



Tool ONTAP per la documentazione di VMware vSphere 10,3

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

Sommario

| | |
|--|----|
| Tool ONTAP per la documentazione di VMware vSphere 10,3 | 1 |
| Note di rilascio | 2 |
| Note di rilascio | 2 |
| Novità dei tool ONTAP per VMware vSphere 10,3 | 2 |
| Confronto tra i tool ONTAP per i tool VMware vSphere 9 e ONTAP per le funzionalità VMware vSphere 10 | 3 |
| Concetti | 5 |
| Panoramica sui tool ONTAP per VMware vSphere | 5 |
| Concetti e termini chiave | 5 |
| Controllo degli accessi in base al ruolo | 8 |
| Scopri i tool ONTAP per VMware vSphere 10 RBAC | 8 |
| RBAC con VMware vSphere | 9 |
| RBAC con ONTAP | 13 |
| Alta disponibilità per i tool ONTAP per VMware vSphere | 16 |
| AutoSupport | 16 |
| Interfaccia utente di ONTAP tools Manager | 16 |
| Implementa i tool ONTAP per VMware vSphere | 19 |
| Avvio rapido dei tool ONTAP per VMware vSphere | 19 |
| Workflow di implementazione ha (High Availability, alta disponibilità) | 21 |
| Prerequisiti per gli strumenti ONTAP per la distribuzione di VMware vSphere | 21 |
| Requisiti di sistema | 21 |
| Requisiti minimi di archiviazione e applicazione | 22 |
| Limiti di configurazione per l'implementazione dei tool ONTAP per VMware vSphere | 22 |
| Tool ONTAP per VMware vSphere - Storage Replication Adapter (SRA) | 23 |
| Requisiti delle porte | 23 |
| Prima di iniziare... | 24 |
| Foglio di lavoro distribuzione | 25 |
| Configurazione del firewall di rete | 26 |
| Implementa i tool ONTAP per VMware vSphere | 26 |
| Codici di errore di distribuzione | 29 |
| Configurare i tool ONTAP per VMware vSphere | 32 |
| Aggiungere istanze di vCenter Server | 32 |
| Registrare il provider VASA con un'istanza di vCenter Server | 32 |
| Installare il plug-in NFS VAAI | 33 |
| Configurare le impostazioni dell'host ESXi | 34 |
| Configurare le impostazioni di multipath e timeout del server ESXi | 34 |
| Impostare i valori dell'host ESXi | 35 |
| Configurare i ruoli e i privilegi degli utenti ONTAP | 36 |
| Requisiti di mappatura degli aggregati delle SVM | 37 |
| Creare manualmente un utente e un ruolo ONTAP | 37 |
| Aggiorna i tool ONTAP per VMware vSphere 10,1 a un utente 10,3 | 45 |
| Aggiungere un backend di storage | 47 |
| Associazione di un backend dello storage a un'istanza di vCenter Server | 48 |

| | |
|--|----|
| Configurare l'accesso alla rete | 49 |
| Creare un datastore | 49 |
| Protezione di datastore e macchine virtuali | 54 |
| Proteggere utilizzando la protezione del cluster host. | 54 |
| Proteggere utilizzando la protezione SRA | 55 |
| Abilitare SRA per proteggere i datastore | 55 |
| Configurare SRA per gli ambienti SAN e NAS | 55 |
| Configurare SRA per ambienti ad alta scalabilità | 56 |
| Configurare SRA sull'appliance VMware Live Site Recovery | 57 |
| Aggiornare le credenziali SRA | 58 |
| Configurare siti protetti e di ripristino | 59 |
| Configurare le risorse protette e del sito di ripristino | 60 |
| Verificare i sistemi storage replicati | 64 |
| Gestisci i tool ONTAP per VMware vSphere | 65 |
| Panoramica dei tool ONTAP per la dashboard di VMware vSphere | 65 |
| Interfaccia utente di ONTAP tools Manager | 66 |
| Comprendere i group e le policy di esportazione negli strumenti ONTAP per VMware vSphere | 68 |
| Policy di esportazione | 72 |
| Abilita i tool ONTAP per i servizi VMware vSphere | 72 |
| Modifica i tool di ONTAP per la configurazione di VMware vSphere | 73 |
| Gestire i datastore | 74 |
| Montare datastore NFS e VMFS | 74 |
| Smontare i datastore NFS e VMFS | 75 |
| Montare un datastore vVols | 75 |
| Ridimensionare il datastore NFS e VMFS | 76 |
| Espandere il datastore vVol | 76 |
| Restringere il datastore vVol | 77 |
| Elimina datastore | 77 |
| Viste dello storage ONTAP per datastore | 78 |
| Vista dello storage della macchina virtuale | 79 |
| Gestire le soglie di storage | 79 |
| Gestire i back-end dello storage | 79 |
| Rileva lo storage | 79 |
| Modificare i backend di archiviazione | 80 |
| Rimuovere i backend di stoccaggio | 80 |
| Drill-down del backend dello storage | 81 |
| Gestire le istanze di vCenter Server | 81 |
| Dissociare i backend di storage con l'istanza di vCenter Server | 81 |
| Modificare un'istanza di vCenter Server | 82 |
| Rimuovere un'istanza di vCenter Server | 82 |
| Gestire i certificati | 82 |
| Accedi ai tool ONTAP per la console di manutenzione di VMware vSphere | 85 |
| Panoramica dei tool ONTAP per la console di manutenzione VMware vSphere | 85 |
| Configurare l'accesso remoto alla diagnostica | 86 |
| Avviare SSH su altri nodi | 87 |

| | |
|---|-----|
| Aggiornare le credenziali vCenter Server e ONTAP | 87 |
| Report sui tool ONTAP | 87 |
| Raccogliere i file di log | 88 |
| Gestire le macchine virtuali | 88 |
| Considerazioni per migrare o clonare macchine virtuali | 89 |
| Migrazione di macchine virtuali con datastore NFS e VMFS in datastore vVol | 90 |
| Pulizia VASA | 90 |
| Rilevamento di host e sistemi storage | 90 |
| Modificare le impostazioni degli host ESXi utilizzando gli strumenti ONTAP | 91 |
| Gestire le password | 92 |
| Modificare la password del gestore strumenti ONTAP | 92 |
| Reimpostare la password di gestione degli strumenti ONTAP | 92 |
| Reimpostare la password utente dell'applicazione | 93 |
| Reimpostare la password utente della console di manutenzione | 93 |
| Gestire la protezione dei cluster di host | 94 |
| Modificare il cluster host protetto | 94 |
| Rimozione della protezione del cluster host | 97 |
| Disattiva AutoSupport | 97 |
| Aggiorna URL proxy AutoSupport | 98 |
| Creare un backup e ripristinare la configurazione | 98 |
| Creare il backup e scaricare il file di backup | 98 |
| Ripristinare | 99 |
| Disinstallare gli strumenti ONTAP per VMware vSphere | 99 |
| Rimuovere i volumi FlexVol | 100 |
| Aggiorna i tool ONTAP per VMware vSphere | 101 |
| Aggiornamento dai tool ONTAP per VMware vSphere 10.x alla 10,3 | 101 |
| Aggiornare i codici di errore | 105 |
| Esegui la migrazione dei tool ONTAP per VMware vSphere dalla 9.xx alla 10,3 | 109 |
| Migrazione dai tool ONTAP per VMware vSphere 9.xx a 10,3 | 109 |
| Migrare il provider VASA e aggiornare l'SRA | 109 |
| Passaggi per migrare il provider VASA | 109 |
| Passaggi per aggiornare l'adattatore di replicazione dello storage (SRA) | 112 |
| Automatizza utilizzando l'API REST | 113 |
| Scopri i tool ONTAP per l'API REST VMware vSphere 10 | 113 |
| Base REST per i web Services | 113 |
| Ambiente di gestione degli strumenti ONTAP | 113 |
| Dettagli di implementazione per i tool ONTAP per le API REST di VMware vSphere 10 | 114 |
| Come accedere all'API REST | 114 |
| Dettagli HTTP | 115 |
| Autenticazione | 116 |
| Richieste sincrone e asincrone | 116 |
| I tuoi primi tool ONTAP per la chiamata alle API REST di VMware vSphere 10 | 117 |
| Prima di iniziare | 117 |
| Fase 1: Acquisire un token di accesso | 117 |
| Passaggio 2: Eseguire la chiamata API REST | 118 |

| | |
|--|-----|
| Riferimento API per i tool ONTAP per l'API REST di VMware vSphere 10 | 118 |
| Note legali | 119 |
| Copyright | 119 |
| Marchi | 119 |
| Brevetti | 119 |
| Direttiva sulla privacy | 119 |
| Open source | 119 |

Tool ONTAP per la documentazione di VMware vSphere 10,3

Note di rilascio

Note di rilascio

Scopri le nuove e migliorate funzioni disponibili nei tool ONTAP per VMware vSphere 10,3.

Per un elenco completo delle nuove funzioni e dei miglioramenti, fare riferimento a [Novità dei tool ONTAP per VMware vSphere 10,3](#).

Per ulteriori informazioni sull'opportunità di eseguire la migrazione dagli strumenti ONTAP per VMware vSphere 9 agli strumenti ONTAP 10,3, consultare [Confronto tra i tool ONTAP per i tool VMware vSphere 9 e ONTAP per le funzionalità VMware vSphere 10](#). La migrazione è supportata dai tool ONTAP per VMware vSphere 9,12-D e le release 9,13-D agli strumenti ONTAP per VMware vSphere 10,3.

Per ulteriori informazioni, fare riferimento alla ["Note sulla versione dei tool ONTAP per VMware vSphere 10,3"](#). Per accedere alle Note di rilascio, è necessario accedere con l'account NetApp o creare un account.

Novità dei tool ONTAP per VMware vSphere 10,3

Scopri le nuove funzionalità disponibili nei tool ONTAP per VMware vSphere 10,3.

| Aggiornare | Descrizione |
|---|--|
| Supporto per nuove versioni di piattaforme e applicazioni | I tool ONTAP per VMware vSphere 10,3 ora supportano le seguenti versioni di piattaforme e applicazioni: <ul style="list-style-type: none">• ONTAP 9.16.0 e versioni successive• VMware vSphere 8,0 U3• VMware Live Site Recovery 9,0 |
| Facilità di implementazione | Da oggi puoi implementare i tool ONTAP per VMware vSphere 10,3 con requisiti minimi in un singolo cluster a nodo, per poi aggiornarlo a un'alta disponibilità (ha) o a un'implementazione multi-nodo. |
| Provisioning e configurazione perfetti | I tool ONTAP per VMware vSphere 10,3 hanno rimosso le dipendenze associate a Trident e ora utilizzano il provisioner di storage dinamico per consentire provisioning e configurazione perfetti. |
| Sicurezza avanzata per l'autenticazione delle API REST | Gli strumenti ONTAP per VMware vSphere 10,3 si affidano ora ai certificati firmati CA per le API REST e l'interfaccia utente degli strumenti ONTAP per garantire una maggiore sicurezza. |
| Supporto per i sistemi ASA R2 | I tool ONTAP per VMware vSphere 10,3 supportano il provisioning dei datastore VMFS sui sistemi ASA R2 per proteggere i datastore VMFS con la sincronizzazione attiva di SnapMirror e il ripristino dei siti live di SRA/VMware. |

| Aggiornare | Descrizione |
|--------------------------|---|
| Osservabilità migliorata | I tool ONTAP per VMware vSphere 10,3 estendono il supporto delle metriche di osservabilità per i datastore VMFS e vVol e per le rispettive macchine virtuali. |

Confronto tra i tool ONTAP per i tool VMware vSphere 9 e ONTAP per le funzionalità VMware vSphere 10

Scopri se la migrazione dai tool ONTAP per VMware vSphere 9 ai tool ONTAP per VMware vSphere 10,1 o versioni successive è la soluzione giusta per te. Per le informazioni più aggiornate sulla compatibilità, fare riferimento a ["Tool di matrice di interoperabilità NetApp"](#).

| Funzione | Strumenti ONTAP 9,13 | Strumenti ONTAP 10,1 | Attrezzi ONTAP da 10,2 in poi |
|----------------------------------|---|---|--|
| Proposta di valore chiave | Ottimizza e semplifica le operazioni quotidiane da 0 a 2 con funzionalità di sicurezza, conformità e automazione migliorate | Evoluzione degli strumenti ONTAP 10.x verso la parità 9.x e estensione dei limiti di high Availability, performance e scalabilità | Supporto esteso per includere FC per VMFS e vVol e NVMe-of/FC, NVMe-of/TCP solo per VMFS. Facilità di utilizzo per NetApp SnapMirror, semplice configurazione dei cluster di storage vSphere metro e supporto per il ripristino di tre siti VMware Live Site |
| Qualifica delle release di ONTAP | Da ONTAP 9.9,1 a ONTAP 9.15,1 | Da ONTAP 9.12,1 a ONTAP 9.14,1 | Da ONTAP 9.12.1 a ONTAP 9.15.1 per gli strumenti ONTAP 10,2 ONTAP 9.14.1, 9.15.1 e 9.16.0 per gli strumenti ONTAP 10,3. |
| Supporto alla release VMware | VSphere 7.x-8.x da VMware Site Recovery Manager (SRM) 8,5 a VMware Live Site Recovery 9,0 | VSphere 7.x-8.x da VMware Site Recovery Manager (SRM) 8,7 a VMware Live Site Recovery 9,0 | VSphere 7.x-8.x da VMware Site Recovery Manager (SRM) 8,7 a VMware Live Site Recovery 9,0 |
| Supporto del protocollo | Datastore NFS e VMFS: Datastore vVol NFS (v3 e v4,1), VMFS (iSCSI ed FCP): iSCSI, FCP, NVMe/FC, NFS v3 | Datastore NFS e VMFS: Datastore vVol NFS (v3 e v4,1), VMFS (iSCSI): iSCSI, NFS v3 | Datastore NFS e VMFS: Datastore vVol NFS (v3 e v4,1), VMFS (iSCSI/FCP/NVMe-of): iSCSI, FCP, NFS v3 |
| Scalabilità | Host e VM: 300 host, fino a 10K VM datastore: 600 NFS, fino a 50 VMFS, fino a 250 vVol vVol: Fino a 14.000 | Host e macchine virtuali: 600 host vVol: Fino a 140.000 | Host e macchine virtuali: 600 host vVol: Fino a 140.000 |

| Funzione | Strumenti ONTAP 9,13 | Strumenti ONTAP 10,1 | Attrezzi ONTAP da 10,2 in poi |
|------------------------|---|--|---|
| Osservabilità | Dashboard su performance, capacità e compliance host Report dinamici di VM e datastore | Dashboard aggiornate su performance, capacità e compliance dell'host Report dinamici di VM e datastore | Dashboard aggiornate su performance, capacità e compliance dell'host Report dinamici di VM e datastore |
| Protezione dei dati | Replica SRA per replica basata su VMFS e NFS FlexVols per integrazione vVols SCV e interoperabile per il backup | Replica SRA per datastore iSCSI VMFS e NFS v3 | Replica SRA per archivi dati iSCSI VMFS e NFS v3 protezione su tre siti che combina SMAS e VMware Live Site Recovery. |
| Supporto provider VASA | VASA 4,0 | VASA 3,0 | VASA 3,0 |

Concetti

Panoramica sui tool ONTAP per VMware vSphere

I tool ONTAP per VMware vSphere sono un set di strumenti per la gestione del ciclo di vita delle macchine virtuali. Si integra con l'ecosistema VMware per consentire il provisioning dei datastore e fornire una protezione di base per le macchine virtuali.

I tool ONTAP per VMware vSphere sono una raccolta di microservizi scalabili orizzontalmente, basati sugli eventi e implementati come Open Virtual Appliance (OVA). Questa versione è dotata di integrazione API REST con ONTAP.

I tool ONTAP per VMware vSphere sono composti da:

- Funzionalità della macchina virtuale come protezione di base e disaster recovery
- Provider VASA per gestione granulare delle macchine virtuali
- Gestione basata su criteri dello storage
- Storage Replication Adapter (SRA)
- SnapMirror Active Sync (SMAS)

Concetti e termini chiave

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

Sistemi ASA r2

I nuovi sistemi NetApp ASA R2 forniscono una soluzione hardware e software unificata che crea un'esperienza semplificata specifica delle esigenze dei clienti SAN. ["Informazioni sui sistemi di storage ASA R2"](#).

Autorità di certificazione (CA)

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

Gruppo di coerenza

Un gruppo di coerenza è un insieme di volumi gestiti come singola unità. In ONTAP, i gruppi di coerenza offrono una gestione semplice e una garanzia di protezione per un carico di lavoro applicativo che copre più volumi. Ulteriori informazioni su ["gruppo 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 ai tool ONTAP per l'amministratore di VMware vSphere sulle istanze di vCenter Server gestite e sui backend storage integrati. ONTAP tools Manager aiuta nella gestione di istanze di vCenter Server, backend di storage, certificati, password e download di 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)

Il valore di RPO misura la frequenza di esecuzione del backup o della replica dei dati. Rappresenta il momento in cui i dati devono essere ripristinati dopo un'interruzione per poter riprendere le operazioni di business. Ad esempio, se un'organizzazione ha un RPO di 4 ore, può tollerare la perdita di dati fino a 4 ore in caso di disastro.

