volumi dal cluster ONTAP.
 - e. Per i datastore vVols sui sistemi ASA r2, non è possibile eliminare i volumi di supporto da ONTAP utilizzando l'opzione **Elimina datastore**.
3. Per eliminare i volumi di backup sull'archiviazione ONTAP, selezionare **Elimina volumi sul cluster ONTAP**.



Per i datastore VMFS su storage ONTAP unificato che fanno parte di un cluster host protetto, non è possibile eliminare il volume dal cluster ONTAP.

Quando si elimina un datastore NFS, VMFS o vVols, gli igroup padre rimangono sul sistema ONTAP. Gli igroup figlio che non sono mappati ad alcun LUN vengono eliminati automaticamente. Gli strumenti ONTAP eseguono una pulizia giornaliera per rimuovere gli igroup padre predefiniti non mappati. Eliminare manualmente gli igroup padre personalizzati in ONTAP. Gli strumenti ONTAP non possono riutilizzare igroup padre obsoleti.

Visualizzazioni dello storage ONTAP per i datastore negli ONTAP tools

I tool ONTAP per VMware vSphere mostrano la vista laterale dello storage ONTAP dei datastore e dei relativi volumi nella scheda configura.

Fasi

1. Dal client vSphere, vai al datastore.
2. Selezionare la scheda **Configura** nel riquadro di destra.
3. Selezionare *Strumenti NetApp ONTAP * > * Archiviazione ONTAP *. La visualizzazione cambia in base al tipo di datastore. Vedere la tabella sottostante:

Tipo datastore	Informazioni disponibili
Datastore NFS	La pagina Dettagli archiviazione contiene backend di archiviazione, informazioni di aggregazione e volume. La pagina Dettagli NFS contiene dati relativi al datastore NFS.
Datastore VMFS	La pagina Dettagli archiviazione contiene i dettagli relativi al backend, all'aggregato, al volume e alla zona di disponibilità dello storage (SAZ). La pagina Dettagli unità di archiviazione contiene i dettagli dell'unità di archiviazione.
Datastore vVol	Elenca tutti i volumi. È possibile espandere o rimuovere lo spazio di archiviazione dal riquadro di archiviazione ONTAP . Gli strumenti ONTAP non supportano questa visualizzazione per i datastore vVols basati sul sistema ASA r2.

Visualizzazione dell'archiviazione della macchina virtuale in ONTAP tools

La vista di archiviazione mostra l'elenco dei vVols creati dalla macchina virtuale.



Questa visualizzazione si applica alle VM con almeno un disco da un datastore vVols gestito da ONTAP tools for VMware vSphere .

Fasi

1. Da vSphere Client vai alla macchina virtuale.
2. Selezionare la scheda **Monitor** nel riquadro di destra.
3. Selezionare **NetApp ONTAP tools > Storage**. I dettagli **archiviazione** vengono visualizzati nel riquadro di destra. È possibile visualizzare l'elenco dei vVol presenti sulla VM.

È possibile utilizzare l'opzione 'Gestisci colonne' per nascondere o visualizzare colonne diverse.

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.

Fasi:

1. Accedere al client vSphere.
2. Nella pagina Collegamenti, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Impostazioni > Impostazioni soglia > Modifica**.
4. Nella finestra **Modifica soglia**, immettere i valori desiderati nei campi **Quasi pieno** e **Pieno** e selezionare **Salva**. È possibile ripristinare i valori di soglia ai valori predefiniti consigliati: 80 per Quasi pieno e 90 per Pieno.

Gestire i backend di storage in ONTAP tools

I backend dello storage sono sistemi utilizzati dagli host ESXi per lo storage dei dati.

Rileva lo storage

È possibile eseguire l'individuazione di un backend di archiviazione su richiesta senza attendere un'individuazione pianificata per aggiornare immediatamente i dettagli di archiviazione. Per le configurazioni MetroCluster , eseguire manualmente la scoperta degli strumenti ONTAP dopo un passaggio.

Segui i passaggi riportati di seguito per scoprire i backend dello storage.

Fasi

1. Accedere al client vSphere.
2. Nella pagina Collegamenti, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Backend di archiviazione** e seleziona un backend di archiviazione.
4. Selezionare il menu ellissi verticali e selezionare **trova memoria**

È possibile tenere traccia dell'avanzamento nel pannello attività recenti.

Modificare i backend di archiviazione

È possibile modificare le credenziali del backend di archiviazione o il nome della porta. È anche possibile modificare il backend di archiviazione per i cluster ONTAP globali utilizzando ONTAP Tools Manager. Se il certificato scade entro 30 giorni o meno, gli strumenti ONTAP mostrano un avviso. Modificare il backend di archiviazione e caricare il nuovo certificato dall'amministratore ONTAP .

Quando si modifica il backend di archiviazione, gli ONTAP tools for VMware vSphere eseguono un'individuazione del backend di archiviazione per aggiornare i dettagli di archiviazione.

Per modificare un backend di archiviazione, attenersi alla procedura descritta in questa sezione.

1. Accedere al client vSphere.
2. Nella pagina Collegamenti, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP , vai su **Backend di archiviazione** e seleziona un backend di archiviazione.
4. Selezionare il menu ellissi verticali e selezionare **Modifica** per modificare le credenziali o il nome della porta. È possibile tenere traccia dell'avanzamento nel pannello attività recenti.

Modificare i cluster ONTAP globali con ONTAP Tools Manager come segue.

1. Avviare Gestione strumenti ONTAP da un browser Web:
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Seleziona i backend di storage dalla barra laterale.
4. Selezionare il backend di archiviazione che si desidera modificare.
5. Selezionare il menu ellissi verticali e selezionare **Modifica**.
6. È possibile modificare le credenziali o la porta. Immettere **Username** e **Password** per modificare il backend di archiviazione.

Rimuovere i backend di stoccaggio

Prima di rimuovere il backend di archiviazione, è necessario rimuovere tutti gli archivi dati collegati. Per rimuovere un backend di archiviazione, seguire i passaggi indicati di seguito.

1. Accedere al client vSphere.
2. Nella pagina Collegamenti, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro degli strumenti ONTAP, vai su **Backend di archiviazione** e seleziona un backend di archiviazione.
4. Selezionare il menu delle ellissi verticali e selezionare **Rimuovi**. Assicurarsi che il backend di archiviazione non contenga alcun archivio dati. È possibile monitorare i progressi nel pannello delle attività recenti.

Puoi eseguire l'operazione di rimozione per i cluster ONTAP globali usando ONTAP tools Manager.

1. Avviare Gestione strumenti ONTAP da un browser Web:
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **backend di archiviazione** dalla barra laterale.
4. Selezionare il backend di archiviazione che si desidera rimuovere
5. Selezionare il menu ellissi verticali e selezionare **Rimuovi**.

Drill-down del backend dello storage

Nella pagina del backend di archiviazione sono elencati tutti i backend di archiviazione. È possibile eseguire operazioni di individuazione, modifica e rimozione dell'archiviazione sui backend di archiviazione aggiunti, ma non sulla singola SVM figlio nel cluster.

Selezionare il cluster padre o figlio per visualizzare il riepilogo dei componenti. Per il cluster padre, utilizzare il menu a discesa delle azioni per individuare l'archiviazione, modificare o rimuovere il backend di archiviazione.

La pagina di riepilogo fornisce i seguenti dettagli:

- Stato del backend dello 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 l'SVM figlio, le informazioni sono le stesse del backend di archiviazione padre.
- Privileges consentiti e limitati per il backend di archiviazione. Per l'SVM figlio, le informazioni sono le stesse del backend di archiviazione padre. Gli strumenti ONTAP mostrano i privilegi solo sui backend di archiviazione basati su cluster. Se si aggiunge SVM come backend di archiviazione, le informazioni sui privilegi non vengono visualizzate.
- La visualizzazione dettagliata 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 SVM ASA R2, il portlet della capacità non è mostrato. Il portale della capacità è richiesto solo quando la proprietà disaggregata è impostata su "true" per la SVM o il cluster.
- Per i sistemi ASA R2 SVM, la sezione delle 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 aggregato.

Gestire le istanze di vCenter Server negli strumenti ONTAP

Le istanze di vCenter Server sono piattaforme di gestione centrali che consentono di controllare host, macchine virtuali e backend dello storage.

Dissociare i backend di storage con l'istanza di vCenter Server

La pagina dell'elenco di vCenter Server mostra il numero associato di backend storage. Ogni istanza di vCenter Server può essere associata o dissociata da un backend dello storage.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Seleziona l'istanza vCenter Server richiesta dalla barra laterale.
4. Seleziona i puntini di sospensione verticali su vCenter Server che desideri associare o dissociare dai backend di storage.
5. Selezionare **dissociare il backend di archiviazione**.

Modificare un'istanza di vCenter Server

Per modificare le istanze di vCenter Server, procedere come segue.

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Seleziona l'istanza vCenter Server applicabile dalla barra laterale
4. Selezionare le ellissi verticali a fronte di vCenter Server che si desidera modificare e selezionare **Modifica**.
5. Nella finestra **Modifica vCenter**, immettere il nome utente, la password e i dettagli della porta.

6. Carica il certificato e seleziona **Modifica**.

Rimuovere un'istanza di vCenter Server

Rimuovere tutti i backend di archiviazione dal vCenter Server prima di rimuoverlo.

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Seleziona le istanze vCenter Server applicabili dalla barra laterale
4. Selezionare le ellissi verticali del vCenter Server che si desidera rimuovere e selezionare **Rimuovi**.



Dopo aver rimosso le istanze di vCenter Server, queste non saranno più gestite dall'applicazione.

Quando si rimuovono le istanze di vCenter Server negli strumenti ONTAP, vengono eseguite automaticamente le seguenti azioni:

- Plug-in non registrato.
- I privilegi dei plug-in e i ruoli dei plug-in vengono rimossi.

Rinnova il certificato di vCenter Server

Gli strumenti ONTAP ti avvisano quando il certificato vCenter sta per scadere o è scaduto. Dopo aver rinnovato il certificato vCenter, caricare il nuovo certificato negli strumenti ONTAP seguendo i passaggi seguenti:

1. Accedere alla shell di diagnostica remota degli strumenti ONTAP .
2. Ottenere il certificato vCenter rinnovato dalla shell di diagnostica:

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN  
CERTIFICATE/,/END CERTIFICATE/p'
```

3. Assicurarsi che il certificato sia in formato Base 64 ASCII e includa le righe iniziali e finali, ad esempio:

Gestisci i certificati degli strumenti ONTAP

Per impostazione predefinita, durante la distribuzione viene generato un certificato autofirmato per gli strumenti ONTAP e VASA Provider. È possibile utilizzare l'interfaccia di ONTAP Tools Manager per rinnovare questo certificato o sostituirlo con un certificato CA personalizzato. Nelle distribuzioni multi-vCenter è obbligatorio utilizzare certificati CA personalizzati.

Prima di iniziare

Prima di iniziare, dovresti avere a disposizione quanto segue:

- Il nome di dominio mappato all'indirizzo IP virtuale.
- nslookup riuscito del nome di dominio, a conferma che la risoluzione avviene nell'indirizzo IP corretto.
- Certificati creati con il nome di dominio e l'indirizzo IP degli strumenti ONTAP .



Un indirizzo IP degli strumenti ONTAP deve corrispondere a un nome di dominio completo (FQDN). I certificati devono contenere lo stesso FQDN mappato all'indirizzo IP degli strumenti ONTAP in nomi alternativi oggetto o oggetto.



Non è possibile passare da un certificato CA firmato a un certificato autofirmato.

Aggiornare il certificato degli strumenti ONTAP

La scheda Strumenti di ONTAP mostra dettagli quali il tipo di certificato (autofirmato/CA firmato) e il nome di dominio. Durante la distribuzione, il certificato autofirmato viene generato per impostazione predefinita. È possibile rinnovare il certificato o aggiornarlo alla CA.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **certificati > ONTAP tools > Rinnova** per rinnovare i certificati.

È possibile rinnovare il certificato se è scaduto o si sta avvicinando alla data di scadenza. L'opzione di rinnovo è disponibile quando il tipo di certificato è firmato CA. Nella finestra a comparsa, fornire i dettagli relativi al certificato del server, alla chiave privata, alla CA principale e al certificato intermedio.



Il sistema non sarà in linea fino a quando il certificato non verrà rinnovato e l'utente verrà disconnesso dall'interfaccia di gestione degli strumenti ONTAP.

4. Per aggiornare il certificato autofirmato al certificato CA personalizzato, selezionare l'opzione **certificati > Strumenti ONTAP > Aggiorna a CA**.
 - a. Nella finestra a comparsa, caricare il certificato del server, la chiave privata del certificato del server, il certificato della CA principale e i file di certificato intermedi.
 - b. Inserisci il nome di dominio completo (FQDN) dell'IP del Load Balancer per il quale hai generato questo certificato e aggiorna il certificato.



Il sistema non sarà in linea fino al completamento dell'aggiornamento e l'utente verrà disconnesso dall'interfaccia di gestione degli strumenti ONTAP.

Aggiornare il certificato del provider VASA

I tool ONTAP per VMware vSphere vengono implementati con un certificato autofirmato per il provider VASA. Con questo, è possibile gestire solo un'istanza di vCenter Server per i datastore vVol. Quando si gestiscono più istanze di vCenter Server e si desidera attivare la funzionalità vVol, è necessario modificare il certificato autofirmato in un certificato CA personalizzato.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare **certificati > fornitore VASA o Strumenti ONTAP > Rinnova** per rinnovare i certificati.
4. Selezionare **certificati > Provider VASA o Strumenti ONTAP > Aggiorna a CA** per aggiornare il certificato autofirmato al certificato CA personalizzato.
 - a. Nella finestra a comparsa, caricare il certificato del server, la chiave privata del certificato del server, il certificato della CA principale e i file di certificato intermedi.
 - b. Inserisci il nome di dominio completo (FQDN) dell'IP del Load Balancer per il quale hai generato

questo certificato e aggiorna il certificato.



Il sistema non sarà in linea fino al completamento dell'aggiornamento e l'utente verrà disconnesso dall'interfaccia di gestione degli strumenti ONTAP.

Accedi ai tool ONTAP per la console di manutenzione di VMware vSphere


Scopri la console di manutenzione di ONTAP tools

La console di manutenzione per gli ONTAP tools for VMware vSphere consente di gestire le impostazioni di applicazioni, sistema e rete. È possibile aggiornare le password di amministratore e manutenzione, generare bundle di supporto, configurare i livelli di registro, gestire le impostazioni TLS e abilitare la diagnostica remota.

Dopo aver distribuito gli ONTAP tools for VMware vSphere, se la console di manutenzione non è accessibile, installare gli strumenti VMware da vCenter Server. Accedi utilizzando il `maint` nome utente e password impostati durante la distribuzione. Utilizzare **nano** per modificare i file nella console di manutenzione o di accesso root.



Impostare una password per `diag` utente durante l'attivazione della diagnostica remota.

Per accedere alla console di manutenzione, utilizzare la scheda **Riepilogo** degli strumenti ONTAP per VMware vSphere distribuiti. Quando si seleziona , viene avviata la console di manutenzione.

Menu console	Opzioni
Configurazione dell'applicazione	<ol style="list-style-type: none">1. Visualizza il riepilogo dello stato del server2. Modifica il livello LOG per i servizi degli strumenti ONTAP3. Cambia il flag di convalida del certificato
Configurazione del sistema	<ol style="list-style-type: none">1. Riavviare la macchina virtuale2. Arrestare la macchina virtuale3. Modificare la password utente "maint"4. Modificare il fuso orario5. Aumentare la dimensione del disco jail (/jail)6. Eseguire l'upgrade7. Installare VMware Tools

Configurazione di rete	<ol style="list-style-type: none"> 1. Visualizzare le impostazioni dell'indirizzo IP 2. Visualizzare le impostazioni di ricerca dei nomi di dominio 3. Modificare le impostazioni di ricerca dei nomi di dominio 4. Visualizza percorsi statici 5. Modificare i percorsi statici 6. Eseguire il commit delle modifiche 7. Eseguire il ping di un host 8. Ripristinare le impostazioni predefinite
Supporto e diagnostica	<ol style="list-style-type: none"> 1. Accedere alla shell di diagnostica 2. Abilitare l'accesso remoto alla diagnostica 3. Fornisci le credenziali vCenter per il backup 4. Esegui backup

Configurare l'accesso diagnostico remoto per ONTAP tools

È possibile configurare i tool ONTAP per VMware vSphere per abilitare l'accesso SSH per l'utente diag.

Prima di iniziare

Abilita l'estensione VASA Provider per la tua istanza di vCenter Server.

A proposito di questa attività

L'utilizzo di SSH per accedere all'account utente DIAG presenta le seguenti limitazioni:

- è consentito un solo account di accesso per ogni attivazione di SSH.
- L'accesso SSH all'account utente DIAG viene disattivato quando si verifica una delle seguenti condizioni:

- Il tempo scade.

La sessione di accesso scade a mezzanotte del giorno successivo.

- Si accede nuovamente come utente di DIAG utilizzando SSH.

Fasi

1. Dal server vCenter, aprire una console per il provider VASA.
2. Accedere come utente di manutenzione.
3. Immettere 4 per selezionare **supporto e diagnostica**.
4. Entra 2 per selezionare **Abilita accesso alla diagnostica remota**.
5. Invio y Nella finestra di dialogo Confirmation (Conferma) per abilitare l'accesso remoto alla diagnostica.
6. Inserire una password per l'accesso remoto alla diagnostica.

Avvia SSH sugli altri nodi di ONTAP tools

Prima di eseguire l'aggiornamento, è necessario avviare SSH su altri nodi.

Prima di iniziare

Abilita l'estensione VASA Provider per la tua istanza di vCenter Server.

A proposito di questa attività

Ripetere questa procedura su ciascun nodo prima di effettuare l'aggiornamento.

Fasi

1. Dal server vCenter, aprire una console per il provider VASA.
2. Accedere come utente di manutenzione.
3. Invio 4 Per selezionare Support and Diagnostics (supporto e diagnostica).
4. Invio 1 Per selezionare Accedi alla shell diagnostica.
5. Invio y per procedere.
6. Eseguire il comando `sudo systemctl restart ssh`.

Aggiorna le credenziali del server vCenter negli ONTAP tools

È possibile aggiornare le credenziali dell'istanza di vCenter Server tramite la console di manutenzione.

Prima di iniziare

È necessario disporre delle credenziali di accesso per gli utenti di manutenzione.

A proposito di questa attività

Se hai modificato le credenziali di vCenter Server dopo la distribuzione, aggiornale utilizzando questa procedura.

Fasi

1. Dal server vCenter, aprire una console per il provider VASA.
2. Accedere come utente di manutenzione.
3. Inserire 2 per selezionare il menu Configurazione di sistema.
4. Entra 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). È possibile impostare il flag di convalida del certificato back-end di archiviazione ONTAP su false se è necessario ignorare i controlli del certificato SAN. Questa impostazione non è applicabile ai certificati di vCenter Server.

Prima di iniziare

È necessario disporre delle credenziali di accesso per gli utenti di manutenzione.

Fasi

1. Da vCenter Server, aprire una console agli strumenti ONTAP.
2. Accedere come utente di manutenzione.
3. Entra 1 per selezionare il menu **Configurazione applicazione**.
4. Entra 3 per modificare il flag di convalida del certificato.

La console di manutenzione mostra lo stato del flag di convalida del certificato e richiede di modificarlo.

5. Inserisci 'y' per attivare/disattivare il flag oppure 'n' per annullare.

Quando si abilita il flag di convalida del certificato (impostato su true), gli strumenti ONTAP verificano che tutti i backend di archiviazione utilizzino certificati con un nome alternativo del soggetto (SAN). Se un backend utilizza un certificato senza SAN, non è possibile abilitare la convalida del certificato. Prima di abilitare questo flag, verificare che tutti i backend di archiviazione utilizzino certificati basati su SAN. Se si disabilita il flag di convalida del certificato (impostato su false), gli strumenti ONTAP ignorano la convalida del certificato per tutti i backend di archiviazione 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.