SnapMirror Active Sync (SMAS)

SnapMirror Active Sync consente ai servizi di business di continuare a funzionare anche in caso di guasto completo del sito, supportando le applicazioni per il failover in modo trasparente con una copia secondaria. Per attivare un failover con la sincronizzazione attiva di SnapMirror sono necessari un intervento manuale e script personalizzato. 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. Il backend dello storage consente all'host ESXi di accedere e gestire i dati persistenti, fornendo le funzionalità e le performance dello storage necessarie per l'ambiente virtualizzato.

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 abilita 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)

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

- **Accesso uniforme all'host** significa che gli host di entrambi i siti sono connessi a tutti i percorsi ai cluster di storage su entrambi i siti. I percorsi tra siti trasversali sono estesi a ogni distanza.
- **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.

File system della macchina virtuale (VMFS)

VMFS è un file system in cluster appositamente progettato per l'archiviazione dei file delle macchine virtuali negli ambienti VMware vSphere.

Volumi virtuali (vVol)

I vVol offrono un'astrazione a livello di volume per lo storage utilizzato da una macchina virtuale. Include diversi vantaggi e offre un'alternativa all'utilizzo di un LUN tradizionale. Di solito, un datastore vVol è associato a una singola LUN che agisce come container per i vVol.

Policy per lo storage delle VM

Le policy 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 offre 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 una tecnologia 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 logica del datastore 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 in base al ruolo

Scopri i tool ONTAP per VMware vSphere 10 RBAC

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 funzionalità che può essere consentita o negata. Potrebbe trattarsi di qualcosa di semplice come la capacità di leggere un file o di un'operazione più astratta specifica di un dato sistema software. Privileges può anche essere definito per limitare l'accesso agli endpoint delle API REST e ai comandi della CLI. Ogni implementazione RBAC include Privileges predefinito e può anche consentire agli amministratori di creare Privileges personalizzato.

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

Esistono due distinti ambienti RBAC da prendere in considerazione quando si utilizzano i tool ONTAP per VMware vSphere 10.

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"](#).

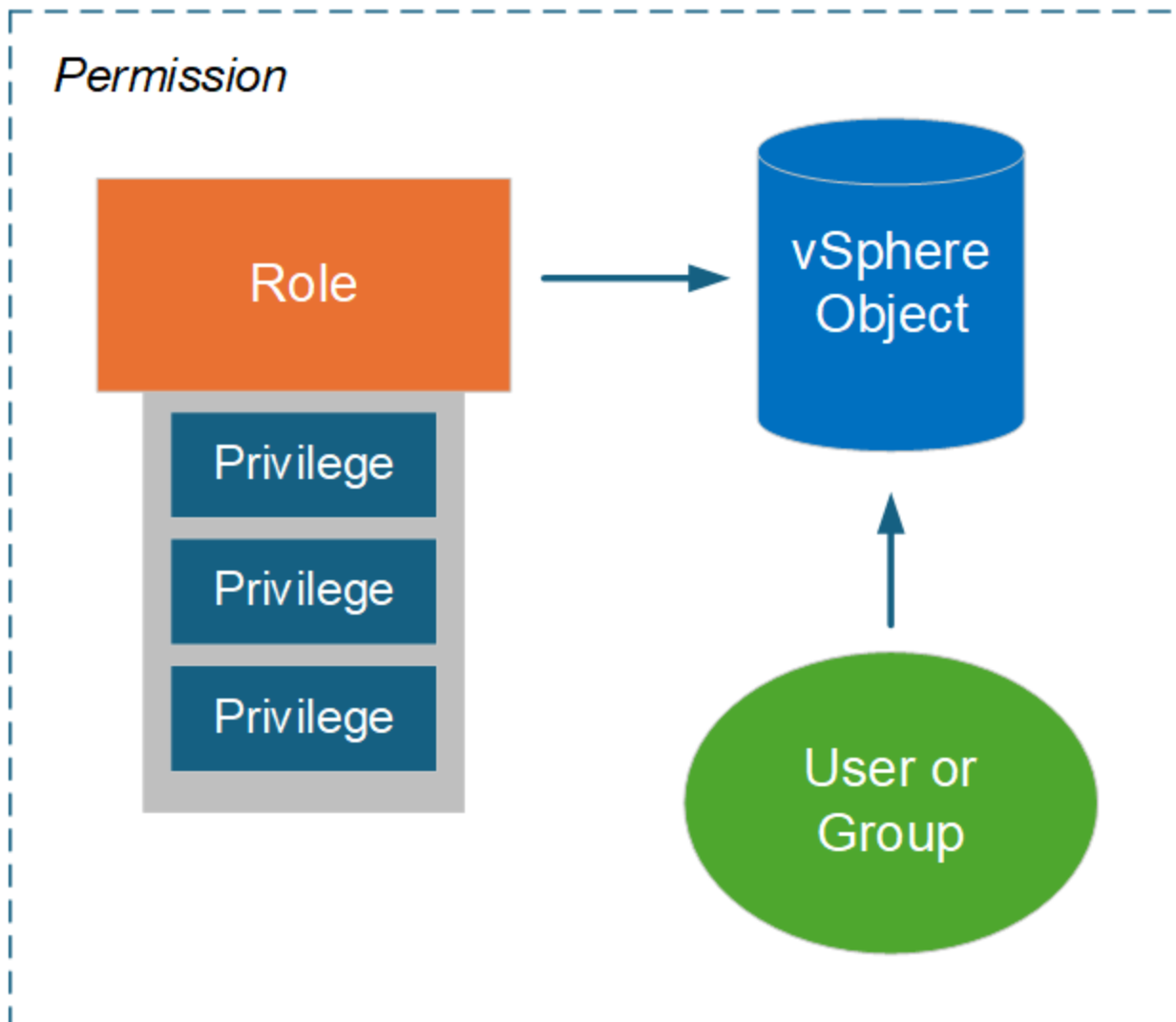
RBAC con VMware vSphere

Ambiente vCenter Server RBAC con tool ONTAP per VMware vSphere 10

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. Insieme a un ruolo, è possibile creare un'autorizzazione per un oggetto nella gerarchia degli oggetti vSphere. L'autorizzazione concede l'accesso in base all'Privileges nel ruolo associato. Tenere presente che i ruoli non vengono assegnati direttamente agli utenti in isolamento. Gli utenti e i gruppi ottengono invece l'accesso a un oggetto tramite Role Privileges come parte dell'autorizzazione più grande di vCenter Server.

USA vCenter Server RBAC con i tool ONTAP per VMware vSphere 10

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 strumenti ONTAP per i ruoli VMware vSphere, selezionare **Menu** nella parte superiore del client vSphere e fare clic su **Amministrazione**, quindi **ruoli** a sinistra. Esistono 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

Ambiente RBAC ONTAP con tool ONTAP per VMware vSphere 10

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"](#).



Il role-based access control ONTAP è personalizzato per un ambiente storage ed è più semplice rispetto all'implementazione RBAC fornita con vCenter Server. ONTAP consente di assegnare un ruolo direttamente all'utente. La configurazione di autorizzazioni esplicite, come quelle utilizzate con vCenter Server, non è necessaria con RBAC di ONTAP.

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"](#).

USA RBAC ONTAP con tool ONTAP per VMware vSphere 10

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

I tool ONTAP per VMware vSphere 10 includono il supporto per la creazione di un utente ONTAP con un ruolo personalizzato. Le definizioni sono contenute in un file JSON che è possibile caricare nel cluster ONTAP. È possibile creare l'utente e personalizzare il ruolo in base all'ambiente e alle esigenze di protezione.

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.

Alta disponibilità per i tool ONTAP per VMware vSphere

I tool ONTAP per VMware vSphere supportano una configurazione ha (High Availability) per fornire funzionalità ininterrotte dei tool ONTAP per VMware vSphere durante i guasti.

La soluzione ad alta disponibilità (ha) offre un rapido ripristino in caso di interruzioni causate da:

- Errore host



È supportato solo il guasto a nodo singolo.

- Errore di rete
- Errore della macchina virtuale (errore del sistema operativo guest)
- Arresto anomalo dell'applicazione (strumenti ONTAP)

Non sono richieste configurazioni aggiuntive per i tool ONTAP per VMware vSphere per l'high Availability (ha).



I tool ONTAP per VMware vSphere non supportano vCenter ha.

Per abilitare la funzionalità ha, l'hot add della CPU e l'hot plug della memoria devono essere abilitati durante l'implementazione o in un secondo momento nei tool ONTAP per le impostazioni della VM di VMware vSphere.

AutoSupport

AutoSupport è un meccanismo che monitora in modo proattivo lo stato di salute del sistema e invia automaticamente messaggi al supporto tecnico NetApp, all'organizzazione di supporto interna e a un partner di supporto.

AutoSupport è attivato per impostazione predefinita quando si configura il sistema di storage per la prima volta. AutoSupport inizia a inviare messaggi al supporto tecnico 24 ore dopo l'attivazione di AutoSupport.

È possibile disattivare AutoSupport utilizzando l'opzione della console di manutenzione **Configurazione applicazione > Disattiva AutoSupport**. Si consiglia di lasciarlo attivato. L'attivazione di AutoSupport consente di velocizzare il rilevamento dei problemi e di ottenere una risoluzione più rapida. Il sistema raccoglie le informazioni AutoSupport e le memorizza localmente, anche quando AutoSupport è disattivato. Tuttavia, non invia il rapporto a nessuna rete. È necessario fornire l'URL proxy utilizzando la console di manutenzione della prima VM. Utilizzare l'opzione **Configurazione applicazione > Aggiorna URL proxy AutoSupport** per immettere l'URL proxy.

Interfaccia utente di ONTAP tools Manager

I tool ONTAP per VMware vSphere sono un sistema multi-tenant in grado di gestire più istanze di vCenter Server. ONTAP Tools Manager offre un maggiore controllo ai tool

ONTAP per l'amministratore di VMware vSphere sulle istanze di vCenter Server gestite e sui backend storage integrati.

ONTAP Tools Manager aiuta a:

- Gestione delle istanze di vCenter Server: Aggiunta e gestione delle istanze di vCenter Server agli strumenti ONTAP.
- Gestione backend dello storage - Aggiungi e gestisci i cluster di storage ONTAP ai tool ONTAP per VMware vSphere e mappali alle istanze vCenter Server integrate a livello globale.
- Download dei bundle di log: Raccolta dei file di log per gli strumenti ONTAP per VMware vSphere.
- Gestione certificati - consente di modificare il certificato autofirmato in un certificato CA personalizzato e di rinnovare o aggiornare tutti i certificati del provider VASA e degli strumenti ONTAP.
- Gestione password - consente di reimpostare la password dell'applicazione OVA dell'utente.

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.

La sezione Panoramica su ONTAP tools Manager aiuta a gestire la configurazione dell'appliance, come la gestione dei servizi, l'upscaling delle dimensioni dei nodi e l'abilitazione ha (High Availability). Puoi anche monitorare le informazioni generali dei tool ONTAP relativi ai nodi, come lo stato di salute, i dettagli di rete e gli avvisi.

The screenshot displays the ONTAP Tools Manager web interface. The top navigation bar shows the ONTAP logo and the text 'ONTAP tools Manager', along with a refresh icon and the user role 'Administrator'. The left sidebar contains a menu with the following items: Overview (selected), Alerts, Jobs, Storage backends, vCenters, Log bundles, Certificates, and Settings. The main content area is titled 'Overview' and includes an 'EDIT APPLIANCE SETTINGS' button. The 'Appliance' section shows a 'Healthy' status with a green checkmark and a table of configuration details: Size: Small, HA: Enabled, VASA provider: Enabled, and SRA: Enabled. The 'Alerts' section, filtered for the last 24 hours, shows 3 Error alerts (red exclamation mark), 2 Warning alerts (orange exclamation mark), and 5 Info alerts (blue 'i'). Below the alerts is a 'VIEW ALL ALERTS (43)' link. The 'ONTAP tools nodes' section displays three nodes: nodename_01, nodename_02, and nodename_03. Each node is shown as 'Online' with a green checkmark and has a 'demo_vm' instance. Each node card includes a 'VIEW DETAILS' link.

| Carta | Descrizione |
|-----------------------------|---|
| Scheda dell'appliance | La scheda dell'appliance fornisce lo stato generale dell'appliance ONTAP Tools. Mostra i dettagli di configurazione del dispositivo e lo stato dei servizi abilitati. Per ulteriori informazioni sull'appliance ONTAP Tools, selezionare il collegamento Visualizza dettagli . Quando è in corso un processo di azione di modifica delle impostazioni del dispositivo, il portlet del dispositivo mostra lo stato e i dettagli del processo. |
| Scheda avvisi | La scheda Alerts elenca gli alert dei tool ONTAP in base al tipo, compresi gli alert a livello di nodo di ha. È possibile visualizzare l'elenco degli avvisi selezionando il testo del conteggio (collegamento ipertestuale). Il collegamento indirizza l'utente alla pagina di visualizzazione degli avvisi filtrata in base al tipo selezionato. |
| Scheda nodi strumenti ONTAP | La scheda dei nodi dei tool ONTAP mostra l'elenco dei nodi con nome del nodo, nome della macchina virtuale del nodo, stato e tutti i dati relativi alla rete. È possibile selezionare on Visualizza dettagli per visualizzare i dettagli aggiuntivi relativi al nodo selezionato. [NOTA] in un setup non ha viene visualizzato un solo nodo. Nel setup ha sono mostrati tre nodi. |

Implementa i tool ONTAP per VMware vSphere

Avvio rapido dei tool ONTAP per VMware vSphere

La guida introduttiva ai tool ONTAP per VMware vSphere include alcuni passaggi. Questa guida rapida illustra la configurazione iniziale degli strumenti ONTAP per VMware vSphere.

Inizialmente, implementerai tool ONTAP per VMware vSphere come configurazione di piccole dimensioni a nodo singolo che offre servizi chiave per supportare i datastore NFS e VMFS. Se devi espandere la configurazione per utilizzare il datastore vVol e l'alta disponibilità (ha), ti basterà completare questo workflow. Per ulteriori informazioni, fare riferimento alla ["Workflow di implementazione HA"](#).

1

Pianificare la distribuzione

Verificare che le versioni host di vSphere, ONTAP e ESXi siano compatibili con la versione dei tool ONTAP. Assegnare una quantità sufficiente di CPU, memoria e spazio su disco. A seconda dei criteri di protezione, potrebbe essere necessario configurare firewall o altre applicazioni di protezione per consentire il traffico di rete.

Assicurarsi che vCenter Server sia installato e accessibile.

- ["Tool di matrice di interoperabilità"](#)
- ["Prerequisiti per gli strumenti ONTAP per la distribuzione di VMware vSphere"](#)
- ["Prima di iniziare"](#)

2

Implementa i tool ONTAP per VMware vSphere

Inizialmente, implementerai strumenti ONTAP per VMware vSphere come configurazione di piccole dimensioni a nodo singolo che offre servizi chiave per supportare datastore NFS e VMFS. Se intendi espandere la configurazione per utilizzare i datastore vVol e l'alta disponibilità (ha), ti troverai al termine di questo workflow. Per eseguire correttamente l'espansione in una configurazione ha, è necessario verificare che le opzioni hot-add della CPU e hot-plug della memoria siano attivate.

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

3

Aggiungere istanze di vCenter Server

Aggiungi una o più istanze di vCenter Server ai tool ONTAP per 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

(Opzionale) attivare la protezione SRA

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

- ["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. Accoppiare i cluster di destinazione e di origine e SVM per la sincronizzazione attiva di SnapMirror. 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

Pianificazione dei backup dei tool ONTAP per il setup di VMware vSphere, utilizzabili per ripristinare il setup in caso di errore.

- ["Creare una copia di backup e ripristinare la configurazione degli strumenti ONTAP"](#)

Workflow di implementazione ha (High Availability, alta disponibilità)

Se stai utilizzando i datastore vVol, devi espandere l'implementazione iniziale dei tool ONTAP in una configurazione ha (High Availability, alta disponibilità) e abilitare i servizi del provider VASA.

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 il datastore vVol è necessario abilitare il servizio Provider VASA. Registra il provider VASA con vCenter e assicurati che le policy storage soddisfino i requisiti di ha, incluse le configurazioni di storage e rete 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"](#)

Prerequisiti per gli strumenti ONTAP per la distribuzione di VMware vSphere

Prima di implementare gli strumenti ONTAP per VMware vSphere, è necessario conoscere i requisiti di spazio per il pacchetto di distribuzione 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 memoria consigliata in base alle dimensioni di distribuzione è illustrata nella tabella seguente:

| Tipo di distribuzione | CPU | Memoria (GB) | Spazio su disco (GB) con thick provisioning |
|--------------------------------------|-----|--------------|---|
| Non ha piccolo | 9 | 18 | 350 |
| Terreno non ha | 13 | 26 | 350 |
| HA Small (cumulativo di tre nodi) | 27 | 54 | 1050 |
| Supporto HA (cumulativo di tre nodi) | 39 | 78 | 1050 |
| HA Large (cumulativo di tre nodi) | 51 | 102 | 1050 |

Requisiti minimi di archiviazione e applicazione

| Storage, host e applicazioni | Requisiti minimi di versione |
|------------------------------|--|
| ONTAP | 9.14.1, 9.15.1 e 9.16.0. FAS, ASA A-Series, ASA C-Series, AFF A-Series, AFF C-Series e ASA R2. |
| Host ESXi | ESXi 7.0.3 |
| Server vCenter | VCenter 7.0U3 |
| Provider VASA | 3,0 |
| Applicazione OVA | 10,3 |

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"](#)

Limiti di configurazione per l'implementazione dei tool ONTAP per VMware vSphere

La seguente tabella illustra la configurazione dei tool ONTAP per VMware vSphere.

| Implementazione | Tipo | Numero di vVol | Numero di host |
|--------------------|-------------|----------------|--|
| Non ha | Piccolo (S) | CIRCA 12K MB | 32 |
| Non ha | Medio (M) | CIRCA 24K MB | 64 |
| Alta disponibilità | Piccolo (S) | CIRCA 24K MB | 64 |
| Alta disponibilità | Medio (M) | circa 50k mb | 128 |
| Alta disponibilità | Grande (L) | circa 100k mb | 256 [NOTA] il numero di host nella tabella mostra il numero totale di host da più vCenter. |

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 delle porte

Nella tabella seguente sono descritte le porte di rete utilizzate da NetApp e le relative finalità. Assicurarsi che queste porte siano aperte e accessibili per facilitare il corretto funzionamento e la comunicazione all'interno del sistema. Verificare che siano state configurate le configurazioni di rete necessarie per consentire il corretto funzionamento del traffico su queste porte per i servizi associati. A seconda dei criteri di protezione in uso, potrebbe essere necessario configurare firewall o altri dispositivi di protezione per consentire questo traffico all'interno della rete.

| Porta | Descrizione |
|--------------|--|
| 22 (TCP) | Ansible utilizza questa porta SSH per la comunicazione durante il provisioning del cluster. Questa porta è necessaria per funzionalità come la modifica della password utente di manutenzione, i messaggi di stato e per aggiornare i valori su tutti e tre i nodi in caso di configurazione ha. |

| | |
|-------------------|---|
| 443 (TCP) | Questa è la porta pass-through per le comunicazioni in entrata per il servizio del provider VASA. Il certificato autofirmato del provider VASA e il certificato CA personalizzato sono ospitati su questa porta. |
| 8443 (TCP) | Questa porta ospita la documentazione API tramite swagger e l'applicazione dell'interfaccia utente di Manager. |
| 2379 (TCP) | Questa è la porta predefinita per le richieste client, ad esempio Get, put, DELETE o Watch for keys nell'archivio valori chiavi etcd. |
| 2380 (TCP) | Questa è la porta predefinita per la comunicazione server-server per il cluster etcd utilizzato per l'algoritmo di consenso raft su cui si basa etcd per la replica e la coerenza dei dati. |
| 7472 (TCP+UDP) | Questa è la porta di servizio delle metriche prometheus. |
| 7946 (TCP+UDP) | Questa porta viene utilizzata per il rilevamento della rete dei container del docker. |
| 9083 (TCP) | Questa porta è una porta di servizio utilizzata internamente per il servizio del provider VASA. |
| 1162 (UDP) | Questa è la porta dei pacchetti trap SNMP. |
| 6443 (TCP) | Fonte: RKE2 nodi agenti. Destinazione: REK2 nodi server. Descrizione: API Kubernetes |
| 9345 (TCP) | Fonte: RKE2 nodi agenti. Destinazione: REK2 nodi server. Descrizione: API supervisore REK2 |
| 8472 (TCP+UDP) | Tutti i nodi devono essere in grado di raggiungere gli altri nodi sulla porta UDP 8472 quando si utilizza VXLAN flanel. Fonte: Tutti e RKE2 i nodi. Destinazione: Tutti e REK2 i nodi. Descrizione: Canal CNI con VXLAN |
| 10250 (TCP) | Fonte: Tutti e RKE2 i nodi. Destinazione: Tutti e REK2 i nodi. Descrizione: Kubelet metriche |
| 30000-32767 (TCP) | Fonte: Tutti e RKE2 i nodi. Destinazione: Tutti e REK2 i nodi. Descrizione: Intervallo porta NodePort |
| 123 (TCP) | Ntpd utilizza questa porta per eseguire la convalida del server ntp. |

Prima di iniziare...

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 necessarie per i tool ONTAP per la distribuzione iniziale di VMware vSphere: Per gli strumenti ONTAP per la distribuzione iniziale di VMware vSphere:

| Requisito | Il tuo valore |
|---|---------------|
| Indirizzo IP per l'applicazione degli strumenti ONTAP. Questo è l'indirizzo IP per accedere all'interfaccia web degli strumenti ONTAP. | |
| Indirizzo IP virtuale degli strumenti ONTAP per le comunicazioni interne. Questo indirizzo IP viene utilizzato per le comunicazioni interne in una configurazione con più istanze degli strumenti ONTAP. Questo indirizzo IP non deve essere uguale all'indirizzo IP dell'applicazione degli strumenti ONTAP. | |
| Nome host DNS per il primo nodo | |

| Requisito | Il tuo valore |
|--|---------------|
| Server DNS primario | |
| Server DNS secondario | |
| Dominio di ricerca DNS | |
| Indirizzo IPv4 per il primo nodo. È un indirizzo IPv4 univoco per l'interfaccia di gestione del nodo sulla rete di gestione. | |
| 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

Aprire le porte richieste per gli indirizzi IP nel firewall di rete. I tool ONTAP devono essere in grado di raggiungere questa LIF tramite la porta 443. Per gli aggiornamenti più recenti, consultare la sezione ["Requisiti delle porte"](#).

Implementa i tool ONTAP per VMware vSphere

I tool ONTAP per l'appliance VMware vSphere sono implementati come nodo singolo di piccole dimensioni con servizi core per supportare i datastore NFS e VMFS.

Prima di iniziare

Una libreria di contenuti in VMware è un oggetto contenitore che memorizza modelli di VM, modelli di vApp e altri tipi di file. La distribuzione con la libreria di contenuti offre un'esperienza senza problemi poiché non dipende dalla connettività di rete.



È necessario archiviare la libreria di contenuti in un datastore condiviso in modo che tutti gli host all'interno di un cluster possano accedervi. Creare una libreria di contenuti per memorizzare l'OVA prima di configurare l'appliance sulla configurazione ha. Non eliminare il modello della libreria di contenuti dopo la distribuzione.



Per consentire l'implementazione ha in un secondo momento, non implementare la macchina virtuale che ospita i tool ONTAP direttamente su un host ESXi. Implementarlo invece su un cluster o un pool di risorse.

Se non disponi di una libreria di contenuti, segui questi passaggi per crearne una:

Creare una libreria di contenuti in un'implementazione con un solo nodo di piccole dimensioni, non è necessario creare una libreria di contenuti.

1. Scaricare il .zip file contenente i file binari (.ova) e i certificati firmati per gli strumenti ONTAP per VMware vSphere dal "[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. Accedere alla libreria di contenuti creata.
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 DRS (Distributed Resource Scheduler) del cluster sull'inventario su 'Conservative'. In questo modo, le VM non vengono migrate durante l'installazione.

All'inizio, i tool ONTAP per VMware vSphere vengono implementati come configurazione non ha. Per scalare l'implementazione ha, è necessario abilitare il plug-in hot della CPU e il plug-in hot della memoria. È possibile eseguire questo passaggio come parte del processo di distribuzione o modificare le impostazioni della macchina virtuale dopo la distribuzione.

Fasi

1. Scaricare il .zip file contenente i file binari (.ova) e i certificati firmati per gli strumenti ONTAP per VMware vSphere dal "[Sito di supporto NetApp](#)". Se l'OVA è stato importato nella libreria di contenuti, è possibile saltare questo passaggio e procedere con il passaggio successivo.
2. Accedere al server vSphere.
3. Passare 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 la procedura descritta nella sezione **What's next?** al termine della distribuzione.

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**, compilare i campi obbligatori e selezionare **Avanti**.

- Le informazioni vengono convalidate durante l'installazione. In caso di discrepanza, viene visualizzato un messaggio di errore sulla console Web e viene richiesto di correggerla.
- 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.
- L'indirizzo IP di interconnessione dei nodi viene utilizzato per la comunicazione interna.

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

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 il completamento dell'attività.

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

In caso di discrepanze nel modulo OVF, viene visualizzata una finestra di dialogo che richiede l'azione correttiva. Utilizzare il pulsante Tab per spostarsi, apportare le modifiche necessarie e selezionare "OK". Sono disponibili tre tentativi per risolvere eventuali problemi. Se i problemi persistono dopo tre tentativi, il processo di installazione si interrompe 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. Spegnerne il nodo ONTAP Tools.
3. Accedere agli strumenti ONTAP per la macchina virtuale 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**.

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 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 distribuzione | Flusso di lavoro | Risoluzione |
|---------------------------------------|---|---|
| 050 | Generazione chiave SSH non riuscita | Riavviare la macchina virtuale primaria (VM). |
| 053 | Installazione RKE2 non riuscita | Eseguire le seguenti operazioni e riavviare la macchina virtuale primaria o ridistribuire: Sudo rke2-killall.sh (tutte le macchine virtuali) sudo rke2-uninstall.sh (tutte le macchine virtuali). |
| 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 ridistribuirlo. |
| 059 | La distribuzione di KubeVip non è riuscita | Garantire che l'indirizzo IP virtuale per il piano di controllo di Kubernetes e l'indirizzo IP del bilanciatore di carico fornito durante l'implementazione appartengano alla stessa VLAN e sono 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

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

Attraverso l'integrazione con vCenter, gli strumenti ONTAP ti consentono di eseguire task di storage come provisioning, snapshot e data Protection direttamente dal client vSphere, eliminando la necessità di passare a console di gestione dello storage separate.

Fasi

1. Aprire un browser Web e accedere 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.



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:

- Il plug-in del client vCenter è registrato 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 di vCenter Server

Puoi registrare il provider VASA con un'istanza di vCenter Server utilizzando i tool ONTAP per VMware vSphere. La sezione Impostazioni provider VASA visualizza lo stato di registrazione provider VASA per vCenter Server selezionato. In una distribuzione multi-vCenter, assicurati di disporre di certificati CA personalizzati per ogni istanza di vCenter Server.

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**. Lo stato di registrazione del provider VASA viene visualizzato come non registrato.
4. Selezionare il pulsante **Registra** per registrare il provider VASA.
5. Immettere un nome per il provider VASA e fornire gli strumenti ONTAP per le credenziali utente dell'applicazione VMware vSphere e selezionare **Registra**.
6. Dopo aver completato la registrazione e l'aggiornamento della pagina, vengono visualizzati lo stato, il nome e la versione del provider VASA registrato. Dopo la registrazione, viene attivata l'azione di annullamento della registrazione.

Al termine

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

Il plug-in NFS vStorage API for Array Integration (NFS VAAI) è un componente software che integra gli storage array VMware vSphere e NFS. Installa il plug-in NFS VAAI utilizzando i tool di ONTAP per VMware vSphere per sfruttare le funzionalità avanzate dello storage array NFS e scaricare alcune operazioni legate allo storage dagli host ESXi allo storage array stesso.

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. Quando il plug-in VAAI viene caricato su vCenter Server, seleziona **Cambia** nella sezione **versione esistente**. Se un plug-in VAAI non viene caricato in vCenter Server, selezionare il pulsante **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**.

Vengono visualizzati solo gli host ESXi idonei per l'installazione del plug-in. È possibile monitorare l'avanzamento dell'installazione nella sezione attività recenti del client web vSphere.

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

Quando l'amministratore VMware riavvia l'host ESXi, i tool ONTAP per VMware vSphere rilevano e attivano automaticamente il plug-in NFS VAAI.

Quali sono le prossime novità?

Dopo aver installato il plug-in NFS VAAI e riavviato l'host ESXi, occorre configurare le policy di esportazione NFS corrette per l'offload delle copie VAAI. Durante la configurazione di VAAI in un ambiente NFS, configurare le regole delle policy di esportazione tenendo presenti i seguenti requisiti:

- Il volume ONTAP rilevante deve consentire NFSv4 chiamate.
- L'utente root deve rimanere come root e NFSv4 deve essere consentito in tutti i volumi padre di giunzione.
- L'opzione per il supporto VAAI deve essere impostata sul relativo server NFS.

Per ulteriori informazioni sulla procedura, fare riferimento all' ["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

La configurazione delle impostazioni di multipath e timeout del server ESXi garantisce disponibilità elevata e integrità dei dati, consentendo di passare senza problemi a un percorso di storage di backup in caso di errore di un percorso primario.

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

A seconda della configurazione e del carico di sistema, questo processo potrebbe richiedere molto tempo. L'avanzamento dell'attività viene visualizzato nel pannello Recent Tasks (attività recenti).

Fasi

1. Dalla home page del client Web VMware vSphere, selezionare **host e cluster**.
2. Fare clic con il pulsante destro del mouse su un host e selezionare **NetApp ONTAP tools > Aggiorna dati host**.
3. Nella pagina dei collegamenti del client Web VMware vSphere, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
4. Andare alla scheda **ESXi host compliance** nella panoramica (dashboard) degli strumenti ONTAP per il plug-in VMware vSphere.
5. Selezionare il collegamento **Applica impostazioni consigliate**.

6. Nella finestra **Apply Recommended host settings** (Applica impostazioni host consigliate*), selezionare gli host che si desidera aggiornare per rispettare le impostazioni consigliate da NetApp e selezionare **Next** (Avanti).



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

7. Nella pagina delle impostazioni, selezionare i valori consigliati secondo necessità.
8. 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

Utilizzando gli strumenti ONTAP per VMware vSphere, è possibile impostare timeout e altri valori sugli host ESXi per garantire le migliori prestazioni e il successo del failover. I valori dei tool ONTAP per i set VMware vSphere si basano su test NetApp interni.

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 definiscono i percorsi preferiti per i sistemi storage NetApp. Determinano quali percorsi disponibili sono ottimizzati (rispetto a quelli non ottimizzati che attraversano il cavo di interconnessione) e impostano il percorso preferito su uno di tali percorsi.

Negli ambienti a performance elevate o quando si eseguono test delle performance con un singolo datastore LUN, prendere in considerazione la possibilità di modificare l'impostazione del bilanciamento del carico della policy di selezione del percorso psp (round-robin) VMW_PSP_RR (Path Selection Policy) dall'impostazione IOPS predefinita di 1000 a un valore di 1.



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

Impostazioni NFS

| Parametro | Impostare questo valore su... |
|---------------------|-------------------------------|
| NET.TcpipelHeapSize | 32 |
| NET.TcpipelHeapMax | 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 degli utenti ONTAP

È possibile configurare nuovi ruoli e privilegi utente per la gestione dei backend di storage utilizzando il file JSON fornito con gli strumenti ONTAP per VMware vSphere e ONTAP System Manager.

Prima di iniziare

- È necessario aver scaricato il file dei privilegi di ONTAP da ONTAP Tools per VMware vSphere utilizzando https://<loadbalancerIP>:8443/Virtualization/user-Privileges/users_roles.zip.
- Il file ONTAP Privileges dovrebbe essere stato scaricato da ONTAP Tools utilizzando https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip.



È possibile creare utenti a livello di cluster o direttamente a livello di Storage Virtual Machine (SVM). Puoi anche creare utenti senza utilizzare il file `user_roles.json` e, in tal caso, devi disporre di un set minimo di privilegi a livello di SVM.

- È necessario aver effettuato l'accesso con i privilegi di amministratore per il backend di archiviazione.

Fasi

1. Estrarre il file scaricato https://<loadbalancerIP>:8443/Virtualization/user-privileges/users_roles.zip.
2. Accedere a ONTAP System Manager utilizzando l'indirizzo IP di gestione del cluster del cluster.
3. Accedere al cluster con admin Privileges. Per configurare un utente, attenersi alla procedura illustrata di seguito:
 - a. Per configurare l'utente degli strumenti ONTAP del cluster, selezionare **cluster > Impostazioni > pannello utenti e ruoli**.
 - b. Per configurare l'utente degli strumenti di SVM ONTAP, selezionare **Storage SVM > Impostazioni > pannello utenti e ruoli**.
 - c. Selezionare **Aggiungi** in utenti.
 - d. Nella finestra di dialogo **Aggiungi utente**, selezionare **prodotti di virtualizzazione**.
 - e. **Sfogliare** per selezionare e caricare il file JSON con privilegi ONTAP.

Il campo prodotto viene compilato automaticamente.
 - f. Selezionare la funzionalità desiderata dal menu a discesa funzionalità prodotto.