Report sui tool ONTAP

I tool ONTAP per il plug-in VMware vSphere forniscono report su macchine virtuali e datastore. Quando si seleziona l'icona degli strumenti NetApp ONTAP per il plug-in VMware vSphere nella sezione Collegamenti del client vCenter, l'interfaccia utente passa alla pagina Panoramica. Selezionare la scheda rapporti per visualizzare la macchina virtuale e il report degli archivi dati.

Il report Macchine virtuali mostra l'elenco delle macchine virtuali rilevate (dovrebbero avere almeno un disco da datastore basati su storage ONTAP) con metriche delle prestazioni. Quando si espande il record della VM, l'interfaccia visualizza tutte le informazioni relative al datastore relative al disco.

Il report sui datastore elenca gli ONTAP tools for VMware vSphere rilevati o riconosciuti che utilizzano qualsiasi storage ONTAP , con metriche delle prestazioni.

È possibile utilizzare l'opzione Gestisci colonne per nascondere o visualizzare colonne diverse.

Gestire le macchine virtuali

Considerazioni sulla migrazione e la clonazione di macchine virtuali per ONTAP tools

È importante tenere presenti alcune considerazioni relative alla migrazione delle macchine virtuali esistenti nel data center.

Migrazione di macchine virtuali protette

È possibile migrare le macchine virtuali protette in:

- Stesso datastore vVol in un host ESXi diverso
- Datastore vVol compatibile diverso nello stesso host ESXi
- Datastore vVol compatibile diverso in un host ESXi diverso

Se si migra la macchina virtuale su un FlexVol volume diverso, il sistema aggiorna il file di metadati per quel volume con le informazioni sulla macchina virtuale. Se una macchina virtuale viene migrata su un host ESXi diverso ma con lo stesso storage, il file di metadati FlexVol volume sottostante non verrà modificato.

Clonare macchine virtuali protette

È possibile clonare le macchine virtuali protette nei seguenti modi:

- Stesso container dello stesso volume FlexVol che utilizza un gruppo di replica

Il file di metadati dello stesso volume FlexVol viene aggiornato con i dettagli della macchina virtuale clonata.

- Stesso container di un volume FlexVol diverso che utilizza un gruppo di replica

Il volume FlexVol in cui viene posizionata la macchina virtuale clonata, il file di metadati viene aggiornato con i dettagli della macchina virtuale clonata.

- Datastore di vVol o container diverso

Il volume FlexVol in cui viene posizionata la macchina virtuale clonata, il file di metadati viene aggiornato con i dettagli della macchina virtuale.

Attualmente VMware non supporta macchine virtuali clonate in un modello VM.

È supportato il clone di una macchina virtuale protetta.

Per ulteriori dettagli, fare riferimento ["Creazione di una macchina virtuale per la clonazione"](#) a.

Snapshot delle macchine virtuali

Attualmente sono supportate solo le istantanee delle macchine virtuali senza memoria. Se la macchina virtuale dispone di Snapshot con memoria, la macchina virtuale non viene presa in considerazione per la protezione.

Non è inoltre possibile proteggere macchine virtuali non protette dotate di snapshot di memoria. Per questa versione, è previsto che tu elimini lo snapshot della memoria prima di abilitare la protezione per la macchina virtuale.

Per una VM Windows con tipo di archiviazione ASA r2, uno snapshot della macchina virtuale è di sola lettura. Quando si accende la VM, VASA Provider crea una LUN dallo snapshot di sola lettura e abilita gli IOPS. Quando si spegne la VM, VASA Provider elimina la LUN e disabilita gli IOPS.

Migrare le macchine virtuali negli archivi dati vVols in ONTAP tools

È possibile migrare le macchine virtuali dai datastore NFS e VMFS ai datastore Virtual Volumes (vVol), per sfruttare la gestione delle macchine virtuali basata su policy e altre funzionalità vVol. I datastore di vVol consentono di soddisfare i requisiti di carico di lavoro più elevati.

Prima di iniziare

Assicurarsi che il provider VASA non sia in esecuzione su nessuna delle macchine virtuali che si intende migrare. Se si esegue la migrazione di una macchina virtuale che esegue VASA Provider in un datastore vVols, non è possibile eseguire alcuna operazione di gestione, inclusa l'accensione delle macchine virtuali presenti negli archivi dati vVols.

A proposito di questa attività

Quando esegui la migrazione da un datastore NFS e VMFS a un datastore vVol, vCenter Server utilizza le API vStorage per l'integrazione degli array (VAAI) per eseguire l'offload del carico durante lo spostamento dei dati dai datastore VMFS, ma non da un file NFS VMDK. Gli offload VAAI riducono normalmente il carico sull'host.

Fasi

1. Fare clic con il pulsante destro del mouse sulla macchina virtuale da migrare e selezionare **Migra**.
2. Selezionare **Cambia solo memoria**, quindi selezionare **Avanti**.
3. Selezionare un formato di disco virtuale, una policy di archiviazione della VM e un datastore vVol che corrispondano alle funzionalità del datastore che si sta migrando.
4. Controllare le impostazioni e selezionare **fine**.

Pulisci le configurazioni VASA negli ONTAP tools

Per completare il processo di bonifica VASA, seguire questi passaggi.



Si consiglia di rimuovere tutti i datastore vVols prima di avviare la pulizia VASA.

Fasi

1. Annullare la registrazione del plug-in accedendo a https://OTV_IP:8143/Register.html
2. Verificare che il plug-in non sia più disponibile su vCenter Server.
3. Chiudi i tool ONTAP per VMware vSphere VM.
4. Elimina i tool ONTAP per VMware vSphere VM.

Collegare o scollegare un disco dati da una VM in ONTAP tools

Seguire questi passaggi per collegare o scollegare i dischi dati dalle macchine virtuali in vSphere e gestirne le risorse di archiviazione.

Collegare un disco dati a una macchina virtuale

Collega un disco dati a una macchina virtuale per aggiungere ulteriore spazio di archiviazione.

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su una macchina virtuale nell'inventario e selezionare **Modifica impostazioni**.
3. Nella scheda **hardware virtuale**, selezionare **disco rigido esistente**.
4. Selezionare la macchina virtuale in cui si trova il disco.
5. Selezionare il disco che si desidera collegare e fare clic sul pulsante **OK**.

Risultato

Il disco rigido viene visualizzato nell'elenco Virtual hardware Devices (periferiche hardware virtuali).

Scollegare un disco dati dalla macchina virtuale

Scollega un disco dati da una macchina virtuale quando non ti serve più. Il disco non viene eliminato, ma rimane nel sistema di archiviazione ONTAP .

Fasi

1. Accedere al client vSphere.
2. Fare clic con il pulsante destro del mouse su una macchina virtuale nell'inventario e selezionare **Modifica impostazioni**.
3. Spostare il puntatore sul disco e selezionare **Rimuovi**.



Il disco viene rimosso dalla macchina virtuale. Se altre macchine virtuali condividono il disco, i file del disco non vengono eliminati.

Informazioni correlate

["Aggiungere un nuovo disco rigido a una macchina virtuale"](#)

["Aggiungere un disco rigido esistente a una macchina virtuale"](#)

Scopri i sistemi di archiviazione e gli host negli ONTAP tools

Quando gli ONTAP tools for VMware vSphere vengono avviati per la prima volta in vSphere Client, rilevano automaticamente gli host ESXi, i LUN associati e le esportazioni NFS, nonché i sistemi di storage NetApp che possiedono tali risorse.

Prima di iniziare

- Assicurarsi che tutti gli host ESXi siano accesi e connessi.
- Assicurarsi che tutte le macchine virtuali di archiviazione (SVM) da rilevare siano in esecuzione e che ogni nodo del cluster disponga di almeno un LIF dati configurato per il protocollo di archiviazione in uso (NFS o iSCSI).

A proposito di questa attività

È possibile scoprire nuovi sistemi di archiviazione o aggiornare quelli esistenti per ottenere i dettagli più recenti su capacità e configurazione. È anche possibile modificare gli ONTAP tools for VMware vSphere per l'accesso al sistema di storage.

Durante il rilevamento dei sistemi storage, i tool di ONTAP per VMware vSphere raccolgono informazioni dagli host ESXi gestiti dall'istanza di vCenter Server.

Fasi

1. Dalla home page di vSphere Client, selezionare **host e cluster**.
2. Fare clic con il pulsante destro del mouse sul data center desiderato e selezionare **Strumenti NetApp ONTAP * > *Aggiorna dati host**.

Nella finestra di dialogo **Conferma**, confermare la scelta.

3. Selezionare i controller di archiviazione rilevati che hanno lo stato `Authentication Failure` e selezionare **azioni > Modifica**.
4. Inserire le informazioni richieste nella finestra di dialogo **Modify Storage System** (Modifica sistema di storage).
5. Ripetere i passaggi 4 e 5 per tutti i controller storage con `Authentication Failure` stato.

Al termine del processo di rilevamento, eseguire le seguenti operazioni:

- Utilizzare gli strumenti ONTAP per 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.
- Fornire le credenziali del sistema storage.

Modificare le impostazioni degli host ESXi utilizzando gli strumenti ONTAP

Utilizzare la dashboard degli strumenti ONTAP in VMware vSphere per identificare i problemi di configurazione, selezionare gli host ESXi, rivedere le impostazioni consigliate NetApp e applicarle.

Prima di iniziare

Il portlet dei sistemi host ESXi visualizza i problemi con le impostazioni dell'host ESXi. Seleziona un problema per visualizzare il nome host o l'indirizzo IP.

Fasi

1. Accedere al client vSphere.
2. Nella pagina Collegamenti, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Accedere al portlet **ESXi host compliance** nella Panoramica (dashboard) degli strumenti ONTAP per il plug-in VMware vSphere.
4. Selezionare il collegamento **Applica impostazioni consigliate**.
5. Nella finestra **Applica impostazioni host consigliate**, seleziona gli host per i quali desideri utilizzare le impostazioni host consigliate NetApp e seleziona **Avanti**.



È possibile espandere l'host ESXi per visualizzare i valori correnti.