Il campo **ruolo** viene compilato automaticamente in base alla capacità del prodotto selezionata.
 - g. Immettere il nome utente e la password richiesti.
 - h. Selezionare il ruolo Privileges (rilevamento, creazione archivio, Modifica archivio, distruzione archivio, NAS/SAN) richiesto per l'utente, quindi selezionare **Aggiungi**.

Vengono aggiunti il nuovo ruolo e l'utente e vengono visualizzati i privilegi dettagliati nel ruolo configurato.

Requisiti di mappatura degli aggregati delle SVM

Per utilizzare le credenziali utente delle SVM per il provisioning dei datastore, i tool interni di ONTAP per VMware vSphere creano volumi nell'aggregato specificato nelle API SUCCESSIVE ai datastore. ONTAP non consente la creazione di volumi su aggregati non mappati in una SVM utilizzando le credenziali utente della SVM. Per risolvere questo problema, è necessario mappare le SVM con gli aggregati utilizzando l'API REST o la CLI di ONTAP, come descritto qui.

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

Seguire le istruzioni in questa sezione per creare manualmente l'utente e i ruoli senza utilizzare 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 di SVM ONTAP del cluster, selezionare **Storage SVM > Impostazioni > pannello utenti e ruoli**
3. Crea ruoli:
 - a. Selezionare **Aggiungi** nella tabella **ruoli**.
 - b. Immettere i dettagli **nome ruolo** e **attributi ruolo**.

Aggiungere il percorso **REST API** e il relativo accesso dal menu a discesa.
 - a. 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

In questa sezione sono elencati i privilegi minimi richiesti per gli utenti cluster con ambito globale non amministratore creati senza utilizzare il file JSON degli utenti. Se un cluster viene aggiunto nell'ambito locale, si consiglia di utilizzare il file JSON per creare gli utenti, poiché gli strumenti ONTAP per VMware vSphere richiedono più dei soli privilegi di lettura per il provisioning su ONTAP.

Utilizzo delle API:

| API | Livello di accesso | Utilizzato per |
|------------------------------|----------------------------|--|
| /api/cluster | Sola lettura | Rilevamento della configurazione del cluster |
| /api/cluster/licenze/licenze | Sola lettura | Controllo licenza per licenze specifiche del protocollo |
| /api/cluster/nodi | Sola lettura | Rilevamento del tipo di piattaforma |
| /api/security/accounts | Sola lettura | Individuazione dei privilegi |
| /api/security/ruoli | Sola lettura | Individuazione dei privilegi |
| /api/storage/aggregati | Sola lettura | Controllo dello spazio di aggregazione durante datastore/provisioning dei volumi |
| /api/storage/cluster | Sola lettura | Per ottenere i dati di spazio ed 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 di QoS e policy VM |
| /api/svm/svm | Sola lettura | Per ottenere la configurazione SVM nel caso in cui il cluster venga aggiunto localmente. |
| /api/network/ip/interfaces | Sola lettura | Aggiunta del backend dello storage - per identificare l'ambito della LIF di gestione è Cluster/SVM |

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



Servono rilevamento, creazione, modifica e distruzione di Privileges per eseguire operazioni di PATCH e rollback automatico in caso di guasto nei datastore. La mancanza di questi Privileges insieme causa interruzioni del flusso di lavoro e problemi di pulizia.

Creazione di strumenti ONTAP per l'utente basato su API VMware vSphere ONTAP con rilevamento, creazione dello storage, modifica dello storage, distruzione dello storage Privileges consente l'avvio delle rilevazioni e la gestione dei 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

```

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
```

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

Per creare un utente SVM scoped con tutta la Privileges, esegui i seguenti comandi:

```
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_
```

Per sbloccare l'account, per consentire l'accesso all'interfaccia di gestione eseguire il seguente comando:

```
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

Se i tool di ONTAP per l'utente di VMware vSphere 10,1 sono un utente con ambito cluster creato utilizzando il file json, esegui i seguenti comandi nell'interfaccia dell'interfaccia dell'interfaccia dell'interfaccia dell'utente di ONTAP utilizzando l'utente di amministrazione per l'upgrade 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
```

Se i tool di ONTAP per l'utente di VMware vSphere 10,1 sono un utente con ambito SVM creato utilizzando il file json, esegui i seguenti comandi nell'interfaccia dell'interfaccia dell'interfaccia dell'interfaccia dell'interfaccia utente di ONTAP utilizzando l'utente di amministrazione per 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>
```

Aggiungendo al ruolo esistente il comando `vserver nvme namespace show` e `vserver nvme subsystem show`, si aggiungono i seguenti comandi.