6. Nella pagina delle impostazioni, selezionare i valori consigliati secondo necessità.
7. Nel pannello di riepilogo, controllare i valori e selezionare **fine**. È possibile tenere traccia dell'avanzamento nel riquadro attività recenti.

Informazioni correlate

["Configurare le impostazioni dell'host ESXi"](#)

Gestire le password

Modificare la password del gestore strumenti ONTAP

È possibile modificare la password dell'amministratore utilizzando ONTAP Tools Manager.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedi con i tuoi ONTAP tools for VMware vSphere .
3. Selezionare l'icona **amministratore** nell'angolo superiore destro della schermata e selezionare **Modifica password**.
4. Nella finestra pop-up per cambiare la password, inserisci la vecchia e la nuova password. La schermata dell'interfaccia utente mostra i requisiti della password.
5. Selezionare **Modifica** per applicare le modifiche.

Reimpostare la password di gestione degli strumenti ONTAP

Se si dimentica la password di ONTAP Tools Manager, è possibile ripristinare l'accesso amministratore utilizzando un token di reimpostazione generato dalla console di manutenzione ONTAP tools for VMware vSphere .

Fasi

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. Generare un token di reimpostazione della password utilizzando gli ONTAP tools for VMware vSphere :
 - a. Accedere al vCenter Server e aprire la console di manutenzione.
 - b. Entra 2 per selezionare **Configurazione di sistema**.
 - c. Entra 3 per selezionare **Cambia password utente 'maint'**.
4. Nella finestra di dialogo per la reimpostazione della password, immettere il token di reimpostazione, il nome utente e la nuova password.
5. Selezionare **Reimposta** per aggiornare le credenziali.
6. Accedi a ONTAP Tools Manager con la nuova password.

Reimposta la password utente dell'applicazione in ONTAP tools

Seguire questi passaggi per reimpostare la password utente dell'applicazione necessaria per la registrazione del provider SRA e VASA con vCenter Server utilizzando gli ONTAP tools for VMware vSphere.

Fasi

1. Apri un browser web e vai su: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Accedere utilizzando le credenziali di amministratore configurate durante la distribuzione degli strumenti ONTAP .
3. Dalla barra laterale, seleziona **Impostazioni**.
4. Nella pagina **Credenziali VASA/SRA**, seleziona **Reimposta password**.
5. Inserisci e conferma la nuova password.
6. Selezionare **Reimposta** per applicare la nuova password.

Reimposta la password della console di manutenzione di ONTAP tools

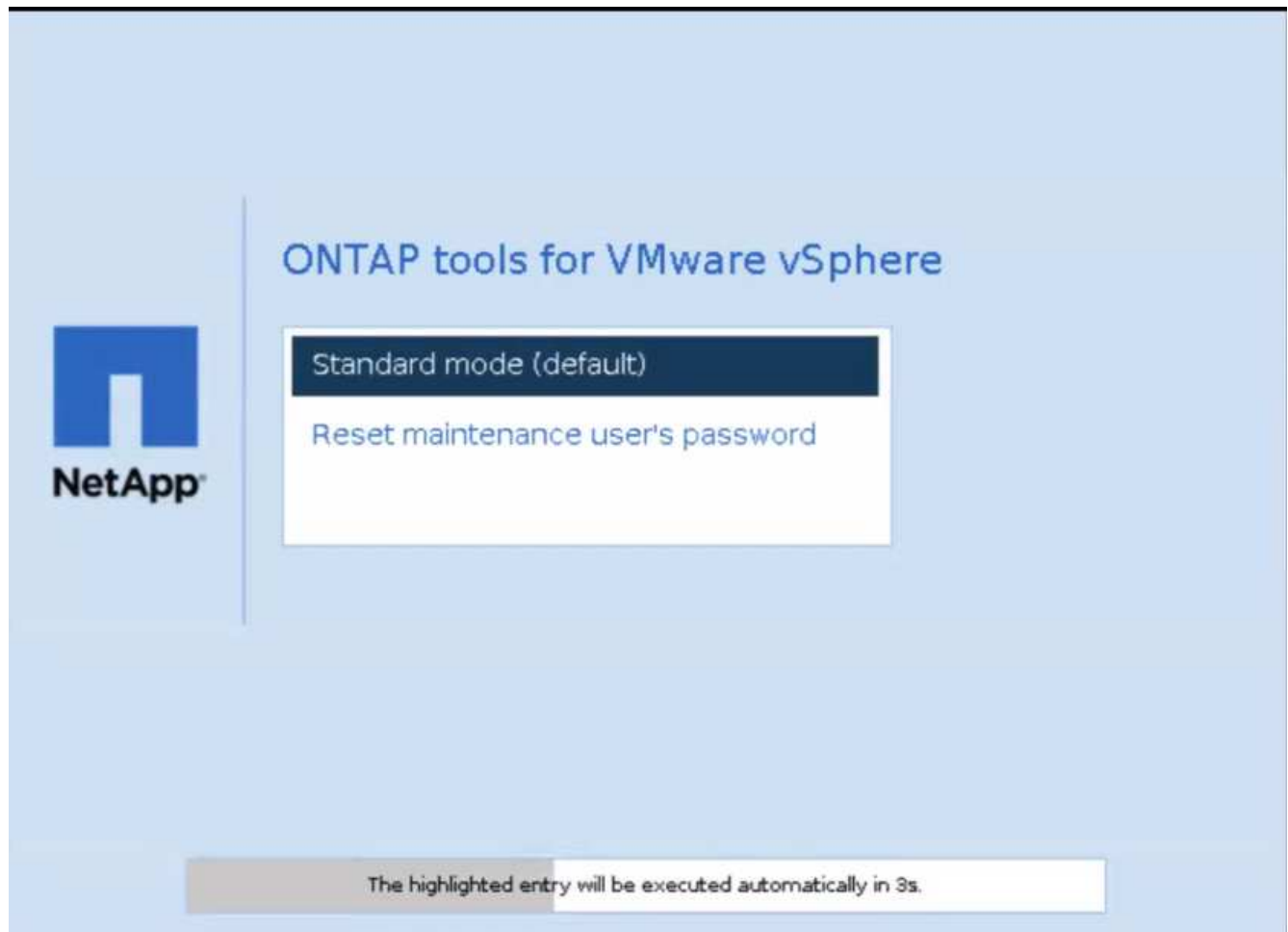
Durante l'operazione di riavvio del sistema operativo guest, il menu GRUB visualizza un'opzione per reimpostare la password utente della console di manutenzione. Utilizzare questa opzione per aggiornare la password utente della console di manutenzione sulla VM. Dopo aver reimpostato la password, la macchina virtuale 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 gli ONTAP tools for VMware vSphere HA, è necessario modificare la password utente della console di manutenzione sul nodo di gestione degli strumenti ONTAP , ovvero node1.

Fasi

1. Accedere a vCenter Server
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **alimentazione > Riavvia sistema operativo guest**
Durante il riavvio del sistema, viene visualizzata la seguente schermata:



Hai 5 secondi per scegliere la tua opzione. Premere un tasto qualsiasi per interrompere l'avanzamento e bloccare il menu di GRUB.

3. Selezionare l'opzione **Reimposta password utente manutenzione**. Si apre la console di manutenzione.
4. Nella console, inserisci e conferma la nuova password. Hai tre tentativi. Il sistema si riavvia dopo aver inserito correttamente la nuova password.
5. Premere **Invio** per continuare. Il sistema aggiorna la password sulla VM.



Lo stesso menu GRUB viene visualizzato anche durante l'accensione della VM. Tuttavia, dovresti utilizzare l'opzione di reimpostazione della password solo con l'opzione **Riavvia sistema operativo guest**.

Gestire la protezione dei cluster di host

Modificare un cluster host protetto in ONTAP tools

È possibile 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.
- Aggiungere nuove relazioni SnapMirror alle impostazioni di protezione.
- Elimina le relazioni SnapMirror esistenti dalle impostazioni di protezione.

- Modificare una relazione SnapMirror esistente.



Dopo aver creato, modificato o eliminato la protezione per un cluster host, è necessario eseguire l'individuazione dello storage per riflettere le modifiche. Se non si esegue la rilevazione dello storage, le modifiche vengono riflesse dopo l'attivazione della rilevazione periodica dello storage.

Monitoraggio della protezione dei cluster host

Monitorare lo stato di protezione, le relazioni SnapMirror, gli archivi dati e lo stato SnapMirror per ciascun cluster host protetto.

Fasi

1. Accedere al client vSphere.
2. Vai a **Strumenti NetApp ONTAP * > *Protezione > Relazioni cluster host**.

Nella colonna Protezione viene visualizzata un'icona che mostra lo stato della protezione.

3. Passare il mouse sull'icona per visualizzare ulteriori dettagli.

Aggiungere nuovi datastore o host

Aggiungere host o creare datastore sul cluster protetto utilizzando l'interfaccia utente di vCenter.

Fasi

1. Accedere al client vSphere.
2. Per modificare le proprietà di un cluster protetto, è possibile effettuare una delle seguenti operazioni
 - a. Vai a **Strumenti NetApp ONTAP * > *Protezione > Relazioni cluster host**, seleziona il menu con i puntini di sospensione accanto al cluster e seleziona **Modifica** o
 - b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Se si crea un datastore nell'interfaccia utente di vCenter, questo appare come non protetto. È possibile visualizzare tutti i datastore nel cluster e il loro stato di protezione in una finestra di dialogo. Selezionare il pulsante **Proteggi** per abilitare la protezione.



Dopo aver creato un datastore nell'interfaccia utente di vCenter Server, selezionare **Scopri** nella pagina di panoramica per visualizzare il datastore come candidato per la protezione nel cluster host. Lo stato di protezione viene aggiornato in protetto dopo la successiva rilevazione periodica della protezione.

4. Se si aggiunge un nuovo host ESXi, lo stato di protezione viene visualizzato come parzialmente protetto. Selezionare il menu con i puntini di sospensione nelle impostazioni SnapMirror e selezionare **Modifica** per impostare la prossimità dell'host ESXi appena aggiunto.



Per le relazioni asincrone, la modifica non è supportata negli strumenti ONTAP perché l'SVM di destinazione per un sito terziario non può essere aggiunto alla stessa istanza. Per modificare la configurazione della relazione, utilizzare System Manager o la CLI sulla SVM di destinazione.

5. Dopo aver apportato le modifiche, seleziona **Salva**.

6. Le modifiche sono visibili nella finestra **Proteggi cluster**.

Gli strumenti ONTAP creano un'attività vCenter e puoi monitorarne l'avanzamento nel pannello **Attività recente**.

Aggiungi una nuova relazione SnapMirror

Fasi

1. Accedere al client vSphere.
2. Per modificare le proprietà di un cluster protetto, è possibile effettuare una delle seguenti operazioni
 - a. Vai a **Strumenti NetApp ONTAP * > *Protezione > Relazioni cluster host**, seleziona il menu con i puntini di sospensione sul cluster e seleziona **Modifica** o
 - b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Selezionare **Aggiungi relazione**.
4. Aggiungere una nuova relazione come tipo di criterio **Asynchronous** o **AutomatedFailOverDuplex**.
5. Selezionare **Proteggi**.

Le modifiche sono visibili nella finestra **Proteggi cluster**.

Gli strumenti ONTAP creano un'attività vCenter e puoi monitorarne l'avanzamento nel pannello **Attività recente**.

Eliminare una relazione SnapMirror esistente

Per eliminare una relazione asincrona SnapMirror, assicurarsi che il sito secondario SVM o cluster sia aggiunto come backend di archiviazione negli ONTAP tools for VMware vSphere. Non è possibile eliminare tutte le relazioni SnapMirror contemporaneamente. L'eliminazione di una relazione comporta anche la rimozione della relazione corrispondente dal cluster ONTAP. Quando si elimina una relazione Automated Failover Duplex SnapMirror, il sistema annulla la mappatura dei datastore di destinazione ed elimina il gruppo di coerenza, i LUN, i volumi e gli iGroup dal cluster ONTAP di destinazione.

Quando si elimina la relazione, il sistema esegue nuovamente la scansione del sito secondario per rimuovere la LUN non mappata come percorso attivo dagli host.

Fasi

1. Accedere al client vSphere.
2. Per modificare le proprietà di un cluster protetto, è possibile effettuare una delle seguenti operazioni
 - a. Vai a **Strumenti NetApp ONTAP * > *Protezione > Relazioni cluster host**, seleziona il menu con i puntini di sospensione sul cluster e seleziona **Modifica** o
 - b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Selezionare il menu puntini di sospensione nelle impostazioni SnapMirror e selezionare **Elimina**.
 - Se si elimina una relazione basata sul tipo di policy asincrona di un cluster host protetto, è necessario rimuovere manualmente gli elementi di archiviazione dal cluster di archiviazione terziario. Gli elementi di archiviazione includono gruppi di coerenza, volumi (per i sistemi ONTAP), unità di archiviazione (LUN/namespace) e snapshot.
 - Se si elimina una relazione basata su policy Automated Failover Duplex (AFD) di un cluster host

protetto, è possibile scegliere di rimuovere gli elementi di archiviazione associati sull'archiviazione secondaria direttamente dall'interfaccia.

- Se si elimina una relazione basata su criteri AFD (Automated Failover Duplex) 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, eliminare gli elementi di archiviazione associati nell'archiviazione secondaria. Se non vengono rimossi, rimangono nel sito secondario.

Gli strumenti ONTAP creano un'attività vCenter e puoi monitorarne l'avanzamento nel pannello **Attività recente**.

Modificare una relazione SnapMirror esistente

Per modificare una relazione asincrona SnapMirror, assicurarsi che il sito secondario SVM o cluster sia aggiunto come backend di archiviazione negli ONTAP tools for VMware vSphere. Per le relazioni Automated Failover Duplex SnapMirror, è possibile aggiornare la prossimità dell'host per configurazioni uniformi o l'accesso dell'host per configurazioni non uniformi. Non è supportato il passaggio tra i tipi di policy Duplex di failover asincrono e automatico. È possibile configurare le impostazioni di prossimità o di accesso per gli host appena scoperti nel cluster.



Non è possibile modificare una relazione asincrona SnapMirror esistente.

Fasi

1. Accedere al client vSphere.
2. Per modificare le proprietà di un cluster protetto, è possibile effettuare una delle seguenti operazioni
 - a. Vai a **Strumenti NetApp ONTAP * > *Protezione > Relazioni cluster host**, seleziona il menu con i puntini di sospensione sul cluster e seleziona **Modifica** o
 - b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **Strumenti NetApp ONTAP * > *Proteggi cluster**.
3. Se è selezionato il tipo di policy AutomatedFailOverDuplex, aggiungere i dettagli di prossimità dell'host o di accesso all'host.
4. Selezionare il pulsante **Proteggi**.

Gli strumenti ONTAP creano un'attività vCenter. Segui i progressi nel pannello **Attività recenti**.

Rimuovere la protezione del cluster host negli ONTAP tools

Quando si rimuove la protezione dei cluster di host, i datastore diventano non protetti.

Fasi

1. Per visualizzare l'elenco dei cluster host protetti, andare su **Strumenti NetApp ONTAP * > *Protezione > Relazioni tra cluster host**.

In questa pagina è possibile monitorare i cluster host protetti, lo stato di protezione, la relazione SnapMirror e lo stato. Selezionare i gruppi di coerenza per visualizzare la capacità, gli archivi dati associati e i gruppi figlio.

2. Nella finestra **Protezione cluster host**, selezionare il menu con i puntini di sospensione accanto al cluster e selezionare **Rimuovi protezione**.
 - Se si rimuove la protezione da un cluster host con solo una relazione asincrona SnapMirror, è necessario eliminare manualmente gli elementi di archiviazione. Gli elementi di archiviazione includono

gruppi di coerenza, volumi (per il sistema ONTAP), unità di archiviazione (LUN) e snapshot.

- Se si rimuove la protezione da un cluster host con solo una relazione di policy SnapMirror basata su duplex di failover automatizzato e un gruppo di coerenza non gerarchico, è possibile eliminare gli elementi di archiviazione associati sull'archiviazione secondaria direttamente dalla stessa schermata.
- Se si rimuove la protezione da un cluster host con criteri SnapMirror e un gruppo di coerenza gerarchica per i backup, viene visualizzato un avviso relativo agli impatti sui backup. Conferma per procedere. Dopo la conferma, eliminare gli elementi di archiviazione associati nell'archiviazione secondaria. Se non si esegue la pulizia, gli elementi di archiviazione rimangono nel sito secondario.

Ripristina la configurazione degli strumenti ONTAP

A partire dagli ONTAP tools for VMware vSphere 10.5, la funzionalità di backup è abilitata per impostazione predefinita.

Il datastore in cui vengono distribuiti gli ONTAP tools for VMware vSphere memorizza i file di backup. Una cartella denominata in base all'indirizzo IP degli strumenti ONTAP (i punti sono sostituiti da caratteri di sottolineatura e con il 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 informativo (*OTV_backup_info.txt*) che contiene il nome dell'ultimo backup.

Assicurarsi che la nuova macchina virtuale utilizzi lo stesso indirizzo IP degli strumenti ONTAP e corrisponda alla configurazione iniziale del sistema, inclusi i servizi abilitati, le dimensioni del nodo e la modalità HA.

Fasi

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 per la macchina virtuale.
 - b. Selezionare la sezione **file**.
 - c. Scarica la directory di backup richiesta.
2. Spegnerla macchina virtuale esistente. Quindi, distribuisci una nuova macchina virtuale utilizzando lo stesso file OVA della distribuzione originale.
3. Da vCenter Server, aprire la console di manutenzione.
4. Accedere come utente di manutenzione.
5. Immettere 4 per selezionare **supporto e diagnostica**.
6. Immettere 2 per selezionare l'opzione **attiva accesso diagnostico remoto** e creare una nuova password per l'accesso diagnostico.
7. Scegli un file di backup dalla directory scaricata. Fare riferimento al file *OTV_backup_info.txt* per identificare il backup più recente.
8. Utilizzare il seguente comando per trasferire il file di backup sulla nuova macchina virtuale. Quando richiesto, immettere la password 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) menzionati nel comando.

9. Dopo aver trasferito il file di backup, accedi alla shell di 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 aver completato il ripristino, gli strumenti ONTAP ripristinano i servizi e gli oggetti vCenter.

Disinstallare ONTAP tools

La disinstallazione degli strumenti ONTAP per VMware vSphere elimina tutti i dati presenti negli strumenti.

Fasi

1. Rimuovere o spostare tutte le macchine virtuali dai tool ONTAP per datastore gestiti da VMware vSphere.
 - Per rimuovere le macchine virtuali, fare riferimento alla ["Rimuovere e registrare nuovamente le macchine virtuali e i modelli VM"](#)
 - Per spostarli in un datastore non gestito, fare riferimento a ["Come migrare la tua macchina virtuale con Storage vMotion"](#)
2. ["Elimina datastore"](#) Creato su tool ONTAP per VMware vSphere.
3. Se hai abilitato il provider VASA, seleziona **Impostazioni > Impostazioni provider VASA > Annulla registrazione** negli strumenti ONTAP per annullare la registrazione dei provider VASA da tutti i server vCenter.
4. Disassociare tutti i backend di storage dall'istanza di vCenter Server. Fare riferimento alla ["Dissociare i backend di storage con l'istanza di vCenter Server"](#).
5. Eliminare tutti i backend di archiviazione. Fare riferimento alla ["Gestire i back-end dello storage"](#).
6. Rimuovere l'adattatore SRA da VMware Live Site Recovery:
 - a. Accedere come amministratore all'interfaccia di gestione dell'appliance VMware Live Site Recovery utilizzando la porta 5480.
 - b. Selezionare **schede di replica archiviazione**.
 - c. Selezionare la scheda SRA appropriata, quindi scegliere **Elimina** dal menu a discesa.
 - d. Verificare di conoscere i risultati dell'eliminazione della scheda e selezionare **Elimina**.
7. Elimina le istanze del server vCenter integrate negli strumenti ONTAP per VMware vSphere. Fare riferimento alla ["Gestire le istanze di vCenter Server"](#).
8. Spegnerne gli strumenti ONTAP per le VM VMware vSphere da vCenter Server ed eliminare le VM.

Cosa succederà?

["Rimuovere i volumi FlexVol"](#)

Rimuovere i volumi FlexVol dopo aver disinstallato ONTAP tools

Se utilizzi un cluster ONTAP dedicato per i tool ONTAP per l'implementazione di VMware,

creerai molti volumi FlexVol non utilizzati. Dopo aver rimosso i tool ONTAP per VMware vSphere, occorre rimuovere i volumi FlexVol per evitare possibili impatti sulle performance.

Fasi

1. Scopri gli ONTAP tools for VMware vSphere dal nodo di gestione degli strumenti ONTAP VM. Eseguire 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, eliminare anche igroup.

2. Ottieni l'elenco dei volumi FlexVol . `kubectl describe persistentvolumes | grep internalName | awk -F='{' '{print $2}'`
3. Rimuovere le macchine virtuali da vCenter Server. Fare riferimento alla ["Rimuovere e registrare nuovamente le macchine virtuali e i modelli VM"](#).
4. Eliminare i volumi FlexVol . Fare riferimento a ["Eliminare un volume FlexVol"](#) . Per eliminare un volume, immettere il nome esatto FlexVol volume nel comando CLI.
5. Eliminare gli igroup SAN dal sistema di storage ONTAP in caso di distribuzione iSCSI. Fare riferimento alla ["Visualizza e gestisci GLI iniziatori SAN e igroups"](#).

Aggiorna i tool ONTAP per VMware vSphere

Aggiornamento dagli ONTAP tools for VMware vSphere 10.x alla versione 10.5

È possibile effettuare l'aggiornamento dagli ONTAP tools for VMware vSphere 10.3 o 10.4 alla versione 10.5. Tuttavia, per eseguire l'aggiornamento dagli strumenti ONTAP 10.0, 10.1 o 10.2 alla versione 10.5, è necessario prima eseguire l'aggiornamento alla versione 10.3 o 10.4 prima di procedere alla versione 10.5.



- Per i sistemi ASA r2, assicurarsi di eseguire l'aggiornamento agli ONTAP tools for VMware vSphere alla versione 10.5 e ONTAP alla versione 9.16.1, prima di configurare altre zone di disponibilità dello storage (SAZ).
- Se l'aggiornamento dagli ONTAP tools for VMware vSphere 10.3 o 10.4 alla versione 10.5 non riesce, non è possibile eseguire il rollback. Utilizzare un RPO basso o un ripristino snapshot per ripristinare la configurazione. Per gli ONTAP tools for VMware vSphere 10.2 e versioni precedenti, utilizzare zero-RPO per ripristinare la configurazione.

Prima di iniziare

- Assicurarsi che tutti i nodi siano attivi.
- Assicurarsi che il certificato del 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.
- Verificare che la configurazione del nodo corrisponda alle specifiche riportate nella tabella seguente.

Tipo di implementazione	CPU (core) per nodo	Memoria (GB) per nodo	Spazio su disco (GB) per nodo	CPU totale (core)	Memoria (GB)	Spazio su disco totale (GB)
Non ha Small	9	18	350	9	18	350
Terreno non ha	13	26	350	13	26	350
HA piccolo	9	18	350	27	54	1050
HA Media	13	26	350	39	78	1050
HA grande	17	34	350	51	102	1050

- Assicurarsi che il plug-in a caldo per CPU e RAM sia abilitato.
- Abilita il backup con RPO basso e assicurati che un backup sia visibile nell'interfaccia di vCenter Client. Scaricare la cartella di backup prima dell'aggiornamento.
- Si consiglia un backup con RPO basso. Tuttavia, in una distribuzione non HA, è possibile eseguire uno snapshot inattivo della macchina virtuale degli strumenti ONTAP prima dell'aggiornamento.

Fare riferimento a ["Modifica le impostazioni di backup"](#) E ["Ripristina la configurazione degli strumenti ONTAP"](#) per maggiori informazioni su backup e ripristino.

Fasi

1. Carica gli strumenti ONTAP per l'aggiornamento ISO di VMware vSphere nella libreria di contenuti.
2. Nella pagina della VM primaria, seleziona **Azioni > Modifica impostazioni**. Per identificare il nome della VM primaria:
 - a. Abilita la shell diag su qualsiasi nodo
 - b. Eseguire il seguente comando:

```
grep sourceHost /opt/netapp/meta/ansible_vars.yaml
```
3. Selezionare il **file ISO della libreria di contenuti** nella finestra di modifica delle impostazioni sotto il campo **Unità CD/DVD**.
4. Selezionare il file ISO, selezionare la casella **Connesso** per il campo **Unità CD/DVD** e fare clic su **OK**.
5. Da vCenter Server, aprire una console agli strumenti ONTAP.
6. Accedere come utente di manutenzione.
7. Immettere **2** per selezionare il menu **Configurazione di sistema**.
8. Immettere **7** per selezionare l'opzione **Aggiorna**.
9. Quando richiesto, fornire le credenziali vCenter. Questa è l'istanza vCenter in cui sono ospitati gli strumenti ONTAP .

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 limitato all'istanza vCenter che ospita gli strumenti ONTAP . È possibile creare un utente e un ruolo vCenter dedicati con solo le autorizzazioni richieste per la distribuzione del modello OVF. Per i dettagli, vedere i ruoli elencati in ["Ruoli inclusi nei tool ONTAP per VMware vSphere 10"](#).

Per l'istanza vCenter che verrà gestita dagli strumenti ONTAP , assicurarsi che l'account utente vCenter disponga dei privilegi di amministratore.

Durante l'aggiornamento, se in uno qualsiasi dei certificati back-end di archiviazione integrati mancano le voci Subject Alternative Name (SAN), verrà visualizzato un messaggio che indica il SAN mancante. Se si sceglie di procedere senza convalidare il SAN, l'aggiornamento continuerà, ma questa opzione non è consigliata a causa dei potenziali rischi per la sicurezza.

10. Quando si esegue l'aggiornamento, le seguenti azioni vengono eseguite automaticamente:
 - a. Il certificato gateway viene rinnovato con un periodo di validità di 1 anno. Quando si rimuove il precedente adattatore SRA e si carica 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 ONTAP e vCenter Server vengono convalidati e aggiunti agli strumenti ONTAP
 - d. Il backup è abilitato

Cosa succederà

Dopo l'aggiornamento agli ONTAP tools for VMware vSphere 10.5:

- Monitorare gli avvisi di sistema e pianificare il rinnovo del certificato del gateway prima che scada tra un anno.
- Rimuovere l'adattatore ONTAP Tools 10.4 o 10.3 SRA e caricare il file tar dell'adattatore 10.5 SRA.
- Eseguire il comando di installazione dopo aver caricato il tar dell'adattatore SRA. Quindi, eseguire nuovamente la scansione degli adattatori SRA per aggiornare la pagina Adattatori VMware Site Recovery

Storage Replication.

Dopo l'aggiornamento potrai:

- Disattivare i servizi dall'interfaccia utente di Manager
- Passaggio da un setup non ha a un setup ha
- È possibile espandere una configurazione non HA di piccole dimensioni a una configurazione non HA di medie dimensioni, oppure a una configurazione HA di medie o grandi dimensioni.

Informazioni correlate

["Migrazione dagli ONTAP tools for VMware vSphere 9.xx a 10.5"](#)

Codici di errore di aggiornamento di ONTAP tools

È possibile che si verifichino codici di errore durante gli strumenti ONTAP per l'operazione di aggiornamento di VMware vSphere.

I codici di errore sono composti da cinque cifre, in cui le prime due rappresentano lo script che ha riscontrato il problema e le ultime tre cifre rappresentano il flusso di lavoro specifico all'interno dello script.

Tutti i registri degli errori vengono registrati nel file `ansible-perl-errors.log` per facilitare il monitoraggio e la risoluzione dei problemi. Questo file di registro contiene il codice di errore e l'attività Ansible non riuscita.



I codici di errore forniti in questa pagina sono solo a scopo di riferimento. Se l'errore persiste o se non è stata menzionata alcuna soluzione, contattare il team di supporto.

Nella tabella seguente sono elencati i codici di errore e i nomi dei file corrispondenti.

Codice errore	Nome script
00	firstboot-network-config.pl, distribuzione in modalità
01	firstboot-network-config.pl, aggiornamento della modalità
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, implementazione, ha
04	firstboot-deploy-otv-ng.pl, implementazione, non ha
05	firstboot-deploy-otv-ng.pl, riavviare
06	firstboot-deploy-otv-ng.pl, upgrade, ha
07	firstboot-deploy-otv-ng.pl, upgrade, non ha
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Le ultime tre cifre del codice di errore indicano l'errore specifico del flusso di lavoro nello script:

Codice errore di aggiornamento	Flusso di lavoro	Risoluzione
052	L'ISO potrebbe essere uguale alla versione corrente o due release superiori rispetto alla versione corrente.	Utilizzare una versione ISO compatibile per eseguire l'aggiornamento dalla versione corrente.
068	Il rollback dei pacchetti Debian non è riuscito	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
069	Ripristino dei file non riuscito	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
070	Impossibile eliminare il backup	-
071	Il cluster Kubernetes non era integro	-
074	Montaggio ISO non riuscito	Controllare /var/log/upgrade-run.log e riprovare l'aggiornamento.
075	I controlli preliminari dell'aggiornamento non sono riusciti	Riprovare a eseguire l'aggiornamento.
076	Aggiornamento del Registro di sistema non riuscito	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
077	Ripristino del Registro di sistema non riuscito	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
078	Aggiornamento dell'operatore non riuscito	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
079	Il richiamo dell'operatore non è riuscito	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
080	Aggiornamento servizi non riuscito	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
081	Ripristino servizi non riuscito	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
082	Eliminazione delle vecchie immagini dal contenitore non riuscita	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
083	Eliminazione backup non riuscita	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.

Codice errore di aggiornamento	Flusso di lavoro	Risoluzione
084	La modifica di JobManager in produzione non è riuscita	Per ripristinare/completare l'aggiornamento, procedere come segue. 1. Attivare la shell diagnostica 2. Esegui il comando: <i>Sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Controllare i log in /var/log/post-deploy-upgrade.log
087	Procedura di post-aggiornamento non riuscita.	Per ripristinare/completare l'aggiornamento, procedere come segue. 1. Attivare la shell diagnostica 2. Eseguire <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> comando 3. Controllare i log in /var/log/post-deploy-upgrade.log
088	La configurazione della rotazione del registro per il giornale non è riuscita	Verificare le impostazioni di rete della VM compatibili con l'host su cui è ospitata la VM. È possibile provare a eseguire la migrazione della macchina virtuale su un altro host e riavviare.
089	La modifica della proprietà del file di configurazione rotazione del registro di riepilogo non è riuscita	Riprovare a eseguire l'aggiornamento.
095	Aggiornamento del sistema operativo non riuscito	Nessun ripristino per l'aggiornamento del sistema operativo. I servizi degli strumenti ONTAP vengono aggiornati e saranno in esecuzione nuovi pod.
096	Installa il provisioner di storage dinamico	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
097	La disinstallazione dei servizi per l'aggiornamento non è riuscita	Utilizzare un RPO pari a zero o un ripristino basato su snapshot e riprovare l'aggiornamento.
098	la copia del segreto dockercred dal sistema ntv allo spazio dei nomi del provisioner di storage dinamico non è riuscita	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
099	Impossibile convalidare la nuova aggiunta di HDD	Aggiungi il nuovo HDD a tutti i nodi in caso di ha e a un nodo in caso di implementazione non ha.
109	il backup dei dati del volume persistente non è riuscito	Controllare i registri di aggiornamento e riprovare l'aggiornamento.

Codice errore di aggiornamento	Flusso di lavoro	Risoluzione
110	ripristino dei dati del volume persistente non riuscito	Utilizza un ripristino basato su RPO pari a zero o su snapshot e riprova l'aggiornamento.
111	Aggiornamento dei parametri di timeout etcd per RKE2 non riuscito	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
112	La disinstallazione del provisioner di storage dinamico non è riuscita	-
113	Aggiornamento delle risorse sui nodi secondari non riuscito	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
104	Riavvio del nodo secondario non riuscito	Riavviare i nodi manualmente uno alla volta
100	il rollback del kernel non è riuscito	-
051	l'aggiornamento del provisioner di storage dinamico non è riuscito	Controllare i registri di aggiornamento e riprovare l'aggiornamento.
056	eliminazione del backup di migrazione non riuscita	NA
090	convalida del certificato per i backend di archiviazione e vCenter non riuscita	Controllare i registri di aggiornamento e il file di registro in /var/log/cert_validation_error.log e riprovare l'aggiornamento.



A partire dai tool ONTAP per VMware vSphere 10,3 zero RPO non è supportato.

Scopri di più ["Come ripristinare i tool ONTAP per VMware vSphere se l'aggiornamento non riesce dalla versione 10,0 alla 10,1"](#)

Migrare gli ONTAP tools for VMware vSphere 9.xx a 10.5

Migrazione dagli ONTAP tools for VMware vSphere 9.xx a 10.5

Lo spostamento degli strumenti NetApp ONTAP tools for VMware vSphere dalla versione 9.xx alla 10.5 richiede un processo di migrazione a causa degli aggiornamenti e dei miglioramenti significativi del prodotto nelle diverse versioni.

È possibile migrare dagli ONTAP tools for VMware vSphere 9.12D1, 9.13D2 e 9.13P2 agli ONTAP tools for VMware vSphere 10.5.

Se nella configurazione sono presenti datastore NFS e VMFS e nessun datastore vVols, è sufficiente disinstallare ONTAP Tools 9.xx e distribuire ONTAP Tools 10.5. Tuttavia, se la configurazione contiene datastore vVols, sarà necessario eseguire un processo di migrazione del provider VASA e dell'SRA.

La tabella seguente descrive il processo di migrazione in questi due diversi scenari.

Se la configurazione ha datastore vVols	Se la configurazione contiene solo datastore NFS e VMFS
Passaggi: 1. "Migrare il provider VASA" 2. "Creare policy di archiviazione VM"	Passaggi: 1. Rimuovere gli strumenti ONTAP 9.xx dal proprio ambiente. Fare riferimento a "Come rimuovere OTV 9.xx dal tuo ambiente" Articolo della Knowledge Base NetApp. 2. "Distribuisce e configura gli ONTAP tools for VMware vSphere 10.5" 3. "Aggiornare il SRA" 4. "Creare policy di archiviazione VM"



Dopo la migrazione dagli ONTAP tools for VMware vSphere 9.xx alla versione 10.5, i datastore vVols che utilizzano il protocollo NVMe/FC diventano non operativi perché gli strumenti ONTAP 10.5 supportano il protocollo NVMe-oF solo con i datastore VMFS.

Migrare il VASA Provider e aggiornare l'SRA negli ONTAP tools

Seguire i passaggi descritti in questa sezione per migrare VASA Provider dagli ONTAP tools for VMware vSphere 9.xx agli ONTAP tools for VMware vSphere 10.5 e aggiornare Storage Replication Adapter (SRA) sull'appliance VMware Live Site Recovery.

Passaggi per migrare il provider VASA

1. Per abilitare la PORTA Derby 1527 sugli strumenti ONTAP esistenti per VMware vSphere, abilitare l'utente root e accedere alla CLI tramite SSH. Quindi, eseguire il seguente comando:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Distribuisci OVA per gli ONTAP tools for VMware vSphere 10.5.
3. Aggiungere l'istanza di vCenter Server che si desidera migrare agli ONTAP tools for VMware vSphere 10.5. Fare riferimento a ["Aggiungere un'istanza di vCenter Server"](#) per maggiori informazioni.
4. ["Attiva provider VASA"](#) servizio sugli ONTAP tools for VMware vSphere 10.5.
5. Integrare il backend di storage localmente dalle API del server vCenter per il plug-in degli strumenti ONTAP . Fare riferimento a ["Aggiungere un backend di archiviazione utilizzando l'interfaccia client vSphere"](#) per maggiori informazioni.
6. Ottieni un token di accesso per autenticare le richieste API REST. Utilizzare l'esempio seguente, sostituendo le variabili con valori specifici per il proprio 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"}'
```