```
vserver nvme namespace create  
  
vserver nvme namespace modify  
  
vserver nvme subsystem create  
  
vserver nvme subsystem modify
```

Aggiungere un backend di storage

L'aggiunta di un backend storage ti consente di integrare un cluster ONTAP.

A proposito di questa attività

In caso di 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. Il tenant di vCenter deve integrare le Storage Virtual Machine (SVM) desiderate. In questo modo, un utente della SVM può eseguire il provisioning del datastore vVol. Puoi aggiungere storage in vCenter utilizzando la SVM.

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.

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.

Utilizzo dell'interfaccia utente del client vSphere



Durante la configurazione di un backend storage tramite l'interfaccia utente client vSphere, è importante sottolineare che il datastore vVol non supporta l'aggiunta diretta di un utente SVM.

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.



Per aggiungere direttamente un utente SVM, puoi aggiungere credenziali basate sul cluster e LIF di gestione indirizzi IPv4 e IPv6 o fornire credenziali basate su SVM con un LIF di gestione SVM.

Cosa succederà?

L'elenco viene aggiornato ed è possibile visualizzare il backend dello storage appena aggiunto nell'elenco.

Associazione di un backend dello storage a un'istanza di vCenter Server

Associare un backend dello storage con vCenter Server per creare una mappatura tra il backend dello storage e l'istanza di vCenter Server integrata a livello globale.

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. Seleziona i puntini di sospensione verticali rispetto all'istanza di vCenter Server da associare ai backend dello storage.
5. Seleziona il backend dello storage dal menu a discesa per associare l'istanza di vCenter Server al backend dello storage richiesto.

Configurare l'accesso alla rete

Se l'accesso alla rete non è stato configurato, tutti gli indirizzi IP rilevati dall'host ESXi vengono aggiunti al criterio di esportazione per impostazione predefinita. È possibile configurarlo per aggiungere alcuni indirizzi IP specifici al criterio di esportazione ed escludere il resto. Tuttavia, quando si esegue un'operazione di montaggio sugli host ESXi esclusi, l'operazione non riesce.

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 di ONTAP, selezionare **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

Quando si crea un datastore a livello di cluster host, il datastore viene creato e montato su tutti gli host della destinazione e l'azione viene attivata solo se l'utente corrente dispone dei privilegi necessari per l'esecuzione.

Creare un datastore vVol

A partire dai tool ONTAP per VMware vSphere 10,3, puoi creare un datastore vVol nei sistemi ASA R2 con efficienza in termini di spazio come thin.vVol. Il provider VASA crea un contenitore e gli endpoint del protocollo desiderati durante la creazione del datastore vVol. Questo contenitore non presenta volumi di supporto.

Prima di iniziare

- Verifica che gli aggregati root non siano mappati alla SVM.
- Assicurarsi che il provider VASA sia registrato con il vCenter selezionato.
- Nel sistema storage ASA R2, la SVM deve essere mappata all'aggregato per l'utente della 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 **NetApp ONTAP tools > Create 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. Selezionare un criterio di esportazione personalizzato per il protocollo NFS o un nome di gruppo iniziatore personalizzato per i protocolli iSCSI e FC nelle **Opzioni avanzate**.



In SVM di tipo sistema storage ASA R2, le unità storage (LUN/namespaces) non vengono create in quanto il datastore è solo un container 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.

Durante la creazione di un nuovo volume, puoi abilitare la QoS nel datastore. Per impostazione predefinita, viene creato un volume per ogni richiesta creata da LUN. Questa fase non è applicabile agli archivi dati vVol che utilizzano i sistemi di storage ASA R2.

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

Creare un datastore NFS

Un datastore NFS (Network file System) di VMware utilizza il protocollo NFS per connettere gli host ESXi a un dispositivo di storage condiviso in una rete. I datastore NFS sono comunemente utilizzati negli ambienti VMware vSphere e offrono diversi vantaggi, come semplicità e flessibilità.

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 archivio dati**.
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 necessario, scegliere **criterio di esportazione personalizzato** nelle opzioni avanzate, ma non è consigliabile. Se utilizzato, assicurati di eseguire il rilevamento in vCenter per tutti gli oggetti.



Impossibile creare un datastore NFS utilizzando la policy per i volumi root/predefinita della SVM.

- Nelle opzioni avanzate, il pulsante di commutazione **asimmetrico** è visibile solo se nel menu a discesa della piattaforma sono selezionate prestazioni o capacità.
 - Quando scegli l'opzione **any** nel menu a discesa delle piattaforme, puoi vedere le SVM che fanno parte di vCenter indipendentemente dalla piattaforma o dal flag asimmetrico.
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**.

Il datastore NFS viene creato e montato su tutti gli host.

Creare un datastore VMFS

Virtual Machine file System (VMFS) è un file system in cluster che archivia i file delle macchine virtuali negli ambienti VMware vSphere. VMFS consente a più host ESXi di accedere contemporaneamente agli stessi file della macchina virtuale, abilitando funzioni quali vMotion e High Availability.

In un cluster protetto:

- È possibile creare solo datastore VMFS. Quando si aggiunge un datastore VMFS a un cluster protetto, il datastore viene protetto automaticamente.
- Non è possibile creare un datastore in un data center con uno o più cluster host protetti.
- Non è possibile creare un datastore nell'host ESXi se il cluster host principale è protetto con una relazione di tipo "criterio duplex failover automatico" (configurazione uniforme/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 vendor della scheda di interfaccia di rete (NIC) supporta ESXi NIC con 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 di 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, attenersi alla seguente procedura per configurare l'host ESXi:
 - a. 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 **NetApp ONTAP tools > Create 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**. Se si sceglie di aggiungere il nuovo datastore a un cluster di datastore VMFS esistente, selezionare il selettore del cluster di 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 dei namespace. Il sottosistema dello spazio dei nomi viene creato utilizzando il nome generato automaticamente che include il nome del datastore. È possibile rinominare il sottosistema dello spazio dei nomi nel campo **nome sottosistema dello spazio dei nomi personalizzato** delle opzioni avanzate del riquadro **Storage**.

6. Dal riquadro **attributi di archiviazione**:
 - a. Selezionare **aggregate** dalle opzioni a discesa.



Per i sistemi di storage ASA R2, l'opzione **aggregato** non è visualizzata poiché lo storage ASA R2 è uno storage disaggregato. Quando scegli una SVM di tipo sistema storage ASA R2, la pagina degli attributi dello storage mostra le opzioni per l'abilitazione della QoS.

- b. Secondo il protocollo selezionato, viene creata un'unità di storage (LUN/namespace) con una riserva di spazio di tipo thin.
- c. Selezionare **Usa volume esistente, attiva QoS** come richiesto e fornire i dettagli.



Nel tipo di storage ASA R2, la creazione o la selezione del volume non è applicabile per la creazione di unità di storage (LUN/namespace). Pertanto, queste opzioni non sono mostrate.



Per la creazione di datastore VMFS con protocollo NVMe/FC o NVMe/TCP, non puoi utilizzare il volume esistente, devi creare un nuovo volume.

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

Il datastore VMFS viene creato e montato su tutti gli host.

Protezione di datastore e macchine virtuali

Proteggere utilizzando la protezione del cluster host

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

Assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Il cluster host contiene datastore provenienti da una sola SVM.
- Il datastore montato sul cluster host non deve essere montato su nessun host esterno al cluster.
- Tutti i datastore montati sul cluster host devono essere datastore VMFS con protocollo iSCSI/FC. I datastore vVol, NFS o VMFS con protocolli NVMe/FC e NVMe/TCP non sono supportati.
- Gli archivi dati FlexVol/LUN Form montati sul cluster host non devono far parte di alcun gruppo di coerenza (CG) esistente.
- Gli archivi dati FlexVol/LUN Forming montati sul cluster host non devono far parte di alcun rapporto SnapMirror esistente.
- Il cluster host deve avere almeno un datastore.

Fasi

1. Accedere al client vSphere
2. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **NetApp ONTAP tools > Protect Cluster**.
3. Nella finestra di protezione del cluster, il tipo di datastore e le informazioni della Storage Virtual Machine (VM) di origine vengono popolate automaticamente. Seleziona il collegamento dei datastore per visualizzare i datastore protetti.
4. Immettere il **nome del gruppo di coerenza**.
5. Selezionare **Aggiungi relazione**.
6. 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 criterio AutomatedFailOverDuplex sono presenti configurazioni host uniformi e non uniformi. Quando si seleziona il pulsante di attivazione/disattivazione **Uniform host Configuration**, la configurazione del gruppo iniziatore dell'host viene replicata implicitamente nel sito di destinazione. Per ulteriori informazioni, fare riferimento alla "[Concetti e termini chiave](#)".

7. Se si sceglie di avere una configurazione host non uniforme, selezionare l'accesso host (origine/destinazione) per ogni host all'interno di quel cluster.
8. Selezionare **Aggiungi**.

9. Nella finestra **Protect cluster** non è possibile modificare il cluster protetto durante l'operazione di creazione. È possibile eliminare e aggiungere nuovamente la protezione. Durante l'operazione Modifica protezione cluster host, è disponibile l'opzione di modifica. È possibile modificare o eliminare le relazioni utilizzando le opzioni del menu puntini di sospensione.
10. Selezionare il pulsante **Proteggi**.

Viene creata un'attività vCenter con i dettagli dell'ID lavoro e il suo avanzamento viene visualizzato nel pannello attività recenti. Si tratta di un'attività asincrona; l'interfaccia utente mostra solo lo stato di inoltro della richiesta e non attende il completamento dell'attività.
11. Per visualizzare i cluster host protetti, accedere a **NetApp ONTAP tools > protezione > Relazioni cluster host**.

Proteggere utilizzando la protezione SRA

Abilitare SRA 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](#)".
- I cluster ONTAP di origine e di destinazione devono avere le stesse pianificazioni SnapMirror personalizzate prima di eseguire i flussi di lavoro 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).

Configurare SRA per gli 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:

- Ripristino sito live di VMware

La documentazione relativa all'installazione di VMware Live Site Recovery si trova sul sito VMware.

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

- SRA

L'adattatore è installato 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 siano in igroup con l' `ostype` opzione impostata su *VMware* sul sistema di storage primario.
3. Verificare che gli host ESXi nel sito di recovery dispongano di una connettività iSCSI appropriata alla Storage Virtual Machine (SVM). Gli host ESXi del sito secondario devono avere accesso allo storage del sito secondario e gli host ESXi del sito primario devono avere accesso allo storage del sito primario.

A tale scopo, verificare che gli host ESXi abbiano LUN locali connessi alla SVM o tramite il `iscsi show initiators` comando 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:

- Ripristino sito live di VMware

La documentazione relativa all'installazione di VMware Live Site Recovery è disponibile sul sito VMware.

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

- SRA

L'adattatore viene installato 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 gli indirizzi validi, quali l'indirizzo IP, il nome host o il nome FQDN su cui sono presenti le esportazioni NFS, siano specificati nel campo **indirizzi NFS** quando si utilizza la procedura guidata di Array Manager per aggiungere array a VMware Live Site Recovery.
4. Utilizzare il `ping` comando 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 per ambienti ad alta scalabilità

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) |

Si consiglia inoltre di attivare `StorageProvider.autoResignatureMode` l'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` a un valore superiore.



L'intervallo di timeout specificato è il valore massimo. Non è necessario attendere il raggiungimento del 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

Dopo aver implementato l'appliance VMware Live Site Recovery, è necessario configurare SRA sull'appliance VMware Live Site Recovery. La corretta configurazione di SRA consente all'appliance VMware Live Site Recovery di comunicare con SRA per la gestione del disaster recovery. È necessario memorizzare gli strumenti ONTAP per le credenziali VMware vSphere (indirizzo IP) nell'appliance VMware Live Site Recovery per consentire la comunicazione tra l'appliance VMware Live Site Recovery e SRA.

Prima di iniziare

Il file `tar.gz` dovrebbe essere stato scaricato da ["Sito di supporto NetApp"](#).

A proposito di questa attività

La configurazione di SRA sull'appliance VMware Live Site Recovery memorizza le credenziali SRA

nell'appliance VMware Live Site Recovery.

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 utilizzando l'account amministratore all'appliance VMware Live Site Recovery utilizzando PuTTY.
4. Passare all'utente root utilizzando il comando: `su root`
5. Eseguire il comando `cd /var/log/vmware/srm` per accedere 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 strumenti ONTAP per l'indirizzo IP e la password di 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>`



È necessario fornire il valore della password tra virgolette singole per assicurarsi che lo script Perl non legga i caratteri speciali nella password come delimitatore dell'input.



Il nome utente e la password dell'applicazione vengono impostati durante la distribuzione di ONTAP Tools. Questo è necessario per la registrazione VASA Provider/SRA.

9. 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).

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.

Aggiornare le credenziali SRA

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.

Configurare siti protetti e di ripristino

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

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. Accedere a vCenter Server e selezionare **Site Recovery > Protection Groups**.
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 **Type**, selezionare l'opzione **Type Field...** come gruppi di datastore (replica basata su array) per NFS e datastore VMFS. Il dominio degli errori non è altro che SVM con replica abilitata. Vengono visualizzate le SVM che hanno implementato solo il peering e che non hanno 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. Selezionare il piano di ripristino esistente o 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**.

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).

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. Fare doppio clic su **Site Recovery** nella home page di vSphere Client e selezionare **Sites**.
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

I siti protetti e di ripristino vengono visualizzati nella finestra di dialogo oggetti.

Configurare le risorse protette e del sito di ripristino

Configurare le mappature di rete

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 le mappature delle cartelle

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

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 gli archivi dati segnaposto

È necessario configurare un datastore segnaposto in modo che conservi un posto nell'inventario vCenter nel sito di ripristino per la macchina virtuale protetta (VM). Non è necessario che l'archivio dati segnaposto sia grande, in quanto le macchine virtuali segnaposto sono piccole e utilizzano solo poche centinaia o meno di kilobyte.

Prima di iniziare

- È necessario aver collegato i siti protetti e di ripristino.
- È necessario configurare le mappature delle risorse.

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 essere locali o remoti e non devono essere replicati.

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

Configurare SRA utilizzando Array Manager

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 si sta effettuando la connessione a un cluster, inserire la LIF di gestione del cluster.
 - Se ci si connette direttamente a una SVM, inserire l'indirizzo IP della LIF di gestione 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 si sta effettuando la connessione a un cluster, inserire il nome della SVM nel campo **SVM name** (Nome SVM).

È anche possibile lasciare vuoto questo campo.
- 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 storage replicati

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. Accedere a **Site Recovery > Array Based Replication**.
3. Selezionare la coppia di array richiesta e verificare i dettagli corrispondenti.

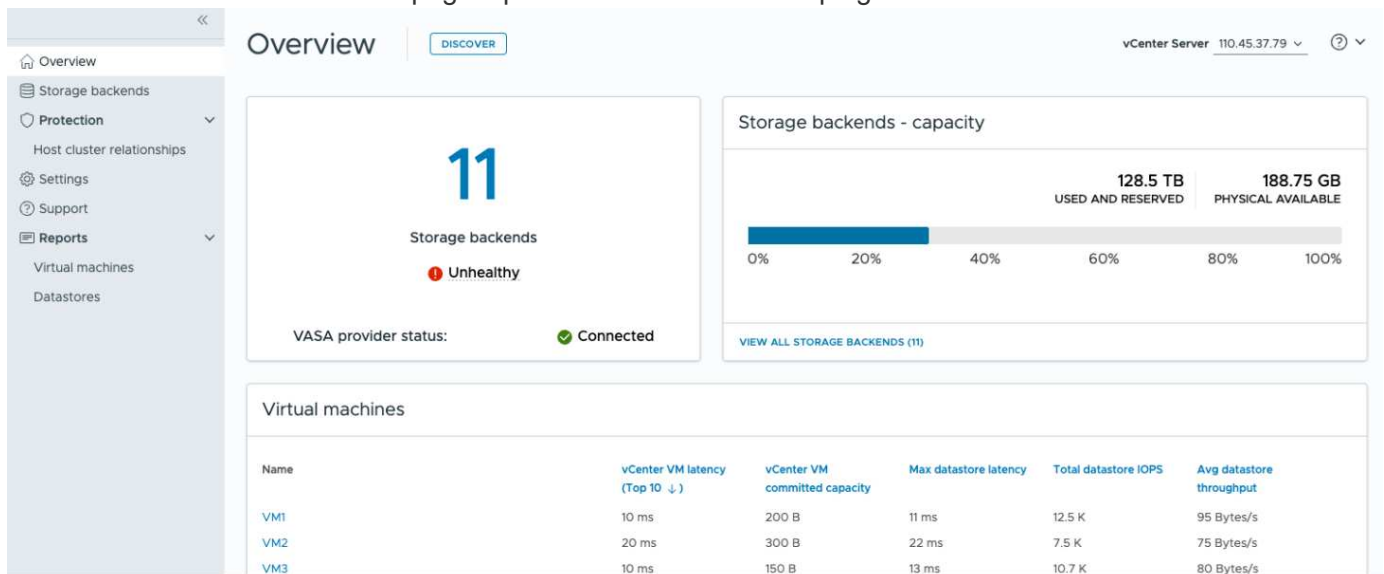
I sistemi di archiviazione devono essere rilevati nel sito protetto e nel sito di ripristino con lo stato "abilitato".

Gestisci i tool ONTAP per VMware vSphere

Panoramica dei tool ONTAP per la dashboard di VMware vSphere

Quando si seleziona l'icona degli strumenti ONTAP per il plug-in VMware vSphere nella sezione Collegamenti del client vCenter, l'interfaccia utente passa alla pagina di panoramica. Questa pagina agisce come la dashboard che fornisce il riepilogo dei tool ONTAP per il plug-in VMware vSphere.

Nel caso della configurazione della modalità di collegamento avanzata (ELM), viene visualizzato il menu a discesa vCenter Server SELECT ed è possibile selezionare un vCenter Server desiderato per visualizzare i dati pertinenti. Questo menu a discesa è disponibile per tutte le altre viste di elenco del plugin. La selezione di vCenter Server effettuata in una pagina persiste nelle schede del plug-in.



Dalla pagina di panoramica, è possibile eseguire l'azione **rilevamento**. L'azione di Discovery esegue il rilevamento a livello di vCenter per rilevare eventuali backend storage, host, datastore e stato/relazioni di protezione aggiunti o aggiornati di recente. È possibile eseguire una ricerca su richiesta delle entità senza dover attendere la ricerca pianificata.



Il pulsante di azione viene attivato solo se si dispone dei privilegi necessari per eseguire l'azione di ricerca.

Una volta inviata la richiesta di rilevamento, è possibile tenere traccia dell'avanzamento dell'azione nel pannello 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 storage per l'istanza di vCenter Server selezionata. Nel caso dei sistemi di storage ASA R2, i dati sulla capacità non vengono mostrati in quanto 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'intestazione 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'intestazione 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 lo stato di conformità generale di tutti gli host ESXi (per il vCenter selezionato) rispetto alle impostazioni dell'host NetApp consigliate per gruppo/categoria di impostazioni. È possibile selezionare il collegamento Applica impostazioni consigliate per applicare le impostazioni consigliate. È possibile selezionare lo stato di conformità degli host per visualizzare l'elenco degli host. |

Interfaccia utente di ONTAP tools Manager

I tool ONTAP per VMware vSphere sono un sistema multi-tenant in grado di gestire più istanze di vCenter Server. ONTAP Tools Manager offre un maggiore controllo ai tool

ONTAP per l'amministratore di VMware vSphere sulle istanze di vCenter Server gestite e sui backend storage integrati.

ONTAP Tools Manager aiuta a:

- Gestione delle istanze di vCenter Server: Aggiunta e gestione delle istanze di vCenter Server agli strumenti ONTAP.
- Gestione backend dello storage - Aggiungi e gestisci i cluster di storage ONTAP ai tool ONTAP per VMware vSphere e mappali alle istanze vCenter Server integrate a livello globale.
- Download dei bundle di log: Raccolta dei file di log per gli strumenti ONTAP per VMware vSphere.