Copia e salva il token di accesso restituito nella risposta.

7. Eseguire la seguente API da Swagger o in Postman per la migrazione.

```
curl -X POST  
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migrati  
on-jobs`
```

Puoi accedere a Swagger tramite questo URL: `https://$FQDN_IP_PORT/` , Per esempio:
`https://10.67.25.33:8443/` .

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
POST	/api/v1

Tipo di lavorazione

Asincrono

Esempio 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 un'altra migrazione delle release:

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*****"
  }
}
```

Esempio di output JSON

Il sistema restituisce un oggetto lavoro. Salvare l'identificativo del lavoro per utilizzarlo nel passaggio successivo.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

8. Utilizzare il seguente URI in Swagger per controllare 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. Aggiungere gli ONTAP tools for VMware vSphere al vCenter Server.
10. Registrare il provider VASA con gli ONTAP tools for VMware vSphere. Per le istruzioni, vedere ["Registrare il provider VASA"](#).
11. 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.
12. Arrestare gli ONTAP tools for VMware vSphere Storage Provider 9.10/9.11/9.12/9.13 VASA Provider seguendo questi passaggi:
 - a. Negli strumenti ONTAP 9.x, aprire la console Web.
 - b. Accedere alla console di manutenzione.
 - c. Entra 1 per selezionare il menu **Configurazione applicazione**.
 - d. Entra 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 provider VASA, il vCenter Server esegue il failover sugli ONTAP tools for VMware vSphere. Tutti i datastore e le VM diventano accessibili e vengono gestiti dagli ONTAP tools for VMware vSphere.
13. I datastore NFS e VMFS migrati vengono visualizzati negli ONTAP tools for VMware vSphere 10.5 dopo il processo di individuazione del datastore, che può richiedere fino a 30 minuti. Controlla la loro visibilità nella pagina di panoramica.
14. Eseguire la migrazione delle patch utilizzando la seguente API in Swagger o in Postman:

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
PATCH	/api/v1

Tipo di lavorazione

Asincrono

Utilizzare il seguente URI in Swagger:

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Metodo HTTP ed endpoint

Questa chiamata API REST utilizza il metodo e l'endpoint seguenti.

Metodo HTTP	Percorso
PATCH	/api/v1

Tipo di lavorazione

Asincrono

Utilizzare il seguente URI in Swagger:

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Esempio 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 di migrazione restituito in risposta all'API post-migrazione.

Dopo aver eseguito l'API di migrazione delle patch, tutte le VM sono conformi al criterio di storage.

Cosa succederà

Dopo aver completato la migrazione e registrato gli strumenti ONTAP 10.5 su vCenter Server, seguire questi passaggi:

- Attendi il completamento di **Discovery** e il sistema aggiornerà automaticamente i certificati su tutti gli host.
- Attendere prima di avviare le operazioni del datastore e della macchina virtuale. Il tempo di attesa dipende dal numero di host, datastore e macchine virtuali. Se non aspetti, potresti riscontrare occasionali guasti.

Dopo l'aggiornamento, se lo stato di conformità della macchina virtuale è obsoleto, riapplicare il criterio di archiviazione attenendosi alla seguente procedura:

1. Vai al datastore e seleziona **Riepilogo > Criteri di archiviazione VM**.
2. Il sistema mostra lo stato di conformità in **Conformità ai criteri di archiviazione delle VM** come **Obsoleto**.
3. Selezionare il criterio VM di archiviazione e la VM corrispondente.
4. Selezionare **Applica**.
5. Lo stato di conformità in **Conformità ai criteri di archiviazione delle VM** risulta conforme.

Informazioni correlate

- ["Scopri i tool ONTAP per VMware vSphere 10 RBAC"](#)
- ["Aggiornamento dagli ONTAP tools for VMware vSphere 10.x alla versione 10.5"](#)

Passaggi per aggiornare l'adattatore di replicazione dello storage (SRA)

Prima di iniziare

Nel piano di ripristino, il sito protetto si riferisce alla posizione in cui le VM sono attualmente in esecuzione, mentre il sito di ripristino è quello in cui le VM verranno ripristinate. L'interfaccia dell'appliance VMware Live Site Recovery visualizza lo stato del piano di ripristino con dettagli sui siti protetti e di ripristino. Nel piano di ripristino, i pulsanti CLEANUP e REPROTECT sono disabilitati, mentre i pulsanti TEST ed RUN rimangono abilitati. Ciò indica che il sito è pronto per il ripristino dei dati. Prima di migrare l'SRA, verificare che un sito sia in stato protetto e l'altro in stato di ripristino.



Non avviare la migrazione se il failover è stato completato ma la nuova protezione 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, pulire il failover di prova e avviare la migrazione.

1. Per eliminare l'adattatore SRA degli strumenti ONTAP per VMware vSphere 9.xx in VMware Site Recovery, procedere come segue:
 - a. Andare alla pagina di gestione della configurazione di VMware Live Site Recovery
 - b. Andare alla sezione **Storage Replication Adapter**.
 - c. Dal menu puntini di sospensione, selezionare **Reimposta configurazione**.
 - d. Dal menu puntini di sospensione, selezionare **Elimina**.
2. Eseguire queste operazioni sui siti di protezione e ripristino.
 - a. ["Abilita i tool ONTAP per i servizi VMware vSphere"](#)
 - b. Configurare gli ONTAP tools for VMware vSphere 10.5 SRA seguendo i passaggi in ["Configurare SRA sull'appliance VMware Live Site Recovery"](#) .
 - c. Nell'interfaccia VMware Live Site Recovery, eseguire **Discover Arrays** e **Discover Devices**. Verificare che i dispositivi vengano visualizzati come prima della migrazione.

Automatizza utilizzando l'API REST

Scopri di più sull'API REST di ONTAP tools

Tool ONTAP per VMware vSphere 10: Set di strumenti per la gestione del ciclo di vita delle macchine virtuali. Include una solida API REST che puoi utilizzare come parte dei processi di automazione.

Base REST per i web Services

Representational state Transfer (REST) è uno stile per la creazione di applicazioni Web distribuite, inclusa la progettazione di API di servizi Web. Stabilisce una serie di tecnologie per esporre le risorse basate su server e gestire i loro stati.

Risorse e rappresentazione dello stato

Le risorse sono i componenti fondamentali di un'applicazione di servizi Web REST. Durante la progettazione di un'API REST, esistono due importanti attività iniziali:

- Identificare il sistema o le risorse basate su server
- Definire gli stati delle risorse e le operazioni di transizione degli stati associati

Le applicazioni client possono visualizzare e modificare gli stati delle risorse attraverso flussi di messaggi ben definiti.

Messaggi HTTP

HTTP (Hypertext Transfer Protocol) è il protocollo utilizzato dal client e dal server dei servizi Web per scambiare messaggi sulle risorse. Segue il modello CRUD basato sulle operazioni generiche di creazione, lettura, aggiornamento ed eliminazione. Il protocollo HTTP include le intestazioni di richiesta e risposta nonché i codici di stato di 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 industriale per rappresentare strutture di dati semplici in testo semplice e viene utilizzato per trasferire informazioni di stato che descrivono le risorse e le azioni desiderate.

Sicurezza

La sicurezza è un aspetto importante di un'API REST. Oltre al protocollo TLS (Transport Layer Security) utilizzato per proteggere il traffico HTTP sulla rete, gli strumenti ONTAP per l'API REST di VMware vSphere 10 utilizzano anche i token di accesso per l'autenticazione. È necessario acquisire un token di accesso e utilizzarlo nelle successive chiamate API.

Supporto di richieste asincrone

Gli strumenti ONTAP per l'API REST VMware vSphere 10 eseguono la maggior parte delle richieste in modo sincrono, restituendo un codice di stato al termine dell'operazione. Supporta inoltre l'elaborazione asincrona per task che richiedono un tempo più lungo per il completamento.

Ambiente di gestione degli strumenti ONTAP

È necessario prendere in considerazione diversi aspetti dell'ambiente di gestione degli strumenti ONTAP.

Macchina virtuale

Gli ONTAP tools for VMware vSphere 10 vengono distribuiti utilizzando l'architettura del plug-in remoto vSphere. Il software, incluso il supporto per l'API REST, viene eseguito in una macchina virtuale separata.

Indirizzo IP degli strumenti ONTAP