- Gestione certificati - consente di modificare il certificato autofirmato in un certificato CA personalizzato e di rinnovare o aggiornare tutti i certificati del provider VASA e degli strumenti ONTAP.
- Gestione password - consente di reimpostare la password dell'applicazione OVA dell'utente.

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.

La sezione Panoramica su ONTAP tools Manager aiuta a gestire la configurazione dell'appliance, come la gestione dei servizi, l'upscaling delle dimensioni dei nodi e l'abilitazione ha (High Availability). Puoi anche monitorare le informazioni generali dei tool ONTAP relativi ai nodi, come lo stato di salute, i dettagli di rete e gli avvisi.

The screenshot shows the ONTAP Tools Manager web interface. The top navigation bar includes the ONTAP logo and the text "ONTAP tools Manager". On the right side of the navigation bar, there is a refresh icon and a user profile icon labeled "Administrator". The main content area is titled "Overview" and includes a button for "EDIT APPLIANCE SETTINGS".

The "Appliance" section displays a green checkmark and the word "Healthy". To the right, configuration details are listed:

| | |
|----------------|---------|
| Size: | Small |
| HA: | Enabled |
| VASA provider: | Enabled |
| SRA: | Enabled |

Below the appliance status is a "VIEW DETAILS" link.

The "Alerts" section shows a summary of alerts for the "Last 24 hours": 3 Error (red exclamation mark), 2 Warning (orange exclamation mark), and 5 Info (blue 'i'). A "VIEW ALL ALERTS (43)" link is provided.

The "ONTAP tools nodes" section displays three nodes:

- nodename_01**: Online, demo_vm1
- nodename_02**: Online, demo_vm2
- nodename_03**: Online, demo_vm3

Each node card includes a "VIEW DETAILS" link.

| Carta | Descrizione |
|-----------------------------|---|
| Scheda dell'appliance | La scheda dell'appliance fornisce lo stato generale dell'appliance ONTAP Tools. Mostra i dettagli di configurazione del dispositivo e lo stato dei servizi abilitati. Per ulteriori informazioni sull'appliance ONTAP Tools, selezionare il collegamento Visualizza dettagli . Quando è in corso un processo di azione di modifica delle impostazioni del dispositivo, il portlet del dispositivo mostra lo stato e i dettagli del processo. |
| Scheda avvisi | La scheda Alerts elenca gli alert dei tool ONTAP in base al tipo, compresi gli alert a livello di nodo di ha. È possibile visualizzare l'elenco degli avvisi selezionando il testo del conteggio (collegamento ipertestuale). Il collegamento indirizza l'utente alla pagina di visualizzazione degli avvisi filtrata in base al tipo selezionato. |
| Scheda nodi strumenti ONTAP | La scheda dei nodi dei tool ONTAP mostra l'elenco dei nodi con nome del nodo, nome della macchina virtuale del nodo, stato e tutti i dati relativi alla rete. È possibile selezionare on Visualizza dettagli per visualizzare i dettagli aggiuntivi relativi al nodo selezionato. [NOTA] in un setup non ha viene visualizzato un solo nodo. Nel setup ha sono mostrati tre nodi. |

Comprendere igroup e le policy di esportazione negli strumenti ONTAP per VMware vSphere

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 strumenti ONTAP per 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 strumenti ONTAP per VMware vSphere 10.x introducono gli igroup nidificati, in cui ogni datastore in vCenter è associato a un igroup padre, mentre ogni host è collegato a un igroup figlio sotto tale igroup padre. È possibile definire igroup padre personalizzati con nomi definiti dall'utente da riutilizzare su più datastore, consentendo una gestione più flessibile e interconnessa degli igroup. Comprendere il flusso di lavoro degli igroup è essenziale per gestire efficacemente LUN e datastore negli strumenti ONTAP per VMware vSphere. Flussi di lavoro diversi generano configurazioni di igroup diverse, come mostrato nei seguenti esempi:



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

| 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 |
| Customlgroup<numero> | Gruppo padre personalizzato definito dall'utente |
| Classiclgroup<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:

- DS1lgroup:
 - host1lgroup → (iqn1: lun1)

Un igroup padre DS1lgroup viene creato sui sistemi ONTAP per DS1, con un igroup figlio host1lgroup mappato a lun1. Le LUN sono sempre mappate a 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)

Viene creato un igroup figlio host2lgroup e aggiunto 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)

L'host1lgroup viene rimosso dalla gerarchia. Gli igroup figlio non vengono eliminati esplicitamente. L'eliminazione avviene in queste due condizioni: • Se non sono mappate LUN, il sistema ONTAP elimina l'igroup figlio. • Un processo di pulizia pianificato rimuove gli igroup figlio non associati a 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 se un altro datastore non riutilizza l'igroup padre. Gli igroup figlio non vengono mai 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 poiché 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 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

Le policy di esportazione controllano l'accesso ai datastore NFS negli strumenti ONTAP per VMware vSphere. Definiscono quali client possono accedere ai datastore e quali autorizzazioni dispongono. Le policy di esportazione vengono create e gestite nei sistemi ONTAP e possono essere associate ai datastore 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 strumenti ONTAP per VMware vSphere rimuovono l'indirizzo IP dell'host dalla policy di esportazione. Se nessun altro host utilizza quella policy di esportazione, questa verrà eliminata. Quando si elimina un datastore NFS, gli strumenti ONTAP per 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, mantiene l'indirizzo IP dell'host e rimane invariata. Quando si eliminano i datastore, la policy di esportazione rimuove 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, in quanto può causare problemi di accesso e latenza.

Argomenti correlati

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

Abilita i tool ONTAP per i servizi VMware vSphere

Manager consente di abilitare servizi come provider VASA, importare la configurazione vVol e il disaster recovery (SRA) utilizzando ONTAP tools Manager.

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 il provider VASA, l'importazione della configurazione vVol e il disaster recovery (SRA) in base alle proprie 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.



Prima di disabilitare i servizi opzionali, assicurarsi che i server vCenter gestiti dagli strumenti ONTAP non li utilizzino.

L'opzione **Consenti importazione della configurazione vVol** viene visualizzata solo quando il servizio provider VASA è attivato. Questa opzione consente la migrazione dei dati vVol dagli strumenti ONTAP 9.x agli strumenti ONTAP 10,3.

Modifica i tool di ONTAP per la configurazione di VMware vSphere

Utilizzando ONTAP tools Manager, scala in verticale i tool ONTAP per la configurazione di VMware vSphere per aumentare il numero di nodi nell'implementazione o modificare la configurazione in impostazione ha (High Availability). I tool ONTAP per l'appliance VMware vSphere vengono inizialmente implementati in una configurazione non ha a nodo singolo.

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.

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**, è possibile scalare in verticale per aumentare le dimensioni del nodo e abilitare la configurazione ha in base alle proprie esigenze. Sono necessarie le credenziali vCenter Server per apportare eventuali modifiche.

Quando gli strumenti ONTAP sono nella configurazione ha, puoi modificare i dettagli della libreria di contenuti. È necessario fornire nuovamente la password per la nuova modifica.



Nei tool ONTAP per VMware vSphere, è consentito solo aumentare le dimensioni del nodo, non è possibile ridurre le dimensioni del nodo. In una configurazione non ha, è supportata solo una configurazione di dimensioni medie. In un'impostazione ha sono supportate le configurazioni di medie e grandi dimensioni.

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.



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

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.



La maggior parte delle opzioni di input sono precompilate con i dettagli della rete del nodo 1 per semplificare il flusso di lavoro. Tuttavia, è possibile modificare i dati di input prima di passare alla pagina finale della procedura guidata. È possibile immettere i dettagli dell'indirizzo IPv6 per gli altri due nodi solo quando l'indirizzo IPv6 è attivato sul primo nodo.

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. Utilizzando l'ID lavoro, è anche possibile tenere traccia dello stato del lavoro di modifica delle impostazioni del dispositivo dalla vista processi.

In caso di errore dell'implementazione ha e lo stato del nuovo nodo diventa "nuovo", elimina la nuova VM in vCenter prima di riprovare l'operazione di abilitazione ha.

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

Gestire i datastore

Montare datastore NFS e VMFS

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.

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.
- L'opzione mount datastore è disabilitata quando il cluster di 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 i datastore NFS/VMFS su host o cluster host, fare clic con il pulsante destro del mouse e selezionare **NetApp ONTAP tools > Mount Datastores**.
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.

Smontare i datastore NFS e VMFS

L'azione del datastore smonta un datastore NFS o VMFS dagli host ESXi. L'azione di disinstallazione del datastore è abilitata per i datastore NFS e VMFS, rilevati o gestiti dai tool ONTAP per 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 **Unmount datastore**.

Viene visualizzata una finestra di dialogo che elenca gli host ESXi su cui è montato il datastore. Quando l'operazione viene eseguita su un archivio dati 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 l'archivio dati protetto non è montato, l'impostazione di protezione in uscita potrebbe causare una protezione parziale. Fare riferimento a ["Modificare il cluster host protetto"](#) per abilitare la protezione completa.

Quali sono le prossime novità?

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

Montare un datastore vVols

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.

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**.

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

Ridimensionare il datastore NFS e VMFS

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 di un datastore NFS e VMFS. Un volume FlexVol che fa parte di un datastore NFS e VMFS non può ridursi al di sotto delle dimensioni esistenti, ma può crescere 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, specificare una nuova dimensione per l'archivio dati e selezionare **OK**.

Espandere il datastore vVol

Quando si fa clic con il pulsante destro del mouse sull'oggetto del datastore nella vista oggetto vCenter, gli strumenti ONTAP per le azioni supportate da VMware vSphere vengono visualizzati nella sezione del plug-in. Le azioni specifiche vengono attivate in base al tipo di datastore e ai privilegi dell'utente corrente.



L'operazione del datastore Expand vVol non è applicabile al datastore vVol basato su 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 o scegliere tra quelli esistenti. L'interfaccia utente è autoesplicativa. Seguire le istruzioni a scelta.
5. Nella finestra **Riepilogo**, rivedere le selezioni e selezionare **Espandi**. È possibile tenere traccia dell'avanzamento nel pannello attività recenti.

Restringere il datastore vVol

L'azione Elimina archivio dati elimina il datastore quando non sono presenti vVol nel datastore selezionato.



L'operazione del datastore Shrink vVol non è supportata per il datastore vVol basato su 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 dispongono di vVol e selezionare **Rimuovi**.



L'opzione per selezionare il volume su cui risiedono i vVol è disattivata.

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 datastore

La rimozione dello storage dall'azione del datastore è supportata su tutti i tool ONTAP per i datastore vVol VMware vSphere rilevati o gestiti in vCenter Server. Questa azione consente la rimozione di volumi dal datastore vVol.

L'opzione di rimozione è disattivata quando sono presenti vVol su un volume specifico. Oltre a rimuovere i volumi dal datastore, puoi eliminare il volume selezionato sullo storage ONTAP.

Eliminare l'attività del datastore dai tool ONTAP per VMware vSphere in vCenter Server esegue le seguenti operazioni:

- Smonta il container vVol.
- Pulisce l'igroup. Se igroup non viene utilizzato, rimuove iqn dall'igroup.
- Elimina il contenitore Vvol.
- Lascia i volumi Flex nell'array di storage.

Segui i passaggi riportati di seguito per eliminare il datastore NFS, VMFS o vVOL dagli strumenti ONTAP da vCenter Server:

Fasi

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



Non è possibile eliminare gli archivi dati se ci sono macchine virtuali che utilizzano tale archivio dati. Prima di eliminare l'archivio dati, è necessario spostare le macchine virtuali in un altro datastore. Non è possibile selezionare la casella di controllo Elimina volume se il datastore appartiene a un cluster di host protetto.

- a. Nel caso del datastore NFS o VMFS, viene visualizzata una finestra di dialogo con l'elenco delle macchine virtuali che utilizzano il datastore.
 - b. Se il datastore VMFS viene creato sui sistemi ASA R2 e fa parte della protezione, devi rimuovere la protezione dal datastore prima di eliminarlo.
 - c. Nel caso dell'archivio dati vVol, l'azione Elimina archivio dati elimina l'archivio dati solo quando non vi sono vVol associati. La finestra di dialogo Elimina datastore offre un'opzione per eliminare i volumi dal cluster ONTAP.
 - d. Nel caso del datastore vVol basato su sistemi ASA R2, la casella di controllo per eliminare i volumi di backup non è applicabile.
3. Per eliminare i volumi di backup sull'archiviazione ONTAP, selezionare **Elimina volumi sul cluster ONTAP**.



Impossibile eliminare il volume sul cluster ONTAP per un datastore VMFS che fa parte del cluster host protetto.

Viste dello storage ONTAP per datastore

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

Fasi

1. Dal client vSphere, accedere al datastore.
2. Selezionare la scheda **Configura** nel riquadro di destra.
3. Selezionare **NetApp ONTAP tools > archiviazione ONTAP**. A seconda del tipo di datastore, la vista cambia. Fare riferimento alla tabella seguente per informazioni:

| Tipo datastore | Informazioni disponibili |
|----------------|---|
| Datastore NFS | La pagina Dettagli archiviazione contiene backend di archiviazione, informazioni di aggregazione e volume. La pagina dei dettagli di NFS contiene dati correlati al datastore NFS. |
| Datastore VMFS | La pagina Dettagli archiviazione contiene informazioni di backend, aggregato e volume di archiviazione. La pagina dettagli LUN contiene i dati relativi al LUN. La pagina namespace details contiene dati relativi al namespace quando il datastore VMFS utilizza il protocollo NVMe/TCP o NVMe/FC. I dettagli del volume e dell'aggregato non vengono visualizzati per i datastore basati sul sistema storage ASA R2. |
| Datastore vVol | Elenca tutti i volumi. È possibile espandere o rimuovere lo spazio di archiviazione dal riquadro di archiviazione di ONTAP. Questa vista non è supportata per il datastore vVol basato sul sistema ASA R2. |

Vista dello storage della macchina virtuale

La vista storage mostra l'elenco dei vVol creati dalla macchina virtuale.



Questa vista è applicabile alla macchina virtuale su cui è montato almeno un disco correlato al datastore vVol gestiti da ONTAP per VMware vSphere.

Fasi

1. Dal client vSphere, passare 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 storage

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 di ONTAP, selezionare **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 consigliati, ovvero 80 per quasi pieno e 90 per completo.

Gestire i back-end dello storage

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

Rileva lo storage

È possibile eseguire il rilevamento di un backend storage on-demand senza attendere un rilevamento pianificato per aggiornare i dettagli dello storage.

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 di ONTAP, accedere a **backend di archiviazione** e selezionare 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

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 di ONTAP, accedere a **backend di archiviazione** e selezionare 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.

È possibile eseguire l'operazione di modifica per i cluster ONTAP globali utilizzando ONTAP Tools Manager seguendo la procedura riportata di seguito.

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 dello storage, occorre eliminare tutti gli archivi dati collegati al back-end dello storage. Per rimuovere un backend dello storage, procedere come segue.

1. Accedere al client vSphere
2. Nella pagina Collegamenti, selezionare **NetApp ONTAP tools** nella sezione dei plug-in.
3. Nel riquadro sinistro degli strumenti di ONTAP, accedere a **backend di archiviazione** e selezionare un backend di archiviazione.
4. Selezionare il menu ellissi verticali e selezionare **Rimuovi**. Assicurarsi che lo storage backend non contenga datastore. È possibile tenere traccia dell'avanzamento nel pannello 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

La pagina del backend di archiviazione elenca tutti i backend di archiviazione. Puoi eseguire operazioni di rilevamento dello storage, modifica e rimozione sui backend dello storage aggiunti, non su una singola SVM figlio sotto il cluster.

Selezionando il cluster padre o il figlio nel back-end dello storage, è possibile visualizzare il riepilogo generale del componente. Selezionando il cluster padre, sarà disponibile il menu a discesa delle azioni da cui è possibile eseguire le operazioni di rilevamento, modifica e rimozione.

La pagina di riepilogo fornisce i seguenti dettagli:

- Stato del backend dello storage
- Informazioni sulla capacità
- Informazioni di base sulla macchina virtuale
- Informazioni di rete quali l'indirizzo IP e la porta della rete. Per la SVM secondaria, le informazioni saranno identiche al back-end dello storage di origine.
- Privilegi consentiti e limitati per il backend di archiviazione. Per la SVM secondaria, le informazioni saranno identiche al back-end dello storage di origine. I privilegi vengono visualizzati solo nei backend di storage basati su cluster. Se Aggiungi SVM come back-end dello storage, le informazioni sui privilegi non verranno visualizzate.
- La vista dettagliata del cluster di ASA R2 non include la scheda dei Tier locali quando la proprietà disaggregata viene impostata su "true" per la 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

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. Modificare i dettagli dell'istanza di vCenter Server e selezionare **Modifica**.

Rimuovere un'istanza di vCenter Server

Prima di rimuoverlo, devi rimuovere tutti i backend dello storage collegati a vCenter Server.

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 sul vCenter Server che si desidera rimuovere e selezionare **Rimuovi**.



Una volta rimosse le istanze di vCenter Server, queste non verranno 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.

Gestire i certificati

Per impostazione predefinita, durante la distribuzione viene generato un certificato autofirmato per gli strumenti ONTAP e per il provider VASA. Utilizzando l'interfaccia di gestione degli strumenti di ONTAP, è possibile rinnovare il certificato o aggiornarlo a una CA personalizzata. I certificati CA personalizzati sono obbligatori in una distribuzione multi-vCenter.

Prima di iniziare

- Il nome di dominio su cui viene rilasciato il certificato deve essere mappato all'indirizzo IP virtuale.
- Eseguire il controllo nslookup sul nome di dominio per verificare se il dominio viene risolto all'indirizzo IP

desiderato.

- I certificati devono essere creati con il nome del dominio e l'indirizzo IP del bilanciatore del carico.



Un indirizzo IP di loadbalancer deve essere mappato a un nome di dominio completo (FQDN). I certificati devono contenere lo stesso FQDN mappato all'indirizzo IP di loadbalancer nei 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. Immettere il nome di dominio per il quale è stato generato il certificato e aggiornare 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. Immettere il nome di dominio per il quale è stato generato il certificato e aggiornare 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