Gli strumenti ONTAP per VMware vSphere 10 espone un singolo indirizzo IP che fornisce un gateway alle funzionalità della macchina virtuale. È necessario fornire l'indirizzo durante la configurazione iniziale ed è assegnato a un componente di bilanciamento del carico interno. L'indirizzo viene utilizzato dall'interfaccia utente di ONTAP tools Manager, nonché per accedere direttamente alla pagina di documentazione di Swagger e all'API REST.

Due API REST

Oltre ai tool ONTAP per le API REST di VMware vSphere 10, il cluster ONTAP dispone di 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, fare riferimento a "[Automazione ONTAP](#)".

Dettagli di implementazione delle API REST di ONTAP tools

Mentre REST stabilisce un insieme comune di tecnologie e Best practice, l'implementazione esatta di ogni API può variare in base alle scelte di progettazione. Prima di utilizzare l'API REST di VMware vSphere 10, è necessario conoscere il modo in cui sono stati progettati i tool ONTAP.

Le API REST comprendono diverse categorie di risorse come vCenter e aggregati. Per ulteriori informazioni, consultare la "[Riferimento API](#)" sezione.

Come accedere all'API REST

Puoi accedere ai tool ONTAP per l'API REST di VMware vSphere 10 tramite l'indirizzo IP del tool ONTAP insieme alla porta. L'URL completo contiene diverse parti, tra cui:

- Porta e indirizzo IP degli strumenti ONTAP
- Versione di API
- Categoria di risorsa
- Risorsa specifica

È necessario configurare l'indirizzo IP durante la configurazione iniziale, mentre la porta rimane fissa a 8443. La prima parte dell'URL è coerente per ogni istanza ONTAP tools for VMware vSphere 10; cambiano solo la categoria della risorsa e la risorsa specifica tra gli endpoint.



I valori dell'indirizzo IP e della porta riportati negli esempi seguenti sono a solo scopo illustrativo. È necessario modificare questi valori per l'ambiente in uso.

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 di elenco dei 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 utilizzando il metodo GET.

Dettagli HTTP

I tool ONTAP per l'API REST di VMware vSphere 10 utilizzano HTTP e i parametri correlati per agire sulle raccolte e sulle istanze delle risorse. Di seguito sono presentati i dettagli dell'implementazione HTTP.

Metodi HTTP

I metodi HTTP o i verbi supportati dall'API REST sono presentati nella tabella seguente.

Metodo	CRUD	Descrizione
OTTIENI	Leggi	Recupera le proprietà degli oggetti per un'istanza o una raccolta di risorse. Questa operazione viene considerata un'operazione di elenco quando viene utilizzata con una raccolta.
POST	Creare	Crea una nuova istanza di risorsa in base ai parametri di input.
IN PRIMO PIANO	Aggiornare	Aggiorna un'intera istanza di risorsa con il corpo della richiesta JSON fornito. I valori chiave non modificabili dall'utente vengono mantenuti.
PATCH	Aggiornare	Richiede che all'istanza della risorsa venga applicata una serie di modifiche selezionate nella richiesta.
ELIMINARE	Eliminare	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
Accettare	Richiesta	Questo è il tipo di contenuto che l'applicazione client può accettare. I valori validi comprendono <code>*/*</code> o <code>application/json</code> .
x-auth	Richiesta	Contiene un token di accesso che identifica l'utente che invia la richiesta tramite l'applicazione client.
Tipo di contenuto	Risposta	Restituito dal server in base all'intestazione della <code>Accept</code> richiesta.

Codici di stato HTTP

I codici di stato HTTP utilizzati dall'API REST sono descritti di seguito.

Codice	Significato	Descrizione
200	OK	Indica il successo delle chiamate che non creano una nuova istanza di risorsa.
201	Creato	È stato creato un oggetto con un identificatore univoco per l'istanza di risorsa.

Codice	Significato	Descrizione
202	Accettato	La richiesta è stata accettata e un lavoro in background è stato creato per eseguire la richiesta.
204	Nessun contenuto	La richiesta è stata completata, anche se non è stato restituito alcun contenuto.
400	Richiesta errata	L'input della richiesta non viene riconosciuto o non è appropriato.
401	Non autorizzato	L'utente non è autorizzato e deve eseguire l'autenticazione.
403	Vietato	Accesso negato a causa di un errore di autorizzazione.
404	Non trovato	La risorsa a cui si fa riferimento nella richiesta non esiste.
409	Conflitto	Tentativo di creazione di un oggetto non riuscito perché l'oggetto esiste già.
500	Errore interno	Si è verificato un errore interno generale nel server.

Autenticazione

L'autenticazione di un client all'API REST viene eseguita utilizzando 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 di ONTAP Tools Manager (nome utente e password).
- I token sono formattati come token Web JSON (JWT).
- Ogni token scade dopo 60 minuti.
- Le richieste API da un client devono includere il token nell' `x-auth` intestazione della richiesta.

Fare riferimento alla "[La 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 vengono completate rapidamente e quindi eseguite in modo sincrono. In altre parole, restituiscono un codice di stato (ad esempio 200) dopo il completamento di una richiesta. Le richieste che richiedono più tempo per essere completate vengono eseguite in modo asincrono utilizzando un processo in background.

Dopo aver emesso una chiamata API che viene eseguita in modo asincrono, il server restituisce un codice di stato HTTP 202. Ciò indica che la richiesta è stata accettata ma non ancora completata. È possibile eseguire una query sul processo in background per determinarne lo stato, incluso il successo o l'errore.

L'elaborazione asincrona è impiegata per diversi tipi di operazioni con esecuzione prolungata, incluse le operazioni di datastore e vVol. Per ulteriori informazioni, fare riferimento alla categoria di gestione lavori dell'API REST nella pagina Swagger.

Effettua la tua prima chiamata API REST degli ONTAP tools

Puoi effettuare una chiamata API utilizzando curl per iniziare con i tool ONTAP per l'API REST di VMware vSphere 10.

Prima di iniziare

È necessario rivedere le informazioni e i parametri richiesti negli esempi di arriccatura.

Informazioni richieste

Sono necessari i seguenti elementi:

- Strumenti ONTAP per l'indirizzo IP o FQDN di VMware vSphere 10 e 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 le variabili di stile Bash. È possibile impostare queste variabili nell'ambiente Bash o aggiornarle manualmente prima di inviare i comandi. Se si impostano le variabili, la shell sostituirà i valori in ogni comando prima di eseguirlo. Le variabili sono descritte nella tabella seguente.

Variabile	Descrizione
\$FQDN_IP_PORT	Il nome di dominio completo o l'indirizzo IP del gestore strumenti ONTAP insieme al numero di porta.
\$MYUSER	Nome utente per l'account Gestore strumenti ONTAP.
\$MYPASSWORD	Password associata al nome utente del gestore strumenti ONTAP.
\$ACCESS_TOKEN	Token di accesso emesso dal gestore strumenti ONTAP.

I seguenti comandi e output della CLI 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
```

Fase 1: Acquisire un token di accesso

È necessario acquisire un token di accesso per utilizzare l'API REST. Di seguito è riportato un esempio di come richiedere un token di accesso. È necessario sostituire i valori appropriati per l'ambiente in uso.

```
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}"
```

Copiare e salvare il token di accesso fornito nella risposta.

Passaggio 2: Eseguire la chiamata API REST

Dopo aver ottenuto un token di accesso, è possibile utilizzare curl per eseguire una chiamata API REST. Includere il token di accesso acquisito nel primo passaggio.

Esempio di arricciamento

```
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 di VMware vCenter configurate in ONTAP Tools Manager.

Riferimento API REST di ONTAP tools

Il riferimento all'API REST dei tool ONTAP per VMware vSphere 10 contiene dettagli su tutte le chiamate API. Questo riferimento è utile quando si sviluppano applicazioni di automazione.

È possibile accedere online ai tool ONTAP per la documentazione dell'API REST di VMware vSphere 10 tramite l'interfaccia utente Swagger. È necessario l'indirizzo IP o FQDN degli strumenti ONTAP per il servizio gateway VMware vSphere 10 e la porta.

Fasi

1. Digitare il seguente URL nel browser sostituendo la combinazione di indirizzo IP e porta appropriata per la variabile e premere **Invio**.

```
https://$FQDN_IP_PORT/
```

Esempio

```
https://10.61.25.33:8443/
```

2. Come esempio di una singola chiamata API, scorrere verso il basso fino alla categoria **vCenters** e selezionare **GET** accanto all'endpoint `/virtualization/api/v1/vcenters`

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Direttiva sulla privacy

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

["Avviso per gli 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 COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.