Panoramica dei tool ONTAP per la console di manutenzione VMware vSphere

È possibile gestire applicazioni, sistemi e configurazioni di rete utilizzando la console di manutenzione degli strumenti ONTAP. È possibile modificare la password di amministratore e la password di manutenzione. È inoltre possibile generare pacchetti di supporto, impostare diversi livelli di log, visualizzare e gestire le configurazioni TLS e avviare la diagnostica remota.

È necessario disporre di strumenti VMware installati dopo la distribuzione degli strumenti ONTAP per VMware vSphere per accedere alla console di manutenzione. `maint` Per accedere alla console di manutenzione degli strumenti ONTAP, è necessario utilizzare come nome utente e password configurati durante la distribuzione. Si consiglia di utilizzare **nano** per modificare i file in manutenzione o nella console di login principale.



È necessario impostare una password per l' `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. Modificare il livello di REGISTRAZIONE per servizi provider VASA e servizi SRA3. Disattiva AutoSupport4. Aggiorna URL proxy AutoSupport |
| 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. Aggiungere un nuovo server NTP6. Aumentare la dimensione del disco jail (/jail)7. Eseguire l'upgrade8. 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 remoto alla diagnostica

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

Prima di iniziare

L'estensione del provider VASA deve essere abilitata per l'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 rimane valida solo fino alla 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 Support and Diagnostics (supporto e diagnostica).
4. Inserire 2 per selezionare attiva accesso diagnostica remota.
5. Immettere y nella finestra di dialogo Conferma per abilitare l'accesso alla diagnostica remota.
6. Inserire una password per l'accesso remoto alla diagnostica.

Avviare SSH su altri nodi

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

Prima di iniziare

L'estensione del provider VASA deve essere abilitata per l'istanza di vCenter Server.

A proposito di questa attività

Eseguire questa procedura su ciascun nodo prima di eseguire l'aggiornamento.

Fasi

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

Aggiornare le credenziali vCenter Server e ONTAP

È possibile aggiornare l'istanza di vCenter Server e le credenziali ONTAP utilizzando 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 sono state modificate le credenziali per vCenter Server, ONTAP o Data LIF dopo la distribuzione, è necessario aggiornare le credenziali 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. Immettere 9 per modificare le credenziali ONTAP.
5. Immettere 10 per modificare le credenziali vCenter.

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 sulle macchine virtuali mostra l'elenco delle macchine virtuali rilevate (deve avere almeno un disco da datastore basati sullo storage ONTAP) con metriche di performance. Quando si espande il record della macchina virtuale, vengono visualizzate tutte le informazioni relative al datastore del disco.

Il report sui datastore mostra l'elenco dei tool ONTAP rilevati o riconosciuti per gli archivi dati gestiti VMware vSphere, su cui viene eseguito il provisioning dal back-end dello storage ONTAP, di tutti i tipi con metriche delle performance.

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

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. Fornire l'etichetta del bundle di log e generare il bundle di log. È possibile visualizzare l'opzione di download quando vengono generati i 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.

Gestire le macchine virtuali

Considerazioni per migrare o clonare macchine virtuali

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 la macchina virtuale viene migrata su un volume FlexVol diverso, anche il rispettivo file di metadati viene aggiornato con le informazioni della macchina virtuale. Se una macchina virtuale viene migrata su un host ESXi diverso ma sullo stesso storage, il file di metadati del volume FlexVol sottostante non verrà modificato.

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 le macchine virtuali clonate su 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.

Inoltre, non è possibile proteggere le macchine virtuali non protette che dispongono di snapshot di memoria. Per questa release, si prevede di eliminare lo snapshot di memoria prima di attivare la protezione per la macchina virtuale.

Per Windows VM con tipo di storage ASA R2, quando si crea una snapshot della macchina virtuale, si tratta di uno snapshot di sola lettura. In caso di chiamata all'accensione per la VM, il provider VASA crea una LUN

utilizzando lo snapshot di sola lettura, quindi la abilita per gli IOPS. Durante la richiesta di spegnimento, il provider VASA elimina il LUN creato, quindi disattiva gli IOPS.

Migrazione di macchine virtuali con datastore NFS e VMFS in datastore vVol

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 vVol ti consentono di soddisfare i requisiti maggiori dei carichi di lavoro.

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. Seleziona un formato di dischi virtuali, una policy storage delle macchine virtuali e un datastore vVol corrispondente alle funzionalità del datastore che stai migrando.
4. Controllare le impostazioni e selezionare **fine**.

Pulizia VASA

Attenersi alla procedura descritta in questa sezione per eseguire la pulizia VASA.



Si consiglia di rimuovere qualsiasi datastore vVol prima di eseguire 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.

Rilevamento di host e sistemi storage

Quando si eseguono per la prima volta i tool ONTAP per VMware vSphere in un client vSphere, i tool ONTAP rilevano gli host ESXi, le loro LUN e le esportazioni NFS e i sistemi storage NetApp che gestiscono tali LUN ed esportazioni.

Prima di iniziare

- Tutti gli host ESXi devono essere accesi e connessi.
- Tutte le Storage Virtual Machine (SVM) da rilevare devono essere in esecuzione e ogni nodo del cluster deve avere almeno una LIF dati configurata per il protocollo storage in uso (NFS o iSCSI).

A proposito di questa attività

È possibile scoprire nuovi sistemi storage o aggiornare le informazioni sui sistemi storage esistenti per ottenere le informazioni più aggiornate sulla capacità e sulla configurazione in qualsiasi momento. Puoi anche modificare le credenziali utilizzate dai tool di ONTAP per VMware vSphere per accedere ai sistemi 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 centro dati desiderato e selezionare **NetApp ONTAP tools > Update host Data** (Strumenti **aggiornamento 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 di archiviazione 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

È possibile utilizzare la dashboard dei tool ONTAP per VMware vSphere per modificare le impostazioni dell'host ESXi.

Prima di iniziare

Se si verifica un problema con le impostazioni dell'host ESXi, il problema viene visualizzato nel portlet dei sistemi host ESXi della dashboard. È possibile selezionare il problema per visualizzare il nome host o l'indirizzo IP dell'host ESXi che presenta il problema.

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 **Apply Recommended host settings** (Applica impostazioni host consigliate), selezionare gli host che si desidera rispettare con le impostazioni dell'host consigliate da NetApp e selezionare **Next** (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. Effettua l'accesso con i tool ONTAP per le credenziali di amministratore di VMware vSphere fornite durante l'implementazione.
3. Selezionare l'icona **amministratore** nell'angolo superiore destro della schermata e selezionare **Modifica password**.
4. Nella finestra a comparsa Modifica password, immettere i dettagli della vecchia password e della nuova password. Il vincolo per la modifica della password viene visualizzato sulla schermata dell'interfaccia utente.
5. Selezionare **Modifica** per implementare le modifiche.

Reimpostare la password di gestione degli strumenti ONTAP

Se hai dimenticato la password di ONTAP Tools Manager, puoi reimpostare le credenziali di amministratore utilizzando il token generato dagli strumenti ONTAP per la console di manutenzione di VMware vSphere.

Fasi

1. Avviare Gestione strumenti ONTAP da un browser Web:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Nella schermata di accesso, selezionare l'opzione **Reimposta password**.

Per reimpostare la password di Manager, è necessario generare il token di reimpostazione utilizzando gli strumenti ONTAP per la console di manutenzione di VMware vSphere.

- a. Da vCenter Server, aprire la console di manutenzione
 - b. Immettere '2' per selezionare l'opzione Configurazione di sistema
 - c. Immettere '3' per modificare la password utente 'Mainta'.
3. Nella finestra a comparsa di modifica della password, immettere il token di reimpostazione della password, il nome utente e i dettagli della nuova password.
 4. Selezionare **Reimposta** per implementare le modifiche. Una volta reimpostata correttamente la password, è possibile utilizzare la nuova password per accedere.

Reimpostare la password utente dell'applicazione

La password utente dell'applicazione viene utilizzata per la registrazione SRA e VASA Provider con 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 **Impostazioni** dalla barra laterale.
4. Nella schermata **credenziali VASA/SRA**, selezionare **Reimposta password**.
5. Fornire una nuova password e confermarla.
6. Selezionare **Reimposta** per implementare le modifiche.

Reimpostare la password utente della console di manutenzione

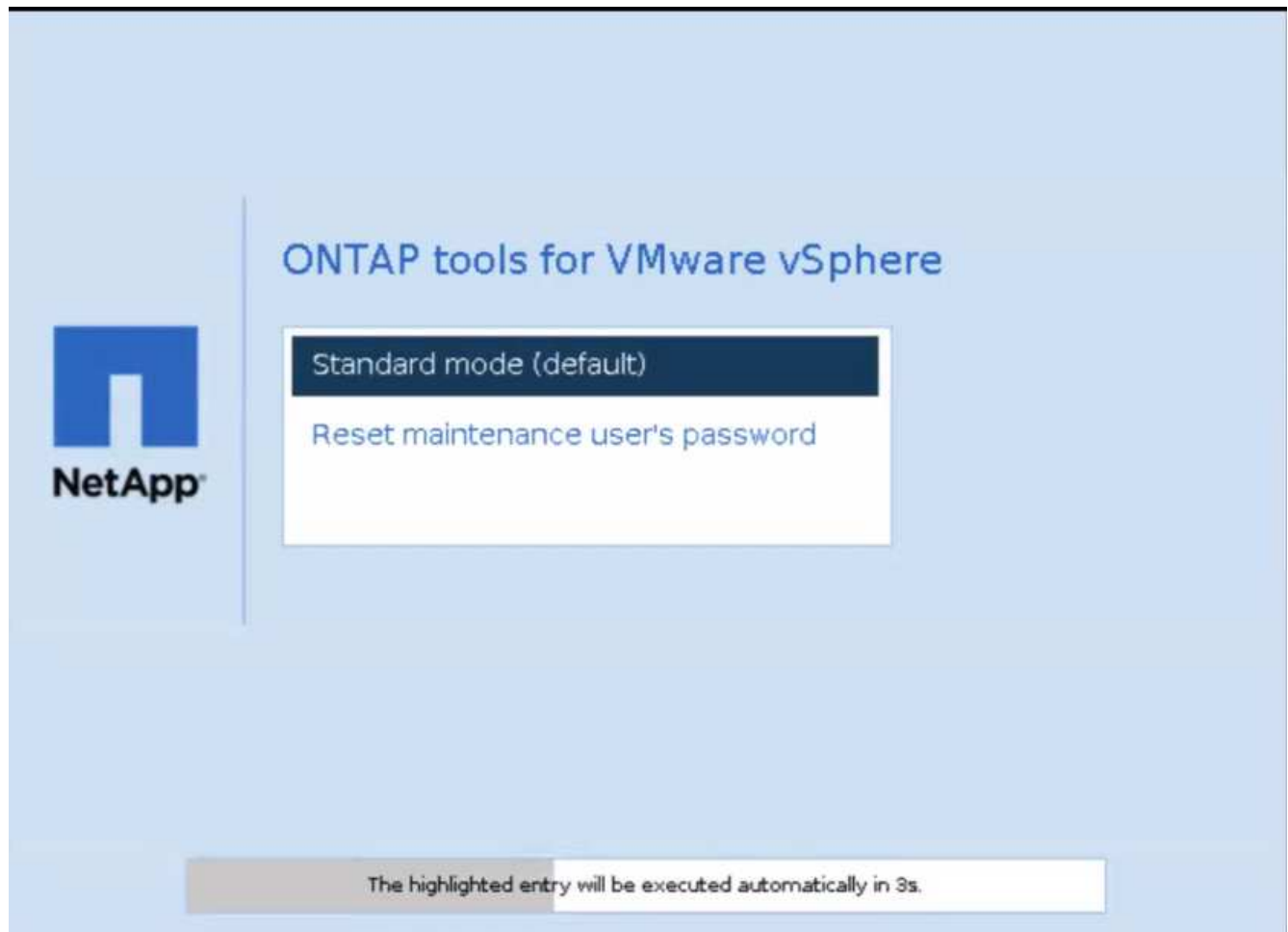
Durante l'operazione di riavvio del sistema operativo guest, il menu GRUB visualizza un'opzione per ripristinare la password utente della console di manutenzione. Questa opzione viene utilizzata per aggiornare la password utente della console di manutenzione presente sulla VM corrispondente. Una volta completata la reimpostazione della password, la VM viene riavviata per impostare la nuova password. Nello scenario di distribuzione ha, dopo il riavvio della VM, la password viene aggiornata automaticamente sulle altre due VM.



Per gli strumenti ONTAP per la distribuzione VMware vSphere HA, è necessario modificare la password utente della console di manutenzione sul primo nodo, 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 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, immettere i dettagli della nuova password. Per reimpostare correttamente la password, i dettagli della nuova password e della nuova password devono corrispondere. Hai tre possibilità di inserire la password corretta. Il sistema si riavvia dopo aver inserito correttamente la nuova password.
5. Premere Invio per continuare. La password viene aggiornata sulla macchina virtuale.



Lo stesso menu di GRUB viene visualizzato anche all'accensione della VM. Tuttavia, è necessario utilizzare l'opzione Reimposta password solo con l'opzione **Riavvia sistema operativo guest**.

Gestire la protezione dei cluster di host

Modificare il cluster host protetto

È possibile eseguire le seguenti attività come parte della protezione delle modifiche. È possibile eseguire tutte le modifiche nello stesso flusso di lavoro.

- Aggiungere 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.

Monitoraggio della protezione dei cluster host

Utilizzare questa procedura per monitorare lo stato della protezione del cluster host. Puoi monitorare ogni cluster host protetto insieme al relativo stato di protezione, ai rapporti SnapMirror, ai datastore e allo stato SnapMirror corrispondente.

Fasi

1. Accedere al client vSphere
2. Accedere a **NetApp ONTAP tools > protezione > host cluster relations**.

L'icona sotto la colonna protezione mostra lo stato della protezione

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

Aggiungere nuovi datastore o host

Utilizzare questa procedura per proteggere gli archivi dati o gli host appena aggiunti. È possibile aggiungere nuovi host al cluster protetto o creare nuovi datastore nel cluster host utilizzando l'interfaccia utente nativa 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. Accedere a **NetApp ONTAP tools > protezione > host cluster relations**, selezionare il menu puntini di sospensione sul cluster e selezionare **Modifica** o.
 - b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **NetApp ONTAP tools > Protect Cluster**.
3. Se è stato creato un datastore nell'interfaccia utente nativa di vCenter, tale datastore viene visualizzato come non protetto. L'interfaccia utente mostra tutti gli archivi dati nel cluster e il relativo stato di protezione in una finestra di dialogo. Selezionare il pulsante **PROTECT** per abilitare la protezione completa.
4. Se è stato aggiunto un nuovo host ESXi, lo stato di protezione viene visualizzato come parzialmente protetto. Selezionare il menu puntini di sospensione nelle impostazioni SnapMirror e selezionare **Modifica** per impostare la prossimità dell'host ESXi appena aggiunto.



In caso di relazione di tipo asincrono, l'azione di modifica non è supportata in quanto non è possibile aggiungere la SVM di destinazione per il terzo sito alla stessa istanza dei tool ONTAP. Tuttavia, puoi utilizzare il System Manager o l'interfaccia a riga di comando della SVM di destinazione per modificare la configurazione della relazione.

5. Selezionare **Salva** dopo aver apportato le modifiche necessarie.
6. Le modifiche sono visibili nella finestra **Proteggi cluster**.

Viene creata un'attività vCenter ed è possibile tenere traccia dell'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. Accedere a **NetApp ONTAP tools > protezione > host cluster relations**, selezionare il menu puntini di sospensione sul cluster e selezionare **Modifica** o.
 - b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **NetApp ONTAP tools > Protect 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**.

Viene creata un'attività vCenter ed è possibile tenere traccia dell'avanzamento nel pannello **attività recente**.

Eliminare una relazione SnapMirror esistente

Per eliminare una relazione SnapMirror asincrona, occorre aggiungere una SVM o un cluster del sito secondario come backend dello storage sui tool ONTAP per VMware vSphere. Non è possibile eliminare tutte le relazioni SnapMirror. Quando elimini una relazione, viene rimossa anche la rispettiva relazione sul cluster ONTAP. Quando si elimina una relazione SnapMirror AutomatedFailOverDuplex, gli archivi dati sulla destinazione non vengono mappati e il gruppo di coerenza, i LUN, i volumi e gli igroup vengono rimossi dal cluster ONTAP di destinazione.

L'eliminazione della relazione attiva una nuova scansione sul sito secondario per rimuovere il LUN non mappato 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. Accedere a **NetApp ONTAP tools > protezione > host cluster relations**, selezionare il menu puntini di sospensione sul cluster e selezionare **Modifica** o.
 - b. Fare clic con il pulsante destro del mouse su un cluster host e selezionare **NetApp ONTAP tools > Protect Cluster**.
3. Selezionare il menu puntini di sospensione nelle impostazioni SnapMirror e selezionare **Elimina**.

Viene creata un'attività vCenter ed è possibile tenere traccia dell'avanzamento nel pannello **attività recente**.

Modificare una relazione SnapMirror esistente

Per modificare una relazione di SnapMirror asincrona, occorre aggiungere la SVM o il cluster del sito secondario come backend dello storage sui tool ONTAP per VMware vSphere. Se si tratta di una relazione SnapMirror AutomatedFailOverDuplex, è possibile modificare la prossimità dell'host in caso di configurazione uniforme e l'accesso all'host in caso di configurazione non uniforme. Non è possibile scambiare i tipi di criteri Asynchronous e AutomatedFailOverDuplex. Puoi impostare la prossimità o l'accesso per gli host appena rilevati sul cluster.



Non è possibile modificare una relazione SnapMirror asincrona esistente.

Fasi

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

Viene creata un'attività vCenter ed è possibile tenere traccia dell'avanzamento nel pannello **attività recente**.

Rimozione della protezione del cluster host

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

Fasi

1. Per visualizzare i cluster host protetti, accedere a **NetApp ONTAP tools > protezione > Relazioni cluster host**.

In questa pagina, puoi monitorare i cluster host protetti insieme al relativo stato di protezione, alla relazione SnapMirror e al relativo stato SnapMirror.

2. Nella finestra **protezione cluster host**, selezionare il menu puntini di sospensione sul cluster, quindi selezionare **Rimuovi protezione**.

Disattiva AutoSupport

Quando si configura il sistema di archiviazione per la prima volta, AutoSupport viene attivato per impostazione predefinita. Invia messaggi al supporto tecnico 24 ore dopo l'attivazione. Quando disabiliti AutoSupport, non riceverai più supporto e monitoraggio proattivi.



Si consiglia di tenere attivato AutoSupport. Aiuta a velocizzare il rilevamento e la risoluzione dei problemi. Il sistema raccoglie le informazioni AutoSupport e le memorizza localmente, anche quando è disattivato.

Fasi

1. Da vCenter Server, aprire la console di manutenzione.
2. Accedere come utente di manutenzione.
3. Immettere 1 per selezionare **Configurazione applicazione**.
4. Immettere 3 per selezionare **Disattiva AutoSupport**.
5. Immettere y nella finestra di dialogo di conferma.

Aggiorna URL proxy AutoSupport

Aggiornare l'URL del proxy AutoSupport per garantire il corretto funzionamento della funzione AutoSupport negli scenari in cui viene utilizzato un server proxy per il controllo dell'accesso alla rete o per le misure di protezione. Consente ai dati AutoSupport di essere instradati attraverso il proxy appropriato, garantendo trasmissione e conformità sicure.

Fasi

1. Da vCenter Server, aprire la console di manutenzione.
2. Accedere come utente di manutenzione.
3. Immettere 1 per selezionare **Configurazione applicazione**.
4. Immettere 4 per selezionare **Aggiorna URL proxy AutoSupport**.
5. Immettere l'URL proxy.

Creare un backup e ripristinare la configurazione

Poiché i tool ONTAP per VMware vSphere 10,3 utilizzano il provisioner di storage dinamico, non puoi ottenere RPO pari a zero. Tuttavia, puoi ottenere un RPO prossimo allo zero. Per ottenere un RPO prossimo allo zero, è necessario creare un backup del setup e ripristinarlo su una nuova macchina virtuale.

Creare il backup e scaricare il file di backup

Fasi

1. Da vCenter Server, aprire la console di manutenzione.
2. Accedere come utente di manutenzione.
3. Immettere 4 per selezionare **supporto e diagnostica**.
4. Immettere 3 per selezionare l'opzione **Abilita backup di sistema**.
5. In caso di non ha, immettere le credenziali vCenter in cui viene implementata la macchina virtuale degli strumenti ONTAP.
6. Immettere il valore della frequenza di backup compreso tra 5-60 minuti.
7. Premere **Invio**

Questo crea il backup e lo invia all'archivio dati della macchina virtuale a intervalli regolari.

8. Per accedere al backup, accedere alla sezione storage e selezionare l'archivio dati della macchina virtuale
9. Selezionare la sezione **file**.

Nella sezione file, è possibile visualizzare la directory. Il nome della directory sarà l'indirizzo IP di ONTAP tools dove i punti (.) sono sostituiti da caratteri di sottolineatura, con il suffisso *backup*.

10. Per ulteriori informazioni sul backup, scaricare il file backup_info.txt da **file > Download**.

Ripristinare

Per ripristinare la configurazione, spegnere la macchina virtuale esistente e installare una nuova macchina virtuale utilizzando l'OVA utilizzato nella distribuzione iniziale.

Devi utilizzare lo stesso indirizzo IP degli strumenti ONTAP (IP del bilanciamento del carico) per la nuova macchina virtuale e la configurazione del sistema come i servizi abilitati, le dimensioni del nodo e la modalità ha deve essere uguale all'implementazione iniziale.

Per ripristinare la configurazione dal file di backup, procedere come segue.

1. Da vCenter Server, aprire la console di manutenzione.
2. Accedere come utente di manutenzione.
3. Immettere 4 per selezionare **supporto e diagnostica**.
4. Immettere 2 per selezionare l'opzione **attiva accesso diagnostico remoto** e creare una nuova password per l'accesso diagnostico.
5. Selezionare un backup qualsiasi dalla directory scaricata. Il nome del file di backup più recente viene registrato nel file *backup_info.txt*.
6. Eseguire il comando riportato di seguito per copiare il backup sulla nuova macchina virtuale e immettere la password diagnostica quando richiesto.

```
scp <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.

7. Dopo aver copiato il file di backup, accedere alla shell di diagnostica ed eseguire il comando seguente:

```
sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
```

I log vengono registrati nel file */var/log/post-deploy-upgrade.log*.

8. Dopo avere completato con successo il recovery, vengono ripristinati i servizi e gli oggetti vCenter.

Disinstallare gli strumenti ONTAP per VMware vSphere

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 alla sezione ["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. Spegnere 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

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. Determinare gli strumenti ONTAP per il tipo di distribuzione VMware vSphere dalla prima VM del nodo.

```
cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol
```

Se si tratta di una distribuzione iSCSI, è necessario eliminare anche gli igroup.

2. Ottieni l'elenco di FlexVol Volumes.

```
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. Elimina i volumi FlexVol da Gestione sistema di ONTAP. Fare riferimento alla "[Eliminare un volume FlexVol](#)". Nel comando CLI per eliminare un volume, fornire il nome esatto dei volumi FlexVol.
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 dai tool ONTAP per VMware vSphere 10.x alla 10,3

L'upgrade è supportato per le implementazioni ha e non ha. I percorsi di aggiornamento supportati sono:

| Dai tool ONTAP per la configurazione di VMware vSphere 10,1 e 10,2 | Ai tool ONTAP per la configurazione di VMware vSphere 10,3 |
|--|--|
| Non ha piccolo | Non ha e avanzato piccolo |
| Terreno non ha | Non ha e terreno avanzato |
| Avanzato piccolo | Non ha e avanzato piccolo |
| Supporto avanzato | Non ha e terreno avanzato |
| HA piccolo | HA piccolo |
| HA medio | HA medio |
| HA grande | HA grande |



Sono supportati gli upgrade dai tool ONTAP per VMware vSphere 10,1 e 10,2 alla versione 10,3. Gli aggiornamenti diretti dagli strumenti ONTAP da 10,0 a 10,3 non sono supportati.

Prima di iniziare

Per un aggiornamento non ha, spegnere la VM degli strumenti ONTAP e, per un aggiornamento ha, spegnere il primo nodo prima di apportare le seguenti modifiche alle impostazioni della macchina virtuale (VM).

- Aggiungere un disco rigido aggiuntivo da 100 GB a ciascun nodo, poiché i dati del servizio vengono memorizzati localmente sulla VM.
- Modificare la CPU e la memoria per la macchina virtuale spenta in base al tipo di implementazione. Abilitare l'hot plug per CPU e RAM.

| 10,3 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 |

- ACCENDERE la macchina virtuale dopo aver apportato le modifiche e attendere che i servizi diventino operativi.

- In caso di implementazione ha, apportare le modifiche alle risorse, abilitare il plug-in hot per CPU e RAM e aggiungere dischi rigidi da 100 GB anche per il secondo e il terzo nodo. Non è necessario riavviare questi nodi.
- Se l'appliance è stata implementata come percorso locale (facile implementazione) con gli strumenti ONTAP 10,1 o 10,2, è necessario creare uno snapshot di pausa prima dell'aggiornamento.

Se si esegue l'aggiornamento dagli strumenti ONTAP per VMware vSphere 10,0 a 10,1, è necessario completare i seguenti passaggi prima di procedere con l'attività di aggiornamento:

Attiva diagnostica

1. Da vCenter Server, aprire una console agli strumenti ONTAP.
2. Accedere come utente di manutenzione.
3. Immettere **4** per selezionare **supporto e diagnostica**.
4. Immettere **2** per selezionare **attiva accesso diagnostico remoto**.
5. Immettere **y** per impostare la password desiderata.
6. Accedere all'indirizzo IP della macchina virtuale dal terminale/putty con l'utente come 'diag' e la password impostata nel passaggio precedente.

Esegui un backup di MongoDB

Esegui i seguenti comandi per eseguire un backup di MongoDB:

- `kn exec -it ntv-mongodb-0 sh - kn` è un alias di `kubectl -n ntv-system`.
- Eseguire il comando `env | grep MONGODB_ROOT_PASSWORD` all'interno del pod.
- Eseguire il comando `exit` per uscire dal pod.
- Eseguire `kN exec ntv-mongodb-0 --mongodump -u root -p MONGODB_root_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip` per sostituire il comando `MONGO_ROOT_PASSWORD` impostato dal comando precedente.
- Eseguire il comando `kN cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz` per copiare il backup mongodb creato utilizzando il comando sopra riportato dal pod all'host.

Prendere l'istantanea quaise di tutti i volumi

- Eseguire il comando '`kN get pvc`' e salvare l'output del comando.
- Acquisire snapshot di tutti i volumi uno alla volta utilizzando uno dei seguenti metodi:
 - Dalla CLI, eseguire il comando `volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>`
 - Dall'interfaccia utente di ONTAP System Manager, cercare il volume in base al nome nella barra di ricerca, quindi aprirlo selezionando il nome. Andare allo snapshot e aggiungere lo snapshot di quel volume.

Istantanea degli strumenti ONTAP per le VM VMware vSphere in vCenter (3VMs in caso di implementazione ha, 1 VM in caso di distribuzione non ha)

- Nell'interfaccia utente del client vSphere, selezionare la VM.
- Andare alla scheda istantanee e selezionare il pulsante **scatta istantanea**. Creare un'istantanea inattiva della VM. Per ulteriori informazioni, fare riferimento alla ["Scattare una fotografia istantanea di una macchina virtuale"](#) sezione.

Prima di eseguire l'aggiornamento, eliminare i pod completati dal bundle di log con il prefisso "generate-support-bundle-job". Se è in corso la generazione del bundle di supporto, attendere che venga completato, quindi eliminare il pod.

Per qualsiasi tipo di aggiornamento, è necessario aggiungere un'unità disco rigido (HDD) aggiuntiva da 100 GB. Per aggiungere un disco rigido, eseguire la seguente operazione.

1. Seleziona la macchina virtuale in configurazione a nodo singolo o in tutte e tre le macchine virtuali nella configurazione ha.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Aggiungi nuovo dispositivo > disco rigido**
3. Aggiungere un disco rigido da 100 GB nel campo **nuovo disco rigido**.
4. Selezionare **Applica**

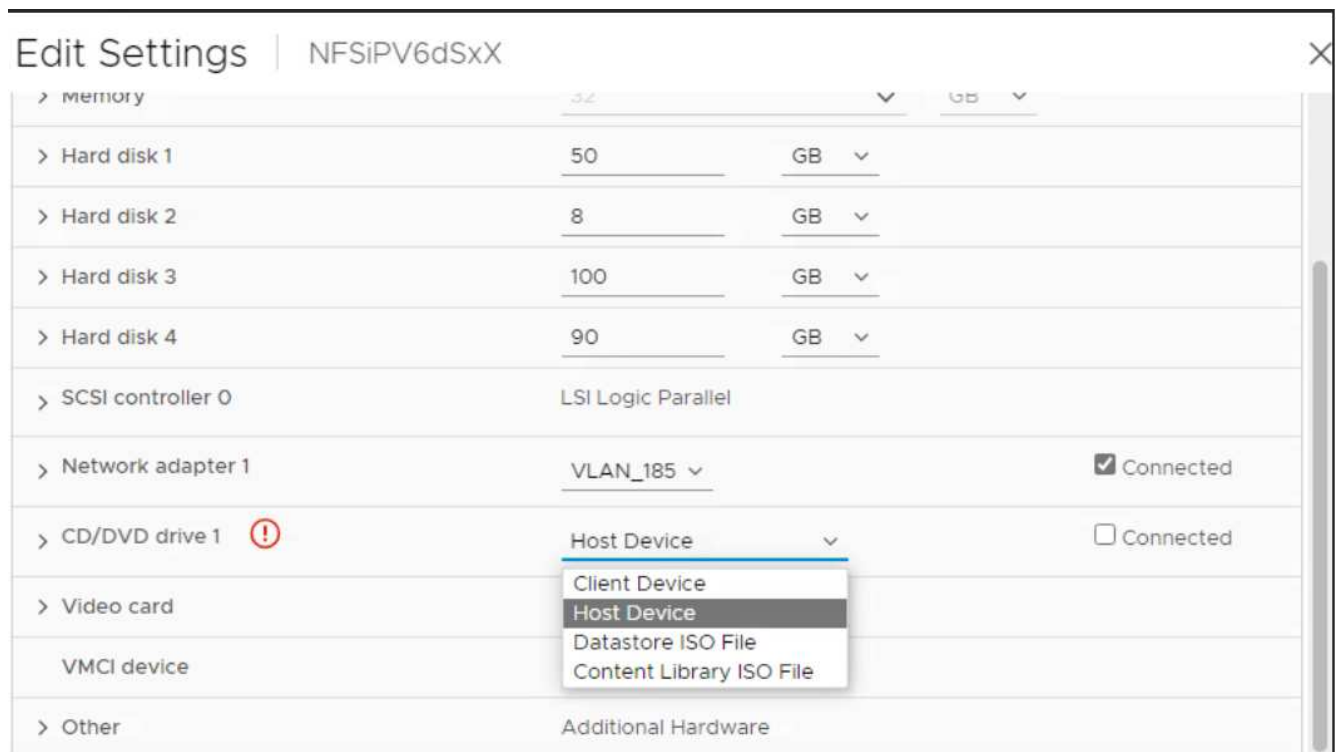
Dopo aver aggiunto il disco rigido, aggiornare le risorse della VM per le rispettive configurazioni e riavviare la VM primaria.

Verrà creato un nuovo disco rigido. Il provisioner dinamico dello storage utilizza questo HDD per generare o replicare i volumi.

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 nel campo **unità CD/DVD**.
4. Selezionare il file ISO e selezionare **OK**. Selezionare la casella di controllo connesso nel campo **unità CD/DVD**.



5. Da vCenter Server, aprire una console agli strumenti ONTAP.
6. Accedere come utente di manutenzione.
7. Immettere **3** per selezionare il menu Configurazione di sistema.
8. Immettere **7** per selezionare l'opzione di aggiornamento.
9. Quando si esegue l'aggiornamento, le seguenti azioni vengono eseguite automaticamente:
 - a. Aggiornamento del certificato
 - b. Aggiornamento del plug-in remoto

Dopo l'aggiornamento ai tool ONTAP per VMware vSphere 10,3, puoi:

- Disattivare i servizi dall'interfaccia utente di Manager
- Passaggio da un setup non ha a un setup ha
- Scala in verticale una configurazione piccola non ha un supporto non ha o una configurazione ha media o grande.
- In caso di aggiornamento non ha, riavviare la macchina virtuale degli strumenti ONTAP per riflettere le modifiche. In caso di upgrade ha, riavviare il primo nodo per riflettere le modifiche sul nodo.

Al termine

Dopo aver eseguito l'aggiornamento dalle versioni precedenti degli strumenti ONTAP per VMware vSphere alla versione 10,3, eseguire nuovamente la scansione degli adattatori SRA per verificare che i dettagli vengano aggiornati nella pagina adattatori di replica dello storage per il ripristino dei siti live di VMware.

Una volta completato l'aggiornamento, eliminare manualmente i Trident Volumes da ONTAP seguendo la procedura indicata di seguito:



Questi passaggi non sono necessari se i tool ONTAP per VMware vSphere 10,1 o 10,2 erano in configurazioni non ha piccole o medie (percorso locale).

1. Da vCenter Server, aprire una console agli strumenti ONTAP.
2. Accedere come utente di manutenzione.
3. Immettere **4** per selezionare il menu **supporto e diagnostica**.
4. Immettere **1** per selezionare l'opzione **Access Diagnostics shell**.
5. Eseguire il seguente comando

```
sudo python3 /home/maint/scripts/ontap_cleanup.py
```

6. Immettere il nome utente e la password di ONTAP

Eliminazione di tutti i volumi Trident in ONTAP utilizzati nei tool ONTAP per VMware vSphere 10,1/10,2.

Informazioni correlate

["Migrazione dai tool ONTAP per VMware vSphere 9.x a 10,3"](#)

Aggiornare i codici di errore

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 |
|---------------------------------------|--|---|
| 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. |

| | | |
|-----|---|--|
| 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. |
| 093 | L'aggiornamento del provisioner di storage dinamico non è riuscito | Riprovare a eseguire l'aggiornamento. |
| 094 | Il rollback del provisioner di storage dinamico non è riuscito | 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. |

| | | |
|-----|--|---|
| 108 | Seeding script non riuscito | - |
| 109 | il backup dei dati del volume persistente non è riuscito | Controllare i registri di aggiornamento e riprovare l'aggiornamento. |
| 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. |



I tool ONTAP per VMware vSphere 10,3 non supportano RPO pari a zero.

Scopri di più su ["Come ripristinare i tool ONTAP per VMware vSphere se l'aggiornamento non riesce dalla versione 10,0 alla 10,1"](#)

Esegui la migrazione dei tool ONTAP per VMware vSphere dalla 9.xx alla 10,3

Migrazione dai tool ONTAP per VMware vSphere 9.xx a 10,3

Lo spostamento degli strumenti NetApp ONTAP per la configurazione di VMware vSphere dalla versione 9.xx alla 10.x richiede un processo di migrazione a causa degli aggiornamenti e dei miglioramenti significativi del prodotto nelle versioni.

Puoi eseguire la migrazione da strumenti ONTAP per le release VMware vSphere 9.12D1 e 9.13D2 a 10,3.

Se nella configurazione sono presenti datastore NFS e VMFS e nessun datastore vVols, è sufficiente disinstallare ONTAP Tools 9.xx e installare ONTAP Tools 10.x. Tuttavia, se la configurazione contiene datastore vVols, sarà necessario eseguire la 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 ONTAP Tools 9.xx dal proprio ambiente. Fare riferimento a "Come rimuovere OTV 9.xx dal tuo ambiente" Articolo della Knowledge Base di NetApp. 2. "Distribuisci e configura gli strumenti ONTAP per VMware vSphere 10.3" 3. "Aggiornare il SRA" 4. "Creare policy di archiviazione VM" |



Dopo la migrazione da tool ONTAP per VMware vSphere 9.xx a 10,3, i datastore vVol che utilizzano il protocollo NVMe/FC non sono più operativi, perché gli strumenti ONTAP 10,3 supportano il protocollo NVMe-of solo con i datastore VMFS.

Migrare il provider VASA e aggiornare l'SRA

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. Implementazione di OVA per tool ONTAP per VMware vSphere 10,3.
3. Aggiungere l'istanza di vCenter Server che si desidera migrare agli strumenti ONTAP per VMware vSphere 10,3. Per ulteriori informazioni, fare riferimento ["Aggiungere un'istanza di vCenter Server"](#) a.
4. Integrare localmente il backend di archiviazione dalle API del server vCenter per il plug-in degli strumenti ONTAP.
5. 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}/migration-jobs>

Si può 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

```
arriciatura -X POST 'https://<OTV-NG-IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
--header 'x-auth: <token_autorizzazione>' \
--header 'Tipo di contenuto: application/json' \
--data '{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "nomeutente": "xxxxx", "password": "" }, "password_database": "" }'
```

Corpo della richiesta per un'altra migrazione delle release:

```
{ "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "nome utente": "xxxxx", "password": "" } }
```

Esempio di output JSON

Viene restituito un oggetto lavoro. È necessario salvare l'identificatore del lavoro per utilizzarlo nel passo successivo.

```
{ "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "running" }
```

6. 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
```

Dopo aver completato il processo, esaminare il rapporto sulla migrazione. Questo rapporto è incluso nei dati del lavoro ed è accessibile dalla risposta del lavoro.

7. Aggiungere gli strumenti ONTAP per il provider di storage VMware vSphere al vCenter Server e ["Registrare il provider VASA"](#) con strumenti ONTAP per VMware vSphere.
8. ["Attiva provider VASA"](#) Servizio sui tool ONTAP per VMware vSphere 10,3.
9. Stop ai tool ONTAP per il provider di storage VMware vSphere 9,10/9,11/9,12/9,13 il servizio provider VASA dalla console di manutenzione.

Non eliminare il provider VASA.

Una volta arrestato il vecchio provider VASA, vCenter Server esegue il failover sui tool ONTAP per VMware vSphere. Tutti i datastore e le macchine virtuali sono accessibili e vengono serviti dai tool ONTAP per VMware vSphere.

10. I datastore NFS e VMFS migrati dai tool ONTAP per VMware vSphere 9.xxx sono visibili nei tool ONTAP per VMware vSphere 10,3 solo dopo l'attivazione del processo di rilevamento del datastore, che potrebbe richiedere fino a 30 minuti. Verificare che i datastore siano visibili nella pagina di panoramica degli strumenti ONTAP per la pagina dell'interfaccia utente del plugin VMware vSphere.
11. 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

Esempio Curl

PATCH Curl -X. <https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43>

Esempio di output JSON

Viene restituito un oggetto lavoro. È necessario salvare l'identificatore del lavoro per utilizzarlo nel passo successivo.

```
{ "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "running" }
```

Il corpo della richiesta è vuoto per l'operazione 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 aver registrato gli strumenti ONTAP 10,3 in vCenter Server, attenersi alla seguente procedura:

- Attendere il completamento di **Discovery**; i certificati verranno aggiornati automaticamente su tutti gli host.
- Consentire un tempo sufficiente prima di avviare le operazioni del datastore e della macchina virtuale. Il periodo di attesa richiesto varia in base al numero di host, datastore e macchine virtuali all'interno della configurazione. La mancata attesa può causare guasti di funzionamento intermittenti.

Dopo l'aggiornamento, se lo stato di conformità della macchina virtuale è obsoleto, riapplicare il criterio di archiviazione attenendosi alla seguente procedura:

1. Accedere al datastore e selezionare **Riepilogo > Criteri archiviazione VM**.

Lo stato di conformità in **conformità ai criteri di archiviazione VM** viene visualizzato come **non aggiornato**.

2. Selezionare il criterio Storage VM e la VM corrispondente
3. Selezionare **Applica**

Lo stato di conformità in **conformità ai criteri di archiviazione VM** è ora visualizzato come conforme.

Informazioni correlate

- ["Scopri i tool ONTAP per VMware vSphere 10 RBAC"](#)
- ["Aggiornamento dai tool ONTAP per VMware vSphere 10.x alla 10,3"](#)

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 SRM 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 iniziare la migrazione se il failover è stato completato ma la nuova protezione è in sospenso. Prima di procedere con la migrazione, assicurarsi che il processo di protezione sia completato. Se è in corso un failover di test, ripulire il failover di test 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. Installare gli strumenti ONTAP per l'adattatore SRA VMware vSphere 10,3 seguendo la procedura descritta in ["Configurare SRA sull'appliance VMware Live Site Recovery"](#).
 - b. Nella pagina dell'interfaccia utente di VMware Live Site Recovery, eseguire le operazioni **Discover Arrays** e **Discover Devices** e verificare che i dispositivi vengano visualizzati come prima della migrazione.

Automatizza utilizzando l'API REST

Scopri i tool ONTAP per l'API REST VMware vSphere 10

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

I tool ONTAP per VMware vSphere 10 vengono implementati utilizzando l'architettura del plug-in remoto di 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 espongono 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 per i tool ONTAP per le API REST di VMware vSphere 10

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 bilanciatore di carico dei 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 e la porta è sempre 8443. Inoltre, per un'istanza specifica dei tool ONTAP per VMware vSphere 10 la prima parte dell'URL è costante. Solo la categoria di risorse e la risorsa specifica variano in base agli 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 di richiesta JSON fornito. Vengono conservati i valori chiave non modificabili dall'utente. |
| 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 '*'/*' 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. |

| Codice | Significato | Descrizione |
|--------|------------------|--|
| 201 | Creato | È stato creato un oggetto con un identificatore univoco per l'istanza di risorsa. |
| 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.

I tuoi primi tool ONTAP per la chiamata alle API REST di VMware vSphere 10

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 arricciatura.

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 per i tool ONTAP per l'API REST di VMware vSphere 10

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 relativo ai tool ONTAP per VMware vSphere 10,3"](#)

Informazioni sul copyright

Copyright © 2025 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 CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